MASTER DATA PROCESSING AGREEMENT

ACUERDO MAESTRO DE PROCESAMIENTO DE DATOS
(de conformidad con el artículo 28 del Reglamento UE 2016/679)

ENTRE

Este acuerdo para la protección de datos personales se celebra entre el Proveedor, como se indica a continuación, y el Cliente, quien acepta el acuerdo. "**Proveedor**" indica la(s) siguiente(s) entidad(es):

(i) TeamSystem SpA, registrado en Pesaro (PU), via Sandro Pertini 88, código fiscal y Nº de IVA 01035310414, y/o

(ii) Reviso Soluciones Cloud S.L., empresa perteneciente al grupo encabezado por TeamSystem

Y

la entidad a la que se refiere el Acuerdo como cliente (en lo sucesivo, el "**Cliente**"),

en lo sucesivo denominadas colectivamente las "**Partes**" o individualmente como la "**Parte**".

CONSIDERANDO QUE:

a) El Cliente ha celebrado un acuerdo (o acuerdos) con el Proveedor (en lo sucesivo, el "**Acuerdo**").

b) En este "*acuerdo maestro de protección de datos*" (en adelante, el "**Acuerdo Maestro**" o "**MDPA**"), las Partes desean establecer cómo y en qué condiciones el Proveedor procesará los datos personales en relación con el Acuerdo y la prestación de los Servicios, así como sus obligaciones relacionadas con dicho procesamiento, incluido el deber del Proveedor como Procesador de Datos en virtud del artículo 28 del Reglamento General sobre Protección de Datos n.º 679, del 27 de abril de 2016 (en adelante, "**RGPD**").

c) Las características específicas de la actividad de procesamiento con respecto a cada uno de los Servicios se detallan en los "términos y condiciones especiales para el procesamiento de datos personales" que están disponibles en el sitio web: www.teamsystem.com/GDPR/DPA (en lo sucesivo, "**DPA- Condiciones especiales**") y se incorporan aquí por esta referencia.

A CONTINUACIÓN, POR LO TANTO, las Partes acuerdan lo siguiente:

1. DEFINICIONES E INTERPRETACIÓN

1.1. Los considerados anteriormente se incorporan a este MDPA mediante esta referencia. Tal como se utiliza en este MDPA, las siguientes palabras y expresiones tendrán los significados que se indican a continuación:

"Decisión de adecuación" significa una decisión de la Comisión Europea, basada en el Artículo 45 (3) de la RGPD, que evalúa que las leyes de un determinado país aseguran un nivel adecuado de protección, según lo exige la Ley de Protección de Datos Aplicable.

"Ley de Protección de Datos Aplicable" significa el RGPD y cualquier otra implementación legal y/o regulación (si corresponde) que sea efectivo bajo el RGPD o, en cualquier modo, en España con respecto a la protección de Datos Personales, incluyendo cualquier decisión emitida por una autoridad supervisora que tenga jurisdicción en la materia, que es y sigue siendo vinculante y efectiva (incluidos los requisitos establecidos en cualquier legislación anterior de protección de datos, en la medida en que sean aplicables y sigan siendo efectivos y vinculantes después del 25 de mayo de 2018).

"Sub-procesador de datos" significa cualquier subcontratista contratado por el Proveedor para cumplir, en su totalidad o en parte, obligaciones contractuales y que, durante dicho

desempeño, puede ser requerido para recopilar, acceder, recibir, almacenar o, de cualquier modo, procesar Datos Personales.

"Dirección de correo electrónico" significa la dirección o direcciones de correo electrónico proporcionadas por el Cliente al suscribirse a los Servicios o comunicadas por otros medios oficiales al Proveedor, donde el Cliente desea recibir comunicaciones del Proveedor.

"Usuario final" significa la persona (en su caso) que se beneficia de los Servicios en última instancia, actuando como Controlador de Datos.

"Instrucciones" significa las instrucciones escritas dadas por el Controlador en este MDPA (incluyendo el DPA relevante - Condiciones Especiales) y, si corresponde, en el Acuerdo.

"Fecha de entrada en vigor de MDPA" significa la fecha en que el Cliente ingresa en este MDPA con el Proveedor.

"Violación de Datos Personales" significa cualquier violación de seguridad que conduzca de manera accidental o ilegal a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a Datos Personales en los sistemas operados por el Proveedor o bajo su control.

"Datos personales" tiene el significado interpretado de acuerdo con la Ley de Protección de Datos aplicable e incluye, sin limitación, todos los datos proporcionados, almacenados, transmitidos, recibidos o procesados, o creados por el cliente o el usuario final en relación con la prestación de los Servicios, en la medida en que sean procesados por el Proveedor en virtud del Acuerdo. Se incluye una lista de las categorías de Datos Personales en DPA - Condiciones especiales.

"Personal del Proveedor" significa los oficiales, empleados, consultores y otro personal del Proveedor, pero no el personal de un Sub-procesador de Datos.

"Solicitud" significa una solicitud presentada por un Sujeto sobre el acceso, borrado o rectificación en relación con sus Datos Personales o para el ejercicio de otros de sus derechos establecidos en el RGPD.

"Servicio(s)" significa el servicio o servicios contemplados en los Acuerdos ejecutados ocasionalmente entre el Cliente y el Proveedor.

"Días laborables" significa cada día del calendario que no sea un sábado, domingo o un día festivo en España.

1.2. Las palabras "incluso" o "incluido" se interpretarán como si estuvieran acompañadas por la expresión "sin limitación", de modo que cualquier lista que siga a cualquiera de estas palabras estará compuesta en consecuencia de meros ejemplos y no será exhaustiva.

1.3. A los fines de esta MDPA, los términos "Sujeto de datos", "Procesamiento", "Controlador de Datos", "Procesador de Datos", "Transferencia" y "Medidas técnicas y organizativas apropiadas" se interpretarán de conformidad con la Ley de Protección de Datos Aplicable.

2. ROLES DE LAS PARTES

2.1. Las Partes reconocen y acuerdan que, en relación con el procesamiento de Datos Personales, el Proveedor actúa como el Procesador de Datos y, como regla general, el Cliente actúa como Controlador de Datos.

2.2. Si el Cliente está llevando a cabo el procesamiento en nombre de otro Controlador de Datos, el mismo Cliente puede actuar como un Procesador de Datos. En tal caso, el Cliente declara y garantiza que todas las instrucciones dadas y actividades llevadas a cabo en relación con el procesamiento de Datos Personales, incluido el nombramiento del Proveedor como un Subprocesador de Datos, que surjan de la ejecución por parte del Proveedor de este MDPA, han sido autorizadas por el correspondiente Controlador de Datos. El Proveedor deberá

presentar evidencia al Proveedor, previa solicitud por escrito de este último, sobre lo anterior.

2.3. En el procesamiento de Datos Personales, cualquiera de las Partes se compromete a cumplir con sus obligaciones bajo la Ley de Protección de Datos Aplicable.

2.4. El Proveedor ha designado un Oficial de Protección de Datos (DPO) domiciliado en la sede de TeamSystem SpA en Pesaro, a través de Sandro Pertini, 88. Correo electrónico: privacy@teamsystem.com. Teléfono: 0721/42661.

3. PROCESAMIENTO DE DATOS PERSONALES

3.1. Al celebrar este Acuerdo (y en cualquier DPA incorporada - Términos especiales), el Cliente confía al Proveedor el procesamiento de los Datos Personales con el fin de proporcionar los Servicios, tal como se detalla en el Acuerdo y en el DPA - Condiciones especiales. Los Términos especiales del DPA están disponibles a través de un enlace en el siguiente sitio web: www.teamsystem.com/GDPR/DPA.

3.2. El Proveedor se compromete a cumplir con las Instrucciones, disponiéndose que: si el Cliente hace una solicitud de enmiendas a cualquier Instrucción dada inicialmente, el Proveedor examinará la viabilidad relevante y luego acordará con el Cliente cómo gestionar dichas modificaciones y los costes asociados.

3.3. En los casos contemplados en el párrafo 3.2 y si las solicitudes realizadas por el Cliente conducen, en la opinión del Proveedor, a la infracción del procesamiento de Datos Personales de la Ley de Protección de Datos Aplicable, el Proveedor quedará liberado de la obligación de realizar tales Instrucciones e informará de inmediato al Cliente de esta ocurrencia. En tal caso, el Cliente puede considerar si se enmiendan las Instrucciones dadas o si se dirige a la Autoridad de Supervisión para que sus solicitudes sean declaradas lícitas.

4. RESTRICCIONES AL USO DE DATOS PERSONALES

4.1. Al procesar Datos Personales para proporcionar los Servicios, el Proveedor se compromete a que dicho procesamiento se lleve a cabo:

4.1.1. Solo en la medida y en el modo necesario para prestar los Servicios o para realizar correctamente sus obligaciones en virtud del Acuerdo y esta MDPA, o establecidas por la ley o por una autoridad supervisora o controladora competente. En este último caso, el Proveedor debe informar al Cliente (a menos que se lo impida la ley aplicable basada en el interés público) mediante un aviso a la dirección de correo electrónico.

4.1.2. De conformidad con las instrucciones del cliente.

4.2 El personal del Proveedor que tiene acceso a, o que lleva a cabo el procesamiento de, Datos Personales ha sido confiado con dicho procesamiento en base a las autorizaciones apropiadas y también ha recibido capacitación según sea necesario con respecto a dicho procesamiento. Además, este Personal está obligado a cumplir con las obligaciones de confidencialidad y con el código ético de la compañía y debe cumplir con las políticas de confidencialidad y protección de datos personales que han sido adoptadas por el Proveedor.

5. ACTIVIDADES DE PROCESAMIENTO ATRIBUIDAS A TERCEROS

5.1. En lo que respecta a las actividades de procesamiento encomendadas a los Subprocesadores de Datos, las Partes acuerdan lo siguiente:

5.1.1.El Cliente acepta expresamente que el Proveedor pueda confiar ciertas operaciones de procesamiento en relación con los Datos Personales a otras compañías pertenecientes

al grupo TeamSystem y/o a aquellos terceros que están especificados en el DPA - Condiciones especiales.

5.1.2. El Cliente acepta además que el Proveedor puede confiar ciertas operaciones de procesamiento en relación con Datos Personales también a otros terceros, de acuerdo con las formas especificadas en el siguiente párrafo 5.1.4.

5.1.3. Se observa que la ejecución de cláusulas contractuales estándar (según lo exige el siguiente artículo 7 para el caso de la transferencia de datos personales al extranjero) entre el cliente y un subprocesador de datos se considerará como un consentimiento para contratar a esa parte para actividades de procesamiento.

5.1.4. En aquellos casos en los que el Proveedor haga uso de los Subprocesadores de Datos para realizar específicas actividades de procesamiento en relación con Datos Personales, el Proveedor:

5.1.4.1. Se compromete a contratar exclusivamente a los Subprocesadores de Datos que otorguen la implementación de medidas técnicas y organizativas apropiadas y garantiza que el acceso a los datos personales, y su procesamiento correspondiente, se limitarán solo en la medida en que sean necesarios para proporcionar los servicios subdelegados.

5.1.4.2. Deberá informar al Cliente sobre dicho compromiso, notificando al menos 15 (quince) días antes del inicio de las actividades de procesamiento por parte del Subprocesador de Datos (incluyendo detalles relativos a la identidad del tercero en cuestión, su ubicación con, si corresponde, la especificación de la ubicación de los servidores para el almacenamiento de datos y las actividades encomendadas) por medio de la dirección de correo electrónico o de cualquier otro medio que el proveedor considere apropiado. El Cliente tendrá derecho a rescindir el Contrato dentro de los 15 (quince) días posteriores a la recepción del aviso, sin perjuicio de las obligaciones del Cliente de pagar los montos adeudados en la fecha de terminación del Contrato.

5.1.5. Información adicional sobre la lista de Subprocesadores de datos, las actividades de procesamiento confiadas a dichas partes y el lugar donde se encuentran, están disponibles en el DPA - Condiciones Especiales relacionados con los servicios activados por el cliente.

6. SEGURIDAD

6.1. *MEDIDAS DE SEGURIDAD DEL PROVEEDOR* - Al procesar los datos personales a los efectos de la prestación de los Servicios, el proveedor se compromete a aplicar las medidas técnicas y organizativas adecuadas para prevenir el procesamiento ilegal o no autorizado, destrucciones accidentales o ilícitas, daños, pérdidas accidentales, la alteración y la divulgación no autorizada de, o acceso a, Datos personales, como se describe en el Anexo 1 de esta MDPA ("**Medidas de seguridad**").

6.1.1. El Anexo 1 a la MDPA establece medidas apropiadas para la protección de los sistemas de archivo que son proporcionales al nivel de riesgo en relación con los Datos Personales, con el fin de garantizar la confidencialidad, integridad, disponibilidad y resistencia de los sistemas y de los servicios del Proveedor, las medidas apropiadas destinadas a permitir el restablecimiento del acceso a los datos personales de manera oportuna en el caso de una violación de datos personales, y las medidas destinadas a evaluar periódicamente la eficacia de tales medidas en el transcurso del tiempo. El Cliente reconoce y acepta que, teniendo en cuenta el estado de las gestiones técnicas,

los costes de implementación y la naturaleza, alcance, contexto y propósitos del procesamiento de datos personales, los procedimientos de seguridad y los principios que han sido adoptados por el Proveedor aseguran un nivel de protección adecuada al riesgo en relación con los datos personales.

6.1.2. El Proveedor puede actualizar y modificar las Medidas de Seguridad especificadas con anterioridad a lo largo del tiempo, siempre que tal actualización y enmiendas no impliquen una reducción del nivel general de seguridad de los Servicios. El Cliente será informado de cualquier actualización y enmienda mediante notificación transmitida a su dirección de correo electrónico.

6.1.3. Si el Cliente solicita medidas adicionales para la seguridad, no incluidas en las *Medidas de Seguridad*, el Proveedor se reserva el derecho a evaluar la factibilidad relevante y podría cargar algún coste adicional de implementación al Cliente.

6.1.4. El Cliente reconoce y acepta que el Proveedor, teniendo en cuenta la naturaleza de los Datos Personales y la información que está disponible para el Proveedor en base a las disposiciones específicas establecidas en el correspondiente DPA - Condiciones Especiales, ayudará al Cliente a garantizar el cumplimiento de las obligaciones de seguridad establecidas en los artículos del 32 al 34 del RGPD de la siguiente manera:

6.1.4.1. Implementando y manteniendo las Medidas de Seguridad actualizadas de acuerdo con las disposiciones establecidas en los párrafos anteriores 6.1.1, 6.1.2, 6.1.3.

6.1.4.2. Al cumplir con las obligaciones especificadas en el párrafo 6.3.

6.1.5. Las Partes acuerdan que, con referencia a los Acuerdos relativos a productos que se deban instalar en las instalaciones del Cliente o de cualquier proveedor del Cliente (en adelante, "**Productos instalables**"), las Medidas de Seguridad anteriores solo se aplicarán en relación con los Servicios que requieren el procesamiento de Datos Personales por parte del Proveedor o por cualquier parte delegada involucrada por este último (*por ejemplo,* soporte y asistencia remota o servicios de migración).

6.1.6. En caso de que el producto admita la integración con aplicaciones de terceros, el Proveedor no será responsable de la implementación de las Medidas de Seguridad en relación con los componentes de dichos terceros o de la forma operativa de ningún producto como consecuencia de dicha integración.

6.2. *MEDIDAS DE SEGURIDAD DEL CLIENTE* - Sin perjuicio de las obligaciones del Proveedor según el párrafo 6.1 anterior, el Cliente reconoce y acepta que, al utilizar los Servicios, sigue siendo un deber exclusivo del Cliente mantenerlos personales, y también por aquellos autorizados por el mismo Cliente para acceder a los Servicios, implementando medidas de seguridad apropiadas en relación con el uso de los Servicios.

6.2.1. A tal efecto, el Cliente se compromete a utilizar los Servicios y las características para el procesamiento de Datos Personales garantizando siempre un nivel de seguridad adecuado al riesgo real.

6.2.2. El Cliente además se compromete a implementar todas las medidas apropiadas para garantizar la protección de las credenciales de autenticación, los sistemas y dispositivos utilizados por el Cliente o por los usuarios del Usuario Final, para obtener acceso a los Servicios. El Cliente también se compromete a guardar y hacer copias de seguridad de los Datos Personales para garantizar su restauración en conformidad con las disposiciones de las leyes.

6.2.3. El Proveedor no tendrá ninguna obligación ni asumirá ninguna responsabilidad en relación con la protección de Datos Personales que el Cliente, o -si corresponde- el

Usuario Final, almacena o transfiere fuera de los sistemas utilizados por el Proveedor o por los Subprocesadores de Datos contratados por el proveedor (por ejemplo, en archivos en papel, o en centros de datos que pertenecen al cliente o al usuario final, como puede ocurrir en el caso de acuerdos sobre productos locales).

6.3. *INFRACCIONES DE DATOS* - Salvo los Acuerdos relativos a los Productos instalables, a los que no se aplicará este párrafo 6.3, el Proveedor, después de haber tenido conocimiento de una Infracción de datos personales, deberá:

6.3.1. Informar al Cliente sin demora indebida a través de la dirección de correo electrónico.

6.3.2. Adoptar medidas razonables para mitigar los daños que puedan surgir y proteger los Datos personales.

6.3.3. Proporcionar al Cliente una descripción de la Infracción de Datos Personales, en la medida de lo posible, incluyendo las medidas tomadas para prevenir o mitigar sus posibles efectos adversos y las actividades recomendadas por el Proveedor al Cliente a fin de abordar la Infracción de Datos Personales.

6.3.4. Guardar toda la información relativa a las Infracciones de Datos Personales, documentos relevantes, comunicaciones y avisos, confidenciales según lo dispuesto en el Acuerdo y abstenerse de divulgar cualquier dato e información a terceros sin la autorización previa por escrito del Controlador de Datos, salvo y en la medida en que dicha divulgación pueda ser estrictamente necesaria para cumplir las obligaciones del Cliente derivadas de la Ley de Protección de Datos Aplicable.

6.4. En los casos contemplados en el párrafo anterior 6.3, el Cliente será el único responsable del rendimiento, cuando lo exija la Ley de Protección de Datos Aplicable, de cualquier obligación de informar a terceros (o al Usuario final si el Cliente es el Procesador de Datos) en el caso de una Infracción de Datos Personales y de cualquier obligación de informar a la Autoridad de Supervisión y los Sujetos de Datos (si el Cliente es el Controlador de Datos).

6.5. Las Partes reconocen y aceptan que una comunicación sobre un Incumplimiento de Datos Personales o la implementación de medidas destinadas a abordar dicha Infracción de Datos Personales no implica el reconocimiento por parte del Proveedor de un incumplimiento o un pasivo en relación con el Incumplimiento de Datos Personales.

6.6. El Cliente informará oportunamente al Proveedor de cualquier abuso o uso indebido de las cuentas o credenciales de autenticación o de cualquier Infracción de Datos Personales de los que pueda tener conocimiento en relación con los Servicios.

7. RESTRICCIONES A LA TRANSFERENCIA DE DATOS PERSONALES A PAÍSES FUERA DEL ESPACIO ECONÓMICA EUROPEO (EEE)

7.1. El Proveedor no transferirá Datos Personales a países que estén fuera del EEE a menos que el Cliente dé su consentimiento a dicha transferencia.

7.2. Si un Subprocesador de Datos que se encuentra en un tercer país necesita una transferencia de Datos Personales para su almacenamiento o procesamiento, a falta de una decisión de adecuación por parte de la Comisión Europea sobre ese país de conformidad con el Artículo 45 de la RGPD, el proveedor:

7.2.1. hará que el subprocesador de datos ejecute las cláusulas contractuales estándar contempladas en la Decisión 2010/87 / UE de la Comisión, de 5 de febrero de 2010, para la transferencia de datos personales a los procesadores establecidos en terceros países ("**Cláusulas contractuales estándar**"), o texto equivalente, ya que puede ser enmendado recientemente. Se le proporcionará a este último una copia de dichas

Cláusulas Contractuales Estándar ejecutadas por el Proveedor en nombre del Cliente. Y/O

7.2.2. puede presentar formas alternativas al Cliente para la transferencia de Datos Personales que cumplan con los requisitos de la Ley de Protección de Datos Aplicable (*por ejemplo,* Protección de Privacidad en caso de que el Procesador de Datos esté en los EE. UU, y su adherencia pueda ser verificada a través de medios y registros oficiales, o transferencia intragrupo si el Subprocesador de Datos pertenece a un grupo de empresas cuyos BCRs han sido aprobados en relación con los Procesadores).

7.3. En los eventos bajo el párrafo anterior 7.2.1, mediante la ejecución de esta MDPA, el Cliente otorga expresamente al Proveedor la autoridad para ejecutar Cláusulas contractuales estándar con los Procesadores secundarios de datos mencionados en el DPA correspondiente - Condiciones especiales. Si el Usuario Final actúa como Controlador de Datos, el Cliente se compromete a informar a dicho Usuario Final de la transferencia y declara y garantiza que la autorización otorgada por dicho Usuario Final para contratar Subprocesadores de Datos fuera del EEE representa una autoridad equivalente a la anterior.

8. AUDITORÍAS Y CONTROLES

8.1. El Proveedor auditará periódicamente la seguridad de los sistemas de procesamiento de Datos Personales y los entornos utilizados por él para la prestación de los Servicios, así como las instalaciones donde se lleva a cabo el procesamiento. El Proveedor puede decidir seleccionar y confiar a ciertos consultores independientes la realización de tales auditorías, que se realizarán de acuerdo con estándares internacionales y/o mejores prácticas y cuyo resultado se describirá en informes especiales ("**Informes**"). Los Informes, que se considerarán como información confidencial del Proveedor, pueden ponerse a disposición del Cliente para permitir la verificación por este último del cumplimiento por parte del Proveedor de las obligaciones de seguridad establecidas en esta MDPA.

8.2. En los casos contemplados en el párrafo 8.1, el Cliente acepta ejercer su derecho de verificación simplemente accediendo a los Informes puestos a su disposición por el Proveedor.

8.3. El Proveedor reconoce que el Cliente tiene derecho, con los modales y en la medida que se especifica a continuación, a realizar auditorías independientes para verificar el cumplimiento por parte del Proveedor de las obligaciones de esta MDPA y el DPA correspondiente - Condiciones Especiales, y con las disposiciones de la ley. Para realizar tales actividades de auditoría, el Cliente puede decidir recurrir a empleados especializados o, a su elección, a consultores externos, siempre que estos últimos estén previamente obligados por las obligaciones de confidencialidad apropiadas.

8.4. En los casos contemplados en el párrafo 8.3 anterior, el Cliente debe enviar una solicitud previa al Oficial de Protección de Datos (DPO) del Proveedor. Ante tal solicitud de auditoría o inspección, el Proveedor y el Cliente acordarán, antes del inicio de las actividades, los detalles de las actividades de verificación (fecha de inicio y duración), los tipos de controles y el alcance de la verificación, las obligaciones de confidencialidad por las cuales el Cliente y los que realizan las actividades deben estar vinculados, y los costes, los cuales deben establecerse en función del tamaño y la duración de las actividades de verificación, y el Proveedor tendrá derecho a cobrar por dichas actividades.

8.5. El Proveedor tiene derecho a objetar, mediante aviso por escrito, en caso de que los auditores externos designados por el Cliente, en la opinión exclusiva del Proveedor, no cumplan con los requisitos de calificación o independencia adecuados, sean competidores del

Proveedor, o sean claramente no aptos. En cualquier caso, el Cliente debe designar nuevos auditores o realizar las auditorías directamente por sí mismo.

8.6. El Cliente se compromete a asumir los costes, si los hubiere, según los determine el Proveedor y se los comunique al Cliente de conformidad con el párrafo 8.4 anterior, de las maneras y dentro de los términos establecidos en el mismo. Todos los costes relacionados con cualquier actividad de verificación confiada por el Cliente a terceros se mantendrán total y exclusivamente a cargo del Cliente.

8.7. Todo lo anterior se entiende sin perjuicio de los derechos del Controlador de Datos y de las autoridades de supervisión establecidas en las Cláusulas Contractuales Estándar ejecutadas en virtud del Artículo 7 anterior (si corresponde), que no se verán afectadas por ninguna disposición establecida en esta MDPA o en el DPA relevante - Condiciones especiales.

8.8. Este artículo 8 no se aplicará a los acuerdos sobre productos locales.

8.9. Las actividades de verificación que involucren a los Subprocesadores de Datos se llevarán a cabo de conformidad con las reglas de acceso y con las políticas de seguridad establecidas por dichos Subprocesadores de Datos.

9. ASISTENCIA PARA GARANTIZAR EL CUMPLIMIENTO

9.1. El Proveedor ayudará al Cliente y promoverá la cooperación que se especifica a continuación para que el Cliente pueda cumplir con sus obligaciones según la Ley de Protección de Datos Aplicable.

9.2. En el caso en el que el Proveedor reciba una Solicitud o un reclamo sobre Datos Personales de un Sujeto de Datos, deberá invitar a este último a dirigir la Solicitud o reclamo al Cliente o al Usuario Final (si este último es el Controlador de Datos). En cualquier caso, el Proveedor informará oportunamente al Cliente de la recepción de la Solicitud a través de la Dirección de Correo Electrónico y le proporcionará al mismo Cliente toda la información disponible, junto con una copia de la Solicitud o reclamo. Esta cooperación se llevará a cabo mediante una excepción a la regla general de que las relaciones con los Sujetos de Datos quedan fuera del alcance de los Servicios y que la responsabilidad de gestionar los reclamos (si los hay) y de servir como contacto para los Sujetos de Datos en el ejercicio de sus derechos recae exclusiva y directamente con el Cliente o con el Usuario Final (si este último es el Controlador de Datos). El Cliente, o Usuario Final (si este último es el Controlador de Datos), será exclusivamente responsable de cualquier respuesta a tales Solicitudes o reclamaciones (si corresponde).

9.3. El Proveedor informará sin demora al Cliente, a menos que la ley lo prohíba, por medio de una notificación a través de la Dirección de Correo Electrónico, de cualquier inspección o solicitud de información que reciba de cualquier autoridad supervisora o policial en relación con el procesamiento de datos personales.

9.4. Si para cumplir con dicha Solicitud, el Cliente necesita recibir cierta información del Proveedor sobre el procesamiento de Datos Personales, el Proveedor deberá proporcionar asistencia en la medida que sea razonablemente posible, siempre que las solicitudes se hayan presentado con el aviso adecuado.

9.5. El Proveedor, teniendo en cuenta la naturaleza de los Datos Personales y de la información disponible para él, deberá ofrecer una asistencia razonable al Cliente para poner a su disposición información útil que permita al Cliente llevar a cabo evaluaciones de impacto en la protección de Datos Personales cuando sea requerido por la ley. En tales casos, el Proveedor deberá poner a disposición información general, basada en el Servicio, como la información incluida en el Acuerdo, en esta MDPA y en el DPA - Condiciones especiales

relacionados con los Servicios en cuestión. En caso de solicitudes de asistencia personalizada, es posible que el Cliente deba pagar un cargo. Es responsabilidad exclusiva del Cliente, o del Usuario Final (si este último es el Controlador de Datos), llevar a cabo la evaluación de impacto en función de las características del procesamiento de Datos Personales realizado por el mismo con respecto a los Servicios.

9.6. El Proveedor se compromete a proporcionar los Servicios basándose en los principios de minimización del procesamiento (privacidad por diseño y por defecto), sin perjuicio de que es responsabilidad del Cliente, o del Usuario Final (si este último es el Controlador de datos), garantizar que el procesamiento se lleva a cabo en cumplimiento de dichos principios y verificar que las medidas técnicas y organizativas del Servicio cumplirán con los requisitos de cumplimiento de la Compañía, incluidos los requisitos establecidos por la Ley de Protección de Datos Aplicable.

9.7. El Cliente reconoce y acepta que, en caso de una Solicitud de un Sujeto de Datos para la portabilidad de Datos Personales, y con referencia exclusiva a los Servicios que generan Datos Personales que son relevantes a este respecto, el Proveedor ayudará al Cliente poniendo a disposición la información necesaria para recuperar los datos requeridos en un formato que cumpla con la Ley de Protección de Datos Aplicable.

9.8. Los párrafos 9.5 y 9.7 no se aplicarán con respecto a ningún acuerdo relativo a los productos locales.

10. OBLIGACIONES DEL CLIENTE Y RESTRICCIONES

10.1. El Cliente se compromete a dar instrucciones de conformidad con la normativa y a utilizar los Servicios de conformidad con la Ley de Protección de Datos Aplicables y con el exclusivo propósito de procesar los Datos Personales que se hayan recopilado de conformidad con la Ley de Protección de Datos Aplicable.

10.2. El procesamiento de Datos Personales (si corresponde) según el Artículo 9 y el Artículo 10 de la RGPD solo se permitirá si así lo establece expresamente el DPA - Condiciones especiales. Sin embargo, para tales casos, el procesamiento de los Datos Personales contemplado en los artículos mencionados anteriormente se realizará exclusivamente previo acuerdo por escrito entre las Partes realizado de conformidad con las disposiciones del párrafo 3.2.

10.3. El Cliente se compromete a cumplir todas las obligaciones impuestas al Controlador de Datos de conformidad con la Ley de Protección de Datos Aplicable (y, en el caso de que dichas obligaciones recaigan sobre el Usuario Final, garantiza que el Usuario Final asuma un compromiso equivalente), incluidas las obligaciones de proporcionar cierta información a los sujetos de los datos (y garantiza que se asignen obligaciones equivalentes al usuario final si este último es el controlador de datos). Además, el Cliente se compromete a garantizar que el procesamiento de los Datos Personales mediante la utilización de los Servicios se realice siempre sobre una base legal adecuada.

10.4. Si debe darse un aviso de información y el consentimiento debe ser recogido por medio del producto contemplado en el Acuerdo, el Cliente declara haber considerado el producto y que dicho producto cumple con las necesidades del Cliente. El Cliente también tendrá la responsabilidad de evaluar si los formularios puestos a disposición por el Proveedor (si corresponde) para ayudar al Cliente a cumplir sus obligaciones de informar y recopilar el consentimiento (*por ejemplo,* modelo de política de privacidad para Aplicaciones o avisos de información que acompañan a las aplicaciones), cuando estén disponibles, cumplen con la Ley de Protección de Datos Aplicable y enmiende dichos formularios si se considera apropiado.

10.5. El Cliente asumirá además la total y exclusiva responsabilidad del tratamiento de los Datos Personales en cumplimiento de las Solicitudes (si las hubiera) enviadas por los Sujetos de Datos y, por lo tanto, para llevar a cabo, por ejemplo, cualquier enmienda, integración, rectificación y borrado de Datos Personales.

10.6. El cliente tiene la obligación de mantener la cuenta asociada a la dirección de correo electrónico siempre activa y actualizada.

10.7. El cliente reconoce que, de acuerdo con el artículo 30 de la RGPD, el Proveedor tiene el deber de mantener un registro de las actividades de procesamiento llevadas a cabo en nombre de los Controladores de Datos (o Procesadores) y que para ello recoge los datos de identificación y contacto de cada Controlador de Datos (y/o Procesador) en nombre del cual actúa y que dicha información debe ponerse a disposición de la autoridad competente, previa solicitud. Por lo tanto, cuando se solicite, el Cliente se compromete a proporcionar al Proveedor los datos de identificación y contacto mencionados anteriormente, de la manera especificada por el Proveedor periódicamente, y a mantener dicha información actualizada a través de los mismos medios.

10.8. Por lo tanto, el Cliente declara que el procesamiento de Datos Personales, como se describe en los Acuerdos, en este MDPA y en el correspondiente DPA - Condiciones Especiales, es legal.

11. DURACIÓN

11.1. Esta MDPA entrará en vigor en la Fecha Efectiva de la MDPA y terminará automáticamente en la fecha de borrado de todos los Datos Personales por parte del Proveedor, según lo dispuesto en esta MDPA y, si así se estipula, en el pertinente DPA - Condiciones Especiales.

12. DISPOSICIONES SOBRE LA DEVOLUCIÓN O ELIMINACIÓN DE DATOS PERSONALES

12.1. Al momento de la cancelación, por cualquier motivo, del Servicio, el Proveedor dejará de procesar Datos Personales y:

12.1.1. Borrará los Datos Personales (incluidas las copias relevantes, si corresponde) de los sistemas del Proveedor o que están bajo el control del Proveedor, dentro del plazo establecido en el Acuerdo, a menos que se requiera la retención de dichos datos para cumplir con las disposiciones de las leyes de España o de Europa.

12.1.2. Destruirá los Datos Personales que puedan haber sido almacenados en papel por el mismo Proveedor, a menos que se requiera la retención de dichos datos para cumplir con las disposiciones de las leyes del España o de Europa.

12.1.3. Pondrá a disposición del Cliente los Datos Personales para su recuperación durante un período de 12 (doce) meses posteriores a la finalización del Acuerdo. Durante dicho período, el procesamiento se limitará exclusivamente a la recuperación contemplada en el párrafo 12.2.

12.2. A menos que se disponga lo contrario en este MDPA, el Cliente reconoce que se le permite, después de la terminación del Servicio, recuperar los Datos Personales de las maneras especificadas en el Acuerdo y acepta su deber de recuperar los Datos Personales, en su totalidad o en parte, para la medida exclusiva que considere apropiada para la retención, y que dicha recuperación debe completarse dentro del término especificado en el párrafo 12.1.3.

12.3. Las Partes acuerdan que las disposiciones de los párrafos 12.1 y 12.2 no se aplicarán a los Acuerdos relativos a productos locales. En estos casos, el Cliente tiene el deber de recuperar los Datos Personales que considere apropiados para el almacenamiento, a más tardar 30 (treinta) días después de la finalización del Acuerdo. El Cliente reconoce y acepta que después de la

expiración de este término, los Datos Personales pueden no estar disponibles. Además, en los eventos considerados en este párrafo 12.3, es deber del Cliente cuidar el borrado de los Datos Personales como lo exige la ley.

12.4. Lo anterior se entiende sin perjuicio de lo que se puede establecer más adelante o de otro modo con respecto al borrado de Datos Personales en los relevantes DPA - Condiciones especiales.

13. RESPONSABILIDAD

13.1. Cualquiera de las Partes es responsable del cumplimiento de las obligaciones impuestas a esa Parte en virtud de este MDPA y las DPA relevantes - Condiciones especiales, así como en virtud de la Ley de Protección de Datos aplicable.

13.2. Sin perjuicio de las disposiciones legales obligatorias, el Proveedor compensará al Cliente en caso de incumplimiento de esta MDPA y/o de la DPA relevante - Condiciones especiales en la medida máxima acordada en el Acuerdo.

14. VARIOS

14.1. Este MDPA reemplaza cualquier otro acuerdo, contrato o acuerdo entre las Partes con respecto a su objeto, así como cualquier instrucción, en cualquier forma, entregada por el Cliente al Proveedor antes de la fecha de este MDPA con referencia a El tratamiento de los Datos Personales en el marco de la ejecución del Acuerdo.

14.2. El Proveedor puede enmendar este MDPA por medio de una notificación por escrito que se enviará al Cliente (por correo electrónico o con la ayuda de programas informáticos o de otro tipo). En este caso, el Cliente tendrá derecho a retirarse del Acuerdo mediante notificación por escrito al Proveedor para que la envíe por correo certificado con acuse de recibo dentro de los 15 días posteriores a la recepción de la notificación del Proveedor. Si el Cliente no ejerce este derecho de retiro dentro de los términos y maneras descritas anteriormente, las enmiendas a este MDPA se considerarán reconocidas y aceptadas por el Cliente y serán finalmente efectivas y vinculantes para las Partes.

14.3. En el caso de cualquier inconsistencia entre las disposiciones de este MDPA y las establecidas en el Acuerdo para la prestación de los Servicios o en cualquier documento del Cliente que no haya sido aceptado expresamente por el Proveedor al retirarse de este MDPA y/o de las respectivas DPA - Condiciones especiales, las disposiciones de esta MDPA y las correspondientes DPA - Condiciones especiales prevalecerán.

Cliente	**Reviso Soluciones Cloud S.L.**
Nombre y apellidos:	Nombre y apellidos:
Cargo:	Cargo:
Firma:	Firma:
Lugar y fecha:	Lugar y fecha:

Anexo 1

Medidas técnicas y organizativas

Además de las medidas de seguridad establecidas en el Acuerdo y en el MDPA, el Controlador de Datos aplicará las siguientes medidas de seguridad organizativas según el tipo de Servicio a través del cual se entrega o suscribe el producto, que se define en la DPA - Condiciones especiales:

A - Cloud SaaS (Nube - Software como servicio)
B - Iaas Services
C - BPO (Business Process Outsourcing)
D - BPI (Business Process Insourcing)
E - En las instalaciones

A - CLOUD SaaS

Medidas de seguridad organizacional	*Políticas y regulaciones para el usuario* - El Proveedor ha adoptado políticas y regulaciones detalladas, que todos los usuarios que tienen acceso a los sistemas de información deben cumplir, con el objetivo de garantizar que el comportamiento de los usuarios sea apropiado para garantizar el cumplimiento de los principios de confidencialidad, disponibilidad e integridad de los datos al utilizar recursos de información. *Autorización de acceso lógico* - El Proveedor define los perfiles de acceso según el privilegio mínimo necesario para llevar a cabo las tareas asignadas. Los perfiles de autorización se seleccionan y configuran antes del inicio del procesamiento y de tal manera que el acceso se restringirá solo a aquellos datos que sean estrictamente necesarios para las actividades de procesamiento. Los perfiles se someten a auditorías periódicas para evaluar si los requisitos para mantener los perfiles asignados todavía se cumplen. *Intervenciones de asistencia* - Las intervenciones de asistencia se gestionarán con el objetivo de garantizar que solo se realicen actividades contractuales y que se evite cualquier procesamiento innecesario en relación con los Datos Personales del Cliente o del Usuario final. *Evaluación de Impacto de la Protección de Datos (DPIA)* - De conformidad con los artículos 35 y 36 del RGPD y en base al documento "WP248 - Directrices sobre la evaluación de impacto de la protección de datos", adoptada por el Grupo de trabajo del artículo 29, el Proveedor ha preparado su propia metodología para el análisis y las evaluaciones de aquellas actividades de procesamiento que, teniendo en cuenta la naturaleza, el alcance, el contexto y los propósitos del procesamiento, pueden generar un alto riesgo para los derechos y libertades de las personas naturales, a fin de poder llevar a cabo una evaluación del impacto en la protección de datos personales antes del procesamiento. *Gestión de incidentes* - El Proveedor ha adoptado un procedimiento específico de gestión de incidentes destinado a garantizar la restauración de las operaciones de servicio ordinarias lo antes posible, al tiempo que garantiza el mantenimiento de los mejores niveles de servicio. *Violación de datos* - El Proveedor ha implementado un procedimiento especial, dirigido a la gestión de eventos e incidentes que probablemente tengan un impacto en los datos personales, que define los roles y responsabilidades, el proceso de detección del incidente / incumplimiento (sospechoso o real), la implementación de las acciones correctivas, la respuesta y la contención de tal incidente / infracción, así como las formalidades para informar al Cliente de violaciones de datos personales. *Capacitación* - El Proveedor ofrecerá periódicamente cursos de capacitación sobre el manejo adecuado de los datos personales a los miembros de su personal que participan en las actividades de procesamiento.

Medidas técnicas de seguridad	*Cortafuegos, IDPS* - Los datos personales deben estar protegidos contra el riesgo de una intrusión criminal mediante los Sistemas de Detección y Prevención de Intrusos (IDPS), que se mantendrán actualizados en función de las mejores tecnologías disponibles. *Seguridad de las líneas de comunicación* - Dentro del alcance de sus responsabilidades, el Proveedor deberá implementar protocolos de comunicación seguros que estén en línea con la tecnología disponible. *Protección contra malware* - Los sistemas deben estar protegidos contra el riesgo de una intrusión y de la actividad de ciertos programas mediante la activación de las herramientas electrónicas adecuadas que se actualizarán periódicamente. Las características del antivirus deben ser implementadas y actualizadas constantemente. *Credenciales de autenticación* - Los sistemas se configurarán de tal manera que el acceso se otorgará exclusivamente a aquellos que cuenten con credenciales de autenticación que permitan una identificación única del usuario. Esto incluye: un código asociado a una contraseña confidencial que solo será conocida por el usuario, o un dispositivo de autenticación que solo será retenido y usado por el usuario, que puede, en ciertos casos, estar asociado con un código de identificación o una contraseña. *Contraseña* - El uso de una contraseña, en lo que concierne a sus características básicas, es la obligación de cambiarla en el primer acceso, la longitud mínima, la ausencia de elementos que puedan ser fácilmente referidos a su titular, las reglas sobre su complejidad, la caducidad, el historial, la evaluación de la fuerza en contexto, la visualización y el almacenamiento, cumplirán con las mejores prácticas. Los usuarios que reciben credenciales también deben recibir instrucciones específicas sobre las medidas que deben adoptarse para garantizar que dichas credenciales permanezcan secretas. *Acceso* - Los sistemas pueden configurarse de tal manera que rastreen las solicitudes de acceso y, cuando sea apropiado, otras actividades que se llevan a cabo en relación con los diferentes tipos de usuarios (Administrador, Superusuario, etc.), y deben estar protegidos por Medidas de seguridad adecuadas que garanticen su integridad. *Copia de seguridad y restauración* - Se implementarán medidas apropiadas destinadas a garantizar la restauración del acceso a los datos en caso de daños a dichos datos o herramientas electrónicas, dentro de términos que sean ciertos y coherentes con los derechos de los interesados. Si cualquier acuerdo así lo requiere, se implementará un plan de operación de continuidad y, cuando sea necesario, se integrará con el plan de recuperación de desastres. Estos planes garantizan la disponibilidad y el acceso a los sistemas también en caso de eventos adversos graves que puedan persistir en el tiempo. *Evaluación de Vulnerabilidad y Prueba de Penetración* - El Proveedor realizará periódicamente análisis de vulnerabilidad dirigidos a evaluar el nivel de exposición a vulnerabilidades conocidas, en relación con las infraestructuras y el marco de operaciones, teniendo en cuenta los sistemas ya operativos que se encuentran en desarrollo. Cuando se considere apropiado, en relación con los riesgos potenciales que se han identificado, las evaluaciones anteriores se complementan, de vez en cuando, con técnicas especiales de prueba de penetración, que simulan el acceso no autorizado en varios escenarios de ataque, con el objetivo de controlar el nivel de seguridad alcanzado por las aplicaciones / sistemas / redes mediante el uso de las vulnerabilidades identificadas para eludir los mecanismos de seguridad físicos / lógicos y obtener acceso a ellos. El resultado de dichas evaluaciones se examina a fondo para detectar e implementar mejoras que son necesarias para garantizar el alto nivel de seguridad que se requiere.

B - Iaas Services

Medidas de Seguridad Organizativa	*Certificaciones* - El Proveedor ha obtenido las siguientes certificaciones / evaluaciones: ● ISO / IEC 27001: 2013: "Prestación de servicios para el diseño y gestión de infraestructura de TIC, gestión de aplicaciones dentro del grupo y gestión de infraestructura Cloud (IaaS)". ● ISO / IEC 27018: 2014 para la protección de datos personales en servicios de nube pública. *Autorización de acceso lógico* - El Proveedor define los perfiles de acceso según el privilegio mínimo necesario para llevar a cabo las tareas asignadas. Los perfiles de autorización se seleccionan y configuran antes del inicio del procesamiento y de tal manera que el acceso se restringirá solo a aquellos datos que sean estrictamente necesarios para las actividades de procesamiento. Los perfiles se someten a auditorías periódicas para evaluar si los requisitos para mantener los perfiles asignados todavía se cumplen. *Usuarios* - Los usuarios de los servicios se dividen en usuarios administrativos de la infraestructura de virtualización y usuarios administrativos de la consola para la administración de la infraestructura de la nube de TeamSystem. Las máquinas virtuales se configurarán de tal manera que el acceso se otorgará exclusivamente a aquellos que cuenten con credenciales de autenticación que permitan la identificación única del usuario. *Seguridad de las líneas de comunicación* - Dentro del alcance de sus responsabilidades, el Proveedor deberá implementar protocolos de comunicación seguros que estén en línea con la tecnología disponible en relación con el proceso de autenticación. *Gestión de cambios* - El Proveedor ha implementado un procedimiento específico para regular el proceso de gestión de cambios en vista de la introducción (en su caso) de innovaciones tecnológicas o en caso de modificaciones (en su caso) de su estructura básica y organizativa. *Capacitación* - El Proveedor ofrecerá periódicamente cursos de capacitación sobre el manejo adecuado de los datos personales a los miembros de su personal que participan en las actividades de procesamiento. *Protección contra malware* - Las máquinas virtuales deben estar protegidas contra el riesgo de una intrusión y de la actividad de ciertos programas mediante la activación de herramientas electrónicas apropiadas actualizadas periódicamente. Todas las máquinas virtuales se administrarán a través de funciones antivirus (tanto a nivel de hipervisor como de infraestructura). *Copia de seguridad y restauración* - Si así lo exige cualquier acuerdo, se deberán implementar medidas adecuadas para garantizar la restauración del acceso a los datos en caso de daños a dichos datos o herramientas electrónicas, dentro de términos que sean ciertos y consistentes con los derechos de los interesados. Es responsabilidad del Controlador de Datos decidir si realizar copias de seguridad de forma independiente durante el término del acuerdo y durante un período de 60 días después de su finalización.

	Acceso - Los sistemas pueden configurarse de tal manera que rastreen las solicitudes de acceso y, cuando sea apropiado, otras actividades que se llevan a cabo, en relación con los diferentes tipos de usuarios (Administrador, Superusuario, etc.), y deben estar protegidos mediante medidas de seguridad adecuadas garantizando su integridad. *Cortafuegos, IDS / IPS* - Los sistemas para prevenir intrusiones, tales como Firewall e IDS / IPS, se colocarán en el segmento de red que conecta la infraestructura de la nube con Internet para interceptar cualquier actividad maliciosa dirigida a degradar, total o parcialmente, la prestación del servicio. En el caso en cuestión, el equipo adoptado pertenece al tipo UTM SourceFire (Cisco), que incluye tanto el Firewall como el componente IDS / IPS. *Gestión de incidentes* - El Proveedor ha adoptado un procedimiento específico de gestión de incidentes destinado a garantizar la restauración de las operaciones de servicio ordinarias lo antes posible, al tiempo que garantiza el mantenimiento de los mejores niveles de servicio. *Alta confiabilidad* - El Proveedor garantiza una alta confiabilidad en los siguientes términos: ● La arquitectura del servidor se basará en la solución de virtualización VMWare y se implementará mediante la creación de redundancias físicas y virtuales de cada sistema, a fin de garantizar la tolerancia a fallos y la eliminación de puntos únicos de fracaso. En particular, en caso de fallo del sistema, el software de administración del entorno virtual podrá reasignar las actividades actuales a otros sistemas (principios de alta disponibilidad y balanceo de carga), minimizando las ineficiencias del servicio y asegurando la persistencia de las conexiones existentes. ● Cada servidor se coloca en una SAN conectada a través de iSCSI de alta velocidad. ● Todos los componentes de la infraestructura, incluidos los servidores, la seguridad y el equipo de red, los sistemas de almacenamiento y la infraestructura SAN, se han duplicado en su totalidad para eliminar puntos únicos de fallo. ● La infraestructura de red ha sido diseñada para proteger los sistemas de front-end de Internet y de las redes internas mediante un DMZ protegido por medio de cortafuegos separados de dos capas (estrategia de defensa en profundidad): un cortafuegos de límite conectado a Internet y un segundo firewall, incluidas las funciones de Prevención de intrusiones y antimalware y pertenecientes a la organización, configuración para proteger la DMZ y los sistemas backend. *Centro de datos* - El entorno de virtualización (incluida la red de área de almacenamiento SAN) se coloca en servidores que están alojados en un centro de datos ubicado en Italia y administrados por un proveedor certificado ISO 27001. En particular, se deben implementar las siguientes medidas de seguridad para proteger el Centro de Datos:

• Seguridad del perímetro exterior:
- Cerco externo que marca el límite de la propiedad a una altura no inferior a 3 metros, equipado con protección pasiva contra el ascenso.
- Monitoreo de áreas externas mediante barreras infrarrojas y / o sistemas de análisis de vídeo y por videovigilancia con sistemas de registro.
- Acceso peatonal individual restringido.
- Restringido el acceso a vehículos.
- Patrullas armadas.

• Seguridad del perímetro interior:
- Sala de vigilancia para el control de áreas internas y externas, supervisión.
- Uso de alarmas, manejo de visitantes mediante la entrega de insignias relativas a políticas de la empresa y con las regulaciones específicas para centros de datos.
- Escritorio de recepción para el control de entrada.
- Torniquetes de tres brazos colocados frente a la sala de vigilancia y recepción.

• Alta seguridad del perímetro interno:
- Acceso sincronizado a salas de sistemas equipados con protección pasiva.
- Sistema de control de entrada basado en listas de personas “AUTORIZADAS”.
- Sensores magnéticos que detectan el estado de las puertas.
- Salidas de emergencia con sensores que detectan el estado de las puertas.

Todas las alarmas están conectadas de forma remota a la sala de vigilancia.

C -BUSINESS PROCESS OUTSOURCING (BPO)

Medidas de Seguridad Organizativa	*Certificaciones* - El Proveedor ha obtenido las siguientes certificaciones / evaluaciones: ● ISO / IEC 27001: 2013: "Entrega de servicios para el diseño y gestión de infraestructura de TIC, gestión de aplicaciones dentro del Grupo y Gestión de infraestructura en la nube (IaaS)". ● ISO / IEC 27018: 2014 para la protección de datos personales en servicios de nube pública. *Políticas y regulaciones de usuario* - El Proveedor ha adoptado políticas y regulaciones detalladas, que todos los usuarios que tienen acceso a los sistemas de información deben cumplir, con el objetivo de garantizar que el comportamiento de los usuarios sea apropiado para garantizar el cumplimiento de los principios de confidencialidad, disponibilidad e integridad de los datos al utilizar recursos de información. *Autorización de acceso lógico* - El Proveedor define los perfiles de acceso según el privilegio mínimo necesario para llevar a cabo las tareas asignadas. Los perfiles de autorización se seleccionan y configuran antes del inicio del procesamiento y de tal manera que el acceso se restringirá solo a aquellos datos que sean estrictamente necesarios para las actividades de procesamiento. Los perfiles se someten a auditorías periódicas para evaluar si los requisitos para mantener los perfiles asignados todavía se cumplen. *Intervenciones de asistencia* - El Proveedor debe gestionar las intervenciones de asistencia con el objetivo de garantizar que solo se realicen actividades contractuales y que se evite cualquier procesamiento innecesario en relación con los Datos personales del Cliente o del Usuario final. *Gestión de cambios* - El Proveedor ha implementado un procedimiento específico para regular el proceso de gestión de cambios en vista de la introducción (en su caso) de innovaciones tecnológicas o en caso de modificaciones (en su caso) de su estructura básica y organizativa. *Evaluación de Impacto de la Protección de Datos (DPIA)* - De conformidad con los artículos 35 y 36 del RGPD y en base al documento "WP248 - Directrices sobre la evaluación de impacto de la protección de datos", adoptada por el Grupo de trabajo del artículo 29, el Proveedor ha preparado su propia metodología para el análisis y las evaluaciones de aquellas actividades de procesamiento que, teniendo en cuenta la naturaleza, el alcance, el contexto y los propósitos del procesamiento, pueden generar un alto riesgo para los derechos y libertades de las personas naturales, a fin de poder llevar a cabo una evaluación del impacto en la protección de datos personales antes del procesamiento. *Gestión de incidentes* - El Proveedor ha adoptado un procedimiento específico de gestión de incidentes destinado a garantizar la restauración de las operaciones de servicio ordinarias lo antes posible, al tiempo que garantiza el mantenimiento de los mejores niveles de servicio.

	Violación de datos - El Proveedor ha implementado un procedimiento especial, dirigido a la gestión de eventos e incidentes que probablemente tengan un impacto en los datos personales, que define los roles y responsabilidades, el proceso de detección del incidente / incumplimiento (sospechoso o real), la implementación de las acciones correctivas, la respuesta y la contención de dicho incidente / infracción, así como los trámites para informar al Cliente sobre infracciones de datos personales. *Capacitación* - El Proveedor ofrecerá periódicamente cursos de capacitación sobre el manejo adecuado de los datos personales a los miembros de su personal que participan en las actividades de procesamiento.

Medidas de seguridad técnicas	*Alta confiabilidad* - El Proveedor garantiza una alta confiabilidad en los siguientes términos: ● La arquitectura del servidor se basará en la solución de virtualización VMWare y se implementará mediante la creación de redundancias físicas y virtuales de cada sistema, a fin de garantizar la tolerancia a fallos y la eliminación de puntos únicos de fracaso. En particular, en caso de fallo del sistema, el software de administración del entorno virtual podrá reasignar las actividades actuales a otros sistemas (principios de alta disponibilidad y balanceo de carga), minimizando las ineficiencias del servicio y asegurando la persistencia de las conexiones existentes. ● Cada servidor se coloca en una SAN conectada a través de iSCSI de alta velocidad. ● Todos los componentes de la infraestructura, incluidos los servidores, la seguridad y el equipo de red, los sistemas de almacenamiento y la infraestructura SAN, se han duplicado en su totalidad para eliminar puntos únicos de fallo. ● La infraestructura de red ha sido diseñada para proteger los sistemas de front-end de Internet y de las redes internas mediante un DMZ protegido por medio de cortafuegos separados de dos capas (estrategia de defensa en profundidad): un cortafuegos de límite conectado a Internet y un segundo firewall, incluidas las funciones de prevención de intrusiones y antimalware y pertenecientes a la organización, configuración para proteger la DMZ y los sistemas backend. *Endurecimiento* - Las actividades de endurecimiento especialmente diseñadas deben implementarse con el objetivo de prevenir incidentes de seguridad, minimizando las debilidades arquitectónicas de los sistemas operativos, las aplicaciones y los equipos de red teniendo en cuenta, en particular, la reducción de los riesgos relacionados con el sistema, vulnerabilidades, la reducción de los riesgos relacionados con las aplicaciones instaladas en los sistemas y el aumento del nivel de protección que cubre los servicios prestados. *Cortafuegos, IDS / IPS* - Los sistemas para prevenir intrusiones, tales como Firewall e IDS / IPS, se colocarán en el segmento de red que conecta la infraestructura de la nube con Internet para interceptar cualquier actividad maliciosa dirigida a degradar, total o parcialmente, la prestación del servicio. En el caso en cuestión, el equipo adoptado pertenece al tipo UTM SourceFire (Cisco), que incluye tanto el Firewall como el componente IDS / IPS. *Seguridad de las líneas de comunicación* - Dentro del alcance de sus responsabilidades, el Proveedor deberá implementar protocolos de comunicación seguros que estén en línea con la tecnología disponible. *Protección contra malware* - Las máquinas virtuales deben estar protegidas contra el riesgo de una intrusión y de la actividad de ciertos programas mediante la activación de herramientas electrónicas apropiadas para ser actualizadas periódicamente. Todas las máquinas virtuales se administrarán a través de funciones antivirus (tanto a nivel de hipervisor como de infraestructura). *Credenciales de autenticación* - Los sistemas se configurarán de tal manera que el acceso se otorgará exclusivamente a aquellos que cuenten con credenciales de autenticación que permitan una identificación única del usuario. Esto incluye: un código asociado a una contraseña confidencial que solo será conocida por el usuario, o un dispositivo de autenticación que solo será retenido y usado por el usuario, que puede, en ciertos casos, estar asociado con un código de identificación o una contraseña.

	Contraseña - El uso de una contraseña, en lo que concierne a sus características básicas, es la obligación de cambiarla en el primer acceso, la longitud mínima, la ausencia de elementos que puedan ser fácilmente referidos a su titular, las reglas sobre su complejidad, la caducidad, el historial, la evaluación de la fuerza en contexto, la visualización y el almacenamiento, cumplirán con las mejores prácticas. Los usuarios que reciben credenciales también deben recibir instrucciones específicas sobre las medidas que deben adoptarse para garantizar que dichas credenciales permanezcan secretas. *Acceso* - Los sistemas pueden configurarse de tal manera que rastreen las solicitudes de acceso y, cuando sea apropiado, otras actividades que se llevan a cabo, en relación con los diferentes tipos de usuarios (Administrador, Superusuario, etc.), y deben estar protegidos mediante medidas de seguridad adecuadas garantizando su integridad. *Copia de seguridad y restauración* - Se implementarán medidas apropiadas destinadas a garantizar la restauración del acceso a los datos en caso de daños a dichos datos o herramientas electrónicas, dentro de términos que sean ciertos y coherentes con los derechos de los interesados. Es responsabilidad del Controlador de Datos decidir si realizar copias de seguridad de forma independiente durante el término del acuerdo y durante un período de 60 días después de su finalización. Si cualquier acuerdo así lo requiere, se implementará un plan de operación de continuidad y, cuando sea necesario, se integrará con el plan de recuperación de desastres. Estos planes garantizan la disponibilidad y el acceso a los sistemas también en caso de eventos adversos graves que puedan persistir en el tiempo. *Evaluación de Vulnerabilidad y Prueba de Penetración* - El Proveedor realizará periódicamente análisis de vulnerabilidad dirigidos a evaluar el nivel de exposición a vulnerabilidades conocidas, en relación con las infraestructuras y el marco de operaciones, teniendo en cuenta los sistemas ya operativos que se encuentran en desarrollo. Cuando se considera apropiado, en relación con los riesgos potenciales que se han identificado, las evaluaciones anteriores se complementan, de vez en cuando, con técnicas especiales de prueba de penetración, que simulan el acceso no autorizado en varios escenarios de ataque, con el objetivo de controlar el nivel de seguridad alcanzado por las aplicaciones / sistemas / redes mediante el uso de las vulnerabilidades identificadas para eludir los mecanismos de seguridad físicos / lógicos y obtener acceso a ellos. El resultado de dichas evaluaciones se examina a fondo para detectar e implementar mejoras que son necesarias para garantizar el alto nivel de seguridad que se requiere. *Administradores del sistema* - Todos los usuarios que operen como administradores del sistema deberán estar indicados en una lista que se actualizará periódicamente y las tareas que se les asignen deberán estar debidamente definidas en documentos especiales de nombramiento. La actividad realizada por los administradores del sistema debe ser monitoreada por medio de un sistema de administración de registros que permita rastrear con precisión todas las actividades realizadas y almacenar dichos datos de manera inmutable para permitir el monitoreo también después del desempeño. El comportamiento de los administradores del sistema debe ser auditado para verificar el cumplimiento de las medidas organizativas, técnicas y de seguridad en relación con el procesamiento de datos personales según lo exigen las normativas vigentes.

	Centro de datos - El entorno de virtualización (incluida la SAN - Red de área de almacenamiento) se coloca en servidores que están alojados en un centro de datos ubicado en Italia y administrados por un proveedor certificado ISO 27001. En particular, se deben implementar las siguientes medidas de seguridad para proteger el Centro de Datos: • Seguridad del perímetro exterior: ● Cerco externo que marca el límite de la propiedad a una altura no inferior a 3 metros, equipado con protección pasiva contra el ascenso. ● Monitoreo de áreas externas mediante barreras infrarrojas y / o sistemas de análisis de vídeo y por videovigilancia con sistemas de registro. ● Acceso peatonal individual restringido. ● Restringido acceso a vehículos. ● Patrullas armadas. • Seguridad del perímetro interior: ● Sala de vigilancia para el control de áreas internas y externas, supervisión. ● Uso de alarmas, manejo de visitantes con la entrega de insignias relativas a políticas de la empresa y con las regulaciones específicas para centros de datos. ● Escritorio de recepción para el control de entrada. ● Torniquetes de tres brazos colocados frente a la sala de vigilancia y recepción. • Alta seguridad del perímetro interno: ● Acceso sincronizado con salas de sistemas equipados con protección pasiva. ● Sistema de control de entrada basado en listas de personas “AUTORIZADAS”. ● Sensores magnéticos que detectan el estado de las puertas. ● Salidas de emergencia con sensores que detectan el estado de las puertas. Todas las alarmas están conectadas de forma remota a la sala de vigilancia.

D - BPI - SEGURO DE PROCESOS DE NEGOCIO

Medidas de Seguridad Organizacional	*Políticas y regulaciones del usuario* - El Proveedor ha adoptado políticas y regulaciones detalladas, que todos los usuarios que tienen acceso a los sistemas de información deben cumplir, con el objetivo de garantizar que el comportamiento de los usuarios sea apropiado para garantizar el cumplimiento de los principios de confidencialidad, disponibilidad e integridad de los datos al utilizar recursos de información. *Autorización de acceso lógico* - El Proveedor define los perfiles de acceso según el privilegio mínimo necesario para llevar a cabo las tareas asignadas. Los perfiles de autorización se seleccionan y configuran antes del inicio del procesamiento y de tal manera que el acceso se restringirá solo a aquellos datos que sean estrictamente necesarios para las actividades de procesamiento. Los perfiles se someten a auditorías periódicas para evaluar si los requisitos para mantener los perfiles asignados todavía se cumplen. *Violación de datos* - El proveedor ha implementado un procedimiento especial, dirigido a la gestión de eventos e incidentes que probablemente tengan un impacto en los datos personales, que define los roles y responsabilidades, el proceso de detección del incidente / incumplimiento (sospechoso o real), la implementación de las acciones correctivas, la respuesta y la contención de dicho incidente / infracción, así como los trámites para informar al Cliente sobre infracciones de datos personales. *Capacitación* - El Proveedor ofrecerá periódicamente cursos de capacitación sobre el manejo adecuado de los datos personales a los miembros de su personal que participan en las actividades de procesamiento.

Medidas Técnicas de Seguridad	*Seguridad de las líneas de comunicación* - Dentro del alcance de sus responsabilidades, el Proveedor deberá implementar protocolos de comunicación seguros que estén en línea con la tecnología disponible en relación con el proceso de autenticación. *Copia de seguridad y restauración* - Si así lo exige cualquier acuerdo, se deben implementar medidas adecuadas para garantizar la restauración del acceso a los datos en caso de daños a dichos datos o herramientas electrónicas, dentro de términos que sean ciertos y consistentes con los derechos de los interesados.

E - ON PREMISES

Medidas de Seguridad Organizativas	*Políticas y regulaciones del usuario* - El Proveedor ha adoptado políticas y regulaciones detalladas, que todos los usuarios que tienen acceso a los sistemas de información deben cumplir, con el objetivo de garantizar que el comportamiento de los usuarios sea apropiado para garantizar el cumplimiento de los principios de confidencialidad, disponibilidad e integridad de los datos al utilizar recursos de información. *Autorización de acceso lógico* - El Proveedor define los perfiles de acceso según el privilegio mínimo necesario para llevar a cabo las tareas asignadas. Los perfiles de autorización se seleccionan y configuran antes del inicio del procesamiento y de tal manera que el acceso se restringirá solo a aquellos datos que sean estrictamente necesarios para las actividades de procesamiento. Los perfiles se someten a auditorías periódicas para evaluar si los requisitos para mantener los perfiles asignados todavía se cumplen. *Intervenciones de asistencia* - El Proveedor debe gestionar las intervenciones de asistencia con el objetivo de garantizar que solo se realicen actividades contractuales y que se evite cualquier procesamiento innecesario en relación con los Datos Personales del Cliente. *Gestión de Incidentes y Violación de Datos* - El proveedor ha implementado un procedimiento especial, dirigido a la gestión de eventos e incidentes que probablemente tengan un impacto en los datos personales, que define los roles y responsabilidades, el proceso de detección del incidente / incumplimiento (sospechoso o real), la implementación de las acciones correctivas, la respuesta y la contención de dicho incidente / infracción, así como los trámites para informar al Cliente sobre infracciones de datos personales. *Capacitación* - El Proveedor ofrecerá periódicamente cursos de capacitación sobre el manejo adecuado de los datos personales a los miembros de su personal que participan en las actividades de procesamiento.

Medidas Técnicas de Seguridad	*Seguridad de las líneas de comunicación* - Dentro del alcance de sus responsabilidades, durante la fase de asistencia técnica, el Proveedor deberá implementar protocolos de comunicación seguros que estén en línea con la tecnología disponible. *Protección contra malware* - Las estaciones de trabajo utilizadas durante la fase de asistencia técnica deben protegerse contra el riesgo de una intrusión y de la actividad de ciertos programas mediante la activación de las herramientas electrónicas adecuadas que se actualizarán periódicamente. Todas las máquinas virtuales se administran a través de funciones antivirus (tanto a nivel de hipervisor como de infraestructura). *Administradores del sistema* - Todos los usuarios que operen como administradores del sistema deberán estar indicados en una lista que se actualizará periódicamente y las tareas que se les asignen deberán estar debidamente definidas en documentos especiales de nombramiento. La actividad realizada por los administradores del sistema debe ser monitoreada por medio de un sistema de administración de registros que permita rastrear con precisión todas las actividades realizadas y almacenar dichos datos de manera inmutable para permitir el monitoreo también después del desempeño. El comportamiento de los administradores del sistema debe ser auditado para verificar el cumplimiento de las medidas organizativas, técnicas y de seguridad en relación con el procesamiento de datos personales según lo exigen las normativas vigentes.