Anexo sobre Procesamiento de datos 1

El presente Anexo sobre Procesamiento de datos (en adelante: "Anexo") se celebra en la Fecha de entrada en vigencia, por y entre:

El Cliente, según se define en el Enunciado de trabajo o SOW

– en lo sucesivo denominado "**Controlador**" –

en la fila

a entidad Datasite, como se define en el Enunciado de trabajo o SOW

– en lo sucesivo denominado "**Procesador**" –

En lo sucesivo, cada uno de los cuales se denominará individualmente también como "**Parte**" y colectivamente como "**Partes**"

Preámbulo:

(A) Las Partes han celebrado un Acuerdo que describe los Servicios que se proporcionarán (definiciones proporcionadas en la Sección 1 a continuación). Como parte de la entrega de Servicios por parte del Procesador, el Controlador podrá transferir Datos personales al Procesador.

(B) En caso de conflicto entre las disposiciones del presente Anexo y las disposiciones establecidas en el Acuerdo, prevalecerá la disposición o las disposiciones del presente Anexo. Los términos en mayúscula no definidos en este Anexo se definen en el Acuerdo.

(C) Para garantizar el cumplimiento de las Partes respecto de las obligaciones de procesamiento de conformidad con las Reglas de protección de datos, que podrán modificarse periódicamente, las Partes acuerdan lo siguiente:

1. Definiciones

1.1. "**Apéndice**" significa el apéndice anexado y parte integrante del presente Anexo;

1.2. "**País de Protección de Datos**" o "Países de Protección de Datos" se refiere a los países donde existen leyes de privacidad, protección de datos o de seguridad de la información que regulan la información privada o los Datos Personales, incluidos, entre otros, el Espacio Económico Europeo, Brasil, Hong Kong, Australia, Singapur, Canadá, el Reino Unido y Suiza.

1.3. "**Reglas de Protección de Datos**" se refiere a las leyes nacionales apropiadas que se aplican al Procesamiento de datos personales en los Países de protección de datos, incluidas, entre otras, las leyes y regulaciones de privacidad y seguridad de la información que se aplican ocasionalmente;

1.4. "**Sujeto de Datos**" se refiere a una persona física identificada o identificable cuyos Datos Personales están sujetos a Procesamiento; una persona identificable es aquella que puede ser identificada, directa o indirectamente, por referencia a un identificador, como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de identidad física, fisiológica, genética, mental, económica, cultural o social;

1.5. "**Incidente de Seguridad de la Información**" se refiere a cualquier transferencia, acceso y divulgación a terceros, o Procesamiento en violación del presente Anexo o de las Reglas de Protección de Datos, o cualquier evento que afecte directa o indirectamente la confidencialidad, integridad y autenticidad de los Datos Personales;

1.6. "**Escudo de Privacidad**" se refiere al Marco del Escudo de Privacidad UE - EE. UU., que entró en vigencia el 1º de agosto de 2016, y el Marco del Escudo de Privacidad Suiza - EE. UU. que entró en vigencia el 12 de abril de 2017.

1.7. **"Acuerdo"** se refiere al Enunciado de Trabajo y los Términos y Condiciones Generales entre el Controlador y el Procesador;

1.8. "**Datos Personales**" se refiere a cualquier información relacionada con un Sujeto de Datos incluido en el Contenido.

1.9. "**Proceso**", "**Procesamiento**" o "**Procesado**" significa cualquier operación o conjunto de operaciones realizadas respecto de los Datos Personales, ya sea por medios automáticos o no automáticos, como recopilación, registro, organización, estructuración, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o poner a disposición, alineación o combinación, bloqueo, borrado o destrucción;

1.10 "**Servicios**" se refiere a la prestación de servicios según se describe en el Acuerdo y en el presente Anexo;

1.11 "**Categorías Especiales de Datos**" se refiere a los Datos Personales que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, los datos genéticos, los datos biométricos que identifican de manera única a una persona natural, así como Datos Personales sobre la salud, la vida sexual u la orientación sexual.

2. Actividades de Procesamiento

El Controlador tendrá la responsabilidad exclusiva de la precisión, calidad y legalidad del Procesamiento de Datos Personales, y deberá cumplir y asumir la responsabilidad por el cumplimiento de las Reglas de Protección de Datos aplicables de parte de sus Usuarios invitados. El Procesador acepta Procesar los Datos personales para proporcionar Servicios de acuerdo con el presente Anexo y el Acuerdo, de conformidad con las instrucciones escritas del Controlador según se establece en el Apéndice 1 de este Anexo, y según lo comunicado por el Controlador ocasionalmente. Si el Procesador cree que una instrucción infringe las Reglas de protección de datos aplicables, lo notificará de inmediato al Controlador. El procesador se compromete a Procesar los Datos personales de acuerdo con las Reglas de protección de datos aplicables.

3. Duración y Rescisión del Presente Anexo

3.1. El presente Anexo es efectivo a partir de la Fecha de Entrada en Vigencia y permanecerá vigente durante el plazo del Acuerdo. Este Anexo se terminará automáticamente con la rescisión o vencimiento de cualquier SOW.

3.2. No obstante la rescisión del presente Anexo, el Procesador y cualquier subcontratista continuarán sujetos a sus obligaciones de confidencialidad.

4. Transferencias Internacionales

El procesador se encuentra certificado bajo los Marcos del Escudo de Privacidad y se encuentra comprometido con sus principios. El Controlador reconoce que el Procesador puede Procesar Datos personales fuera del EEE, Reino Unido y Estados Unidos; sin embargo, los datos personales se seguirán almacenando en un País de protección de datos o en Estados Unidos. El Procesador solo transferirá Datos Personales de conformidad con las Reglas de Protección de Datos y notificará al Controlador si ya no le es posible proporcionar el nivel de protección adecuado según lo requerido por las Reglas de Protección de Datos.

5. Estándares de Confidencialidad y Seguridad de la Información

5.1. El Procesador mantendrá los Datos Personales en estricta confidencialidad. El Procesador se asegurará de que sus empleados conozcan los requisitos aplicables de privacidad y seguridad de la información, y estarán sujetos a obligaciones de confidencialidad legalmente vinculantes.

5.2. El Procesador implementará las medidas operativas, técnicas y organizativas apropiadas para proteger los Datos Personales contra su destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilegal descrito en el Apéndice 2.

5.3. El Procesador actualizará las medidas de seguridad técnicas y organizativas de acuerdo con los adelantos tecnológicos razonables según lo determine el Procesador y proporcionará documentación actualizada al Controlador una vez solicitada bajo la forma de su certificación ISO 27001 actual.

6. Obligaciones de Cooperación y Notificación

6.1. Las Partes cooperarán entre sí para manejar de manera rápida y eficaz las consultas, quejas y reclamos relacionados con el Procesamiento de Datos Personales de cualquier autoridad gubernamental o Sujeto de Datos. Si un Sujeto de Datos solicita directamente ejercer sus derechos de datos personales al Procesador, el Procesador deberá enviar dicha solicitud al Controlador sin demora injustificada. El Procesador notificará al Controlador de inmediato si los Datos Personales pasen a estar sujetos a un control o investigación por parte de las autoridades públicas y no divulgará ningún Dato personal sin el consentimiento previo del Controlador. El Procesador proporcionará a las autoridades públicas, previa solicitud, información sobre el Procesamiento conforme al presente Anexo y permitirá inspecciones dentro del alcance establecido en la presente Sección 7.

6.2. El Procesador notificará, sin demora injustificada, al Controlador sobre cualquier Incidente de Seguridad de la información que pueda afectar los Datos Personales del Controlador. El Procesador proporcionará al Controlador la información para ayudar y asistir razonablemente al Controlador según lo exigido por las Reglas de Protección de Datos.

7. Derechos de Auditoría e Inspección del Controlador

A solicitud del Controlador, el Procesador deberá poner a disposición del Controlador la información necesaria para demostrar el cumplimiento del Controlador con las obligaciones estipuladas en el Anexo y en las Reglas de Protección de Datos, y permitir y contribuir con las auditorías, incluidas las inspecciones realizadas por el Controlador o un auditor externo independiente solicitado por el Controlador con el propósito de verificar el cumplimiento del presente Anexo por parte del Procesador, siempre y cuando las personas que realizan dicha auditoría firmen un acuerdo de confidencialidad con el Procesador. Todas las inspecciones se llevarán a cabo durante las horas normales de trabajo y sin interferir con el curso de las actividades de negocios del Procesador.

8. Uso de Subcontratistas

8.1 El Controlador reconoce y acepta que el Procesador podrá usar Subcontratistas para Procesar Datos Personales. El Procesador pondrá a disposición del Controlador su lista actual de Subcontratistas cuando se le solicite. A cualquier Subcontratista se le permitirá Procesar Datos Personales solo con el fin de entregar los Servicios que el Procesador les ha encargado proporcionar y estará regido contractualmente por obligaciones contractuales no menos protectoras que el presente Anexo. El Procesador será responsable de los actos y omisiones de cualquier Subcontratista de la misma forma que si los actos u omisiones fueran cometidos por el mismo Procesador. El Procesador mantendrá al Controlador informado de cualquier cambio en el Procesamiento de parte de los subcontratistas y le proporcionará una copia de este acuerdo de subcontratación cuando se le solicite.

8.2 Si el Procesador tiene la intención de nombrar o reemplazar a un Subcontratista incluido en el presente Anexo, el Procesador informará al Controlador de esta circunstancia y le dará la oportunidad de objetar razonablemente dichos cambios. El Proveedor proporcionará al Controlador toda la información que el Controlador pueda solicitar razonablemente para evaluar si el nombramiento del Subcontratista propuesto cumple con las obligaciones del Controlador según el presente Anexo y las Reglas de Protección de Datos correspondientes.

9. Devolución y Eliminación de Datos Personales

El Procesador devolverá o destruirá todos los Datos Personales y copias de los mismos a solicitud del Controlador o al momento de poner término del presente Anexo. El Procesador certificará el cumplimiento a solicitud del Controlador.

10. Responsabilidad e Indemnización

10.1 La Responsabilidad y las limitaciones de las Partes estarán regidas por el Acuerdo.

10.2 El Controlador indemnizará al Procesador por todos los reclamos de cualquier tercero con respecto al procesamiento de los datos personales proporcionados al Procesador si el procesamiento de dichos datos no está autorizado por las Reglas de protección de datos.

Controlador:	**Procesador:**
Por : _____	Por : _____
Nombre / Título : _____	Nombre / Título : _____
Fecha : _____	Fecha : _____

Apéndice 1: Datos Personales Procesados y Propósitos

Los Datos Personales se transfieren y procesan para los **siguientes fines**:

- Repositorios seguros en línea e intercambio de datos para la debida diligencia corporativa, transacciones relacionadas o propósitos internos de negocios.

Alcance del Procesamiento:

- Como se describe en el Enunciado de Trabajo, el Procesador proporcionará una sala virtual de datos, un repositorio seguro en línea para almacenar, administrar, colaborar y distribuir datos y documentos.

Categorías de Datos Personales:

- Nombres, dirección, dirección de correo electrónico de la empresa, número de teléfono de la empresa, números de identificación nacionales, compensación y beneficios, información sobre vacaciones y pensiones, títulos y funciones de trabajo y, posiblemente, todos los demás tipos de datos personales incluidos en la información de negocios cargada por el Administrador del Controlador en la sala virtual de datos.

Categorías Especiales de Datos (si corresponde):

Los Datos personales se refieren a las siguientes Categorías Especiales de Datos (especifique):

- Ninguna, a menos que el Controlador identifique lo contrario

Sujetos de Datos:

Los Datos Personales se refieren a las siguientes categorías de Sujetos de Datos:

- Información de negocios que puede incluir datos de propietarios, empleados, clientes, contratistas y proveedores.

Apéndice 2: Medidas de Seguridad de la Información

El Apéndice 2 incluye:

Sección I: Plan General de Seguridad de Datos del Procesador
Sección II: Procedimiento/Proceso de Seguridad de la Información del Procesador

I. Plan General de Seguridad de Datos

El Procesador se compromete a instituir y mantener las siguientes medidas de protección de datos:

	Requisito de Seguridad	Cómo implementa el procesador la medida específica de seguridad de la información
	Describa las medidas de control de acceso (físicas) en su empresa para impedir el acceso de personas no autorizadas a los sistemas de Procesamiento dentro de los cuales se Procesan o utilizan los Datos Personales (si su empresa tiene varias filiales o sucursales, distinga las diferencias entre las ubicaciones).	Todos los centros de datos poseen las certificaciones ISO 27001: 2013 y SOC 2 Tipo 2. Además, los centros de datos están certificados bajo los Marcos del Escudo de Privacidad. Existe un perímetro de múltiples controles de seguridad para todos los centros de datos que incluyen múltiples métodos de autenticación para obtener acceso.
2.	Describa las medidas de control de admisión tomadas en su empresa para evitar que los sistemas de procesamiento se utilicen sin autorización.	Los usuarios autorizados se basan en los requisitos de negocios y requieren la identificación y aprobación de los roles de administración. Se han implementado y se pueden rastrear características de tiempo de espera, requisitos seguros de autenticación y derechos de acceso.
3.	Describa las medidas de control de acceso (virtuales) tomadas en su empresa para garantizar que las personas con derecho a usar un sistema de procesamiento tengan acceso solo a los datos personales a los que tienen derecho de acceso, y que los datos personales no se puedan leer, copiar, modificar o eliminar sin autorización en el curso del procesamiento o uso, y después del almacenamiento.	El acceso de usuarios autorizados se gestiona a través de un procedimiento formal de registro y cancelación de registro para otorgar y revocar el acceso a todos los sistemas y servicios según la función de trabajo. Los informes de auditoría permiten el monitoreo preciso de la actividad del usuario y existen controles de acceso para proteger la integridad y la confidencialidad de los datos.
4.	Describa las medidas de control de transmisión tomadas en su empresa para garantizar que los Datos personales no se puedan leer, copiar, modificar o eliminar sin autorización durante la transmisión o el transporte electrónico, y que es posible verificar y establecer para qué organismos está prevista la transferencia de Datos Personales por medio de las instalaciones de transmisión de datos.	El Procesador tiene una política de medios extraíbles con los controles técnicos adecuados para proteger la integridad y la confidencialidad de los datos y prohibir la transferencia no autorizada de Datos Personales. El acceso remoto se controla mediante la autenticación multifactor. Los datos se cifran en reposo y en tránsito utilizando tecnologías de cifrado aprobadas por el gobierno.

5.	Describa las medidas de control de ingreso de datos para garantizar que sea posible verificar y establecer si los Datos Personales han sido ingresados en los sistemas de procesamiento, modificados o eliminados.	El Procesador tiene independencia respecto de los datos que el cliente elige cargar. Todas las acciones del usuario con respecto a la integridad y la confidencialidad de los datos son rastreadas y se pueden informar. El Controlador puede determinar a su entera discreción qué datos se proporcionan al Procesador.
6.	Describa las medidas de control de asignación en su empresa para garantizar que, en el caso de solicitudes de Procesamiento, los Datos Personales se procesen estrictamente de acuerdo con las instrucciones.	Se llevan a cabo auditorías anuales como parte de la Certificación ISO 27001 y el Informe SOC 2 Tipo 2 para garantizar que se cumplan los requisitos de cumplimiento. Los usuarios autorizados realizan una Capacitación y reconocen el cumplimiento del código de conducta y las políticas de la empresa anualmente. Se exige que todos los empleados y contratistas firmen un
7.	Describa las medidas de control de disponibilidad que su empresa toma para garantizar que los Datos personales estén protegidos contra su destrucción o pérdida accidental.	El Procesador posee redundancia en cada plataforma y mantiene registros de la disponibilidad del sistema. Además, la redundancia permite copias de seguridad continuas del sistema. El Procesador cuenta con Planes de Recuperación ante Desastres y Continuidad del Negocio que se revisan,
8.	Describa las medidas de control de separación que su empresa ha tomado para garantizar que los Datos Personales recopilados para diferentes propósitos puedan procesarse por separado.	La separación lógica se mantiene dentro de la misma base de datos multiinquilino. Los usuarios autorizados están restringidos al proyecto para el que están autenticados. El Procesador mantiene una aplicación de 3 niveles con separación de datos; desarrollo, prueba y producción.

II. Procedimiento/proceso de seguridad de la información del Procesador

El procesador implementa y sigue los siguientes estándares, procesos y procedimientos:

Datasite opera un Sistema de Gestión de Seguridad de la Información que cumple con los requisitos de ISO/IEC 27001: 2013 para el siguiente alcance: La gestión de la seguridad de la información se aplica a los procesos para la protección de la información de los clientes con respecto a los servicios globales de transacciones financieras y elaboración de informes, marketing y comunicaciones para industrias reguladoras, y contenido y colaboraciones de clientes.