CAU-2 /CNP CAUTION /01.01/ CIS DATA SOLUTIONS

A)143

lis data solutions

CNP assurances

LS-041021-228A
Ampliación
Data Store

30/06/2022

Objetivos del proyecto

Ampliación CNP Data Store

lis data solutions

Objetivos

- **Finalizar el proyecto Data Store** (proceso de validación, generación de outputs, inclusión de nuevas fuentes, generación de dashboards, etc)
- **Aportar flexibilidad** en las necesidades de un proyecto que está "vivo"
- **Gestionar mediante metodología ágil** poniendo el foco en el aporte de valor incremental de resultados y seguimiento continuo de tareas/dedicación

Motivación del proyecto

Dentro del **proyecto desarrollo de Data Store** de **CNP** se ha puesto de manifiesto que es necesario adaptar los alcances en función de las necesidades y cambios que van surgiendo a medida que se avanza y evoluciona.

Descripción y objetivos

Tabla de objetivos

OBJETIVO	SOLUCIÓN
Mantener un **control** del estado, dedicaciones estimadas y finalmente realizadas por cada tarea.	**Reuniones de seguimiento** de proyecto que permitan la evaluación del estado del proyecto, la evaluación del alcance con respecto al remanente de horas disponibles, así como la detección y escalado de eventuales riesgos.
Realizar la fase final de validación del **proyecto Data Store**	Proceso de pruebas y validación, generación de outputs, inclusión de nuevas fuentes, generación de dashboards, accesos, permisos, estandarización de imputs y tablas de mantenimiento...
Dotar al proyecto de la **flexibilidad** necesaria para adaptar los alcances, cambiar la prioridades de tareas, añadir o quitar desarrollos a medida que avanza el proyecto.	**CNP** será el encargado de decidir el "qué desarrollar". Gestionar el trabajo redundante y su productividad, definiendo la relación de objetivos a cumplir.
Asegurar una **disponibilidad** de horas a largo plazo y reducir el coste por volumen contratado.	**Contratación de 500 horas** colaboración **Data Engineer/Analyst** con una **validez de 14 meses** (Disponibilidad media mensual de 40h adaptable según planificación a un mes vista)

06| Condiciones Económicas

Resumen del servicio

LS-041021-228A

lis data solutions

Objetivo
Ampliación Proyecto Data Store CNP Assurances, S.A. Sucursal en España y CNP Caution, Sucursal en España

CONCEPTO	TARIFA ESTÁNDAR	TARIFA LONG TERM	DURACIÓN	DEDICACIÓN	TOTAL
Data Engineer/Analyst	550,00€ /JL	480,00€ /JL	14 meses	500h	30.000,00€

Tiempo de ejecución
500 horas. Periodo de validez de 14 meses (del 1 de Junio 2022 al 31 Julio de 2023)

Valoración económica
30.000,00€

Valoración Económica

Plan de Facturación de la oferta LS-041021-228A

HITO	FECHA FACTURA	PORCENTAJE	TOTAL
1	Fecha Firma Oferta	100%	30.000,00€

- 500 horas. Periodo de validez de 14 meses (del 1 de Junio 2022 al 31 Julio de 2023)
- CNP Assurances, S.A. Surcursal en España y CNP Caution Sucursal en España y LIS Data Solutions planificarán la actividad procurando que la dedicación mensual del equipo sea de 40 horas mensuales.
- Los excesos de dedicación mensual deberán ser acordados entre ambas partes.
- Los tiempos de intervención en las tareas se contabilizan en minutos, e incluirán toda la dedicación que se dedique a las tareas por parte de LIS Data Solutions (reuniones y su preparación, análisis, investigaciones, trabajo de desarrollo, etc.) El plazo de inicio y entrega de cada tarea desde su solicitud formal será convenido por ambas Partes en reuniones periódicas de seguimiento.
- Las presente ampliación tiene una vigencia de 14 meses, caducando dicho plazo el efecto será la pérdida de las horas que estén pendientes de disfrutar, sin derecho a reclamar el importe abonado por ellas.
- No incluye costes de infraestructura, licencias, mantenimientos y soporte.
- Esta oferta tendrá validez durante 30 días.
- El importe de las facturas será pagadero a 30 días desde la fecha de emisión de la factura, por transferencia bancaria.
- Al precio final hay que añadirle el 21% de IVA.
- Dicho pago se realiza teniendo en cuenta que el noventa por ciento (90%) del Precio será abonado por CNP CAUTION, mientras que CNP ASSURANCES abonará el diez por ciento (10%) del Precio restante. Asimismo, Lis Data enviará una factura a cada empresa y ambas facturas serán remitirás al siguiente correo electrónico: facturas@cnp.es
- La firma de esta oferta supone la aceptación de las condiciones de los servicios de LIS Data Solutions.

Manuel Coterillo – CEO LIS Data Solutions

David Lattes – CNP ASSURANCES, S.A.,

Sucursal en España Y CNP CAUTION, Sucursal en España

Firmado por ***8441** MANUEL COTERILLO (R: ****0793*) el día 01/07/2022 con un certificado emitido por AC Representación

Condiciones de Contratación

lis data solutions

1. OBJETO

Estas cláusulas constituyen el marco básico de regulación de las relaciones establecidas entre las Partes y forman parte del contrato (el "Contrato" o Proyecto) que regula los términos bajo los cuales LIS DATA SOLUTIONS, S.L. sociedad de nacionalidad española, con domicilio en Vitoria, C/ Pintor J. Ángel Sáez Nº16, y con número de identificación fiscal (CIF) B01507938 ("LIS Data Solutions") proporcionará a a CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA con número de identificación fiscal W0013620J y CNP CAUTION, SUCURSAL EN ESPAÑA con número de identificación fiscal W0010754J (en adelante ambas entidades, "el Cliente") los servicios previstos en la oferta presentada (la "Propuesta").

Las presentes cláusulas serán aplicables a todos los Contratos celebrados entre LIS Data Solutions y el Cliente referentes al Proyecto recogido en esta Propuesta, excepto en aquellos casos en los que sean expresamente derogadas o modificadas.

El Cliente reconoce que la aceptación de las estas condiciones implica su aplicación a la contratación al Proyecto al que se refiere la Propuesta. El hecho de no recurrir en un momento dado, por parte de LIS Data Solutions, a cualquiera de las condiciones, no puede ser interpretado ni equivalente a renunciar a recurrir a ellas en el futuro.

2. CARACTERÍSTICAS DE LOS SERVICIOS

LIS Data Solutions es una sociedad independiente que dispone de los recursos técnicos, materiales y humanos adecuados y suficientes para la ejecución de las actividades previstas, así como para ofrecer y garantizar la consecución, buen fin y resultado de las mismas.

El Cliente contrata la realización del Proyecto de acuerdo con lo establecido en la Propuesta, que ha sido facilitada por LIS Data Solutions y que pueden sufrir variaciones durante el avance del Proyecto, previa aprobación por el CLIENTE. Las tarifas no incluyen el IVA ni cualquier otro impuesto sobre las ventas, o cualquier coste o gasto incidental.

No se considerarán incluidos, salvo que se indique en la Propuesta, los siguientes productos o servicios:

- Licencias de uso de software de terceros.
- Modificaciones sobre software de terceros.
- Hardware necesario, ni su instalación ni mantenimiento.
- Sistemas operativos, ni su instalación ni mantenimiento.

3. VALIDEZ DE LA OFERTA, DURACIÓN Y CANCELACIÓN ANTICIPADA DEL CONTRATO

3.1. Validez de la oferta

El periodo de validez de la Propuesta será el reflejado en la Valoración Económica. En caso de no indicarse, la validez de la misma se entenderá de treinta (30) días naturales. Transcurrido el plazo de validez sin que sea aceptada por parte del Cliente se entenderá caducada, salvo que por acuerdo entre las Partes se decida prorrogar la duración de la misma.

Si el Cliente rechaza el Proyecto una vez la Propuesta ha sido aceptada, estará obligado a asumir el pago de los servicios prestados hasta el momento. Si Lis Data rechaza El Proyecto una vez ha sido aceptada por el Cliente, estará obligado a asumir los costes de los servicios prestados hasta el momento.

3.2. Duración del contrato

El Contrato que vincula a ambas Partes entrará en vigor el día de la firma de la Propuesta 1 de Junio del 2022, y expirará automáticamente el 31 de Julio con la entrega definitiva del Proyecto.

En el caso en que LIS Data decidiera cancelar el Proyecto unilateralmente, deberá notificarlo por escrito al Cliente con una antelación de dos (2) meses y teniendo en cuenta las siguientes consideraciones.

- Lis Data se hará cargo de todos los costes asociados a dicha cancelación.
- Lis Data terminará los servicios que en el momento de la cancelación ya fueran aprobados por ambas partes.
- Lis Data tendrá que entregar todos los materiales, sistemas, BBDD y/o cualquier soporte que pertenezca a el Cliente y que haya sido proporcionado a LIS Data para la ejecución del presente Proyecto teniendo en cuenta las instrucciones establecidas en el anexo 2, apéndice 1 del mismo.

4. RÉGIMEN DE EJECUCIÓN

El desarrollo del Proyecto atenderá a lo establecido en la Propuesta y a lo que se fije definitivamente en el Documento Técnico Funcional, salvo en aquellos supuestos en los que el Proyecto consista en una bolsa de horas.

Atendiendo al hecho de que los datos que proporcione el Cliente y su calidad condicionarán en gran medida los resultados del Proyecto, LIS Data Solutions no garantiza en el momento de aceptación de la presente Propuesta un resultado concreto, comprometiéndose a la prestación del trabajo en si mismo, con la mayor diligencia y responsabilidad debidas para lograr los objetivos previstos.

Ambas Partes entienden que las tecnologías y tiempos de desarrollo previstos en la presente Propuesta son previsiones y estimaciones que pueden variar durante el avance del Proyecto, en función de los sistemas y necesidades del Cliente y del propio Proyecto.

4.1. Compromisos

La ejecución del Proyecto será dirigida y gestionada exclusivamente por LIS Data Solutions, quien se compromete a poner a disposición del Cliente recursos (medios y disposición material y humana) así como las buenas prácticas, diligencia y responsabilidad necesarias.

Debido a lo anterior, el equipo multidisciplinar presentado en la Propuesta no tiene carácter vinculante, pudiendo LIS Data Solutions sustituirlo, en todo o en parte, , que en caso de baja de alguno de los empleados de LIS Data, este se compromete a reemplazarlo en el plazo máximo de dos (2) días laborables por otros consultores capacitados para la correcta ejecución del Proyecto, no suponiendo tal modificación un incumplimiento del Contrato.

El Cliente deberá colaborar activamente con LIS Data Solutions, comprometiéndose a facilitarle acceso a toda la información, documentos, sistemas e instalaciones que se precisen para la ejecución del Proyecto atendiendo en todo momento a las medidas de seguridad y organizativas incluidas en el anexo 2, apéndice 1 del presente acuerdo.. Los retrasos o paralizaciones que ocasione la falta de colaboración del Cliente serán de su exclusiva responsabilidad.

El Cliente acepta que el desarrollo del Proyecto supone una planificación por parte de LIS Data Solutions y la reserva de los recursos personales y materiales de que dispone para la ejecución del Proyecto. Con su firma, el Cliente se compromete a ejecutar el Proyecto sin dilaciones ni paralizaciones por su parte, salvo pacto por escrito entre ambas Partes.

4.2. Alcance del Proyecto

El alcance final del Proyecto quedará limitado a las jornadas laborales previstas en la Propuesta y a los trabajos concretos a realizar, durante ellas, que se establezcan en la propia Propuesta, que será elaborado tras analizar junto al Cliente los requisitos deseables para el Proyecto y que se deberá incorporar en anexo al presente Proyecto.

4.3. Bolsas de Horas

El presente Proyecto se constituye en su totalidad en la modalidad de una "Bolsa de Horas", que permite al Cliente adquirir horas de dedicación de recursos de LIS Data Solutions para llevar acabo las tareas de consultoría y desarrollo que se definan hasta agotar las horas adquiridas, con independencia de que las tareas estén o no terminadas. Si se agotan las horas disponibles, el Cliente siempre puede recargar su bolsa con la adquisición de otra bolsa previo consentimiento del Cliente

LIS Data comunicará al Cliente un día de antes de la reunión semanal entre el Cliente y LIS Data las horas consumidas de la "Bolsa de Horas" establecidas en el presente Proyecto.

Los tiempos de intervención en las tareas se contabilizan en minutos, e incluirán toda la dedicación que se dedique a las tareas por parte de LIS Data Solutions (reuniones y su preparación, análisis, investigaciones, trabajo de desarrollo, etc.) El plazo para iniciar la tarea desde su solicitud formal por el Cliente será convenido por ambas Partes.

5. ENTREGA

LIS Data Solutions desarrollará el Proyecto cumpliendo con las funcionalidades que se describen en la Propuesta y con las especificaciones que se fijarán definitivamente, en su caso, en el Documento Técnico Funcional, comprometiéndose a permitir que el Cliente realice las pruebas oportunas respecto de los prototipos entregados e indique las contingencias identificadas de cara a su subsanación por LIS Data Solutions, y a entregar el Proyecto en perfecto estado de funcionamiento.

Condiciones de Contratación

5.1. Test Final
El Cliente dispondrá del plazo de (15) quince días hábiles, desde la entrega de los desarrollos para realizar las pruebas que estime oportunas (en adelante, el "Test Final"). Las pruebas, test o validaciones que se realicen, así como la conformidad o no de los resultados entregados, se determinarán en función de su adecuación con las funcionalidades y especificaciones previstas en esta Propuesta y en el Documento Técnico Funcional.

Durante el Test Final, el Cliente deberá comunicar a LIS Data Solutions, a la mayor brevedad, los posibles errores o fallos que identifique en el Proyecto. Si transcurridos los quince días el Cliente no comunica posibles errores, se entenderá finalizado el Test Final y que el Proyecto le satisface completamente.

En el caso de que algún error sea comunicado, LIS Data Solutions estudiará la incidencia y la subsanará si procede, informando al Cliente en el momento en el que el Proyecto se encuentre corregido. A partir de dicho momento, el Cliente dispondrá de un nuevo plazo de (10) diez días hábiles para realizar las pruebas que estime necesarias. Transcurrido dicho plazo sin que el Cliente haya comunicado, vía correo electrónico o vía herramienta ticketing o cualquier otro medio que permita dejar constancia de la recepción por parte de Lis Data, posibles errores o fallos que persistan en el Proyecto, se entenderá finalizado el Test Final y que el Proyecto realizado satisface completamente al Cliente.

5.2. Soporte al Cliente
En caso de contratarse, la finalidad de este servicio es resolver pequeñas dudas del usuario o notificar incidencias. El soporte al Cliente se prestará mediante:

- Soporte telefónico, mediante llamada al número de teléfono que se facilite al Cliente.
- Soporte a través de plataformas de videoconferencia (Microsoft Teams, Skype o análogos).
- En caso de ser necesario, conexión remota al sistema del Cliente

Los tiempos de respuesta, días hábiles y horarios para la atención al Cliente se definirán en la Propuesta. En su defecto, LIS Data Solutions prestará el Servicio dentro de las horas hábiles de trabajo y según el calendario laboral oficial: Lunes a Jueves De 08:30 a 14:00 y de 15:30 a 18:00 h. / Viernes: De 08:00 a 14:30, con un tiempo de respuesta inferior a 48 horas.

En ningún caso, habrá gastos por desplazamiento.

6. PRECIO, FACTURACIÓN Y PAGO DE LOS SERVICIOS
6.1. Precio
El Cliente pagará a LIS Data Solutions el precio del Proyecto contratado. Salvo que se indique lo contrario, los precios no incluyen IVA.

No se admitirán revisiones de precios o aumentos de servicios sobre los indicados en la Propuesta, salvo que se autoricen en documento firmado por ambas Partes.

6.2. Facturación y pago de los servicios
LIS Data Solutions procederá a la facturación del importe conforme a lo establecido en la Propuesta y en las presentes Condiciones Generales.

El pago de las facturas emitidas por LIS Data Solutions deberá hacerse efectivo dentro de los treinta (30) días naturales siguientes a su recepción, salvo que se acuerde otro plazo. Dicho pago se realiza teniendo en cuenta que el noventa por ciento (90%) del Precio será abonado por CNP CAUTION, mientras que CNP ASSURANCES abonará el diez por ciento (10%) del Precio restante. Asimismo, Lis Data enviará una factura a cada empresa y ambas facturas serán remitirás al siguiente correo electrónico: facturas@cnp.es

Si alguna factura no fuera abonada en el plazo establecido, LIS Data Solutions tendrá derecho a suspender todo el desarrollo del Proyecto o la prestación de cualquier servicio, con previa notificación al Cliente, siendo de exclusiva responsabilidad del Cliente los daños y perjuicios que por dicha suspensión pudieran producirse.

7. DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL
El Proyecto a realizar está sujeto a derechos de propiedad intelectual e industrial de LIS Data Solutions y/o de terceros. En este último caso, LIS Data manifiesta expresamente que cuenta con las licencias necesarias para hacer uso de los derechos de propiedad intelectual e industrial de tercero, exonerando expresamente al Cliente de cualquier responsabilidad que por su mal uso LIS Data pudiera incurrir. En ningún caso la realización del Proyecto por LIS Data Solutions implica ningún tipo de renuncia, transmisión o cesión total ni parcial de tales derechos.

7.1. Derechos de propiedad intelectual de LIS Data Solutions
Los desarrollos informáticos y algoritmos incluidos en el Proyecto pueden ser realizados parcialmente o totalmente sobre un núcleo de programación preexistente propiedad de LIS Data Solutions, que es objeto de reutilización y personalización en función de las necesidades de este y otros proyectos y/o clientes, y cuyo uso se licencia al Cliente.

A salvo lo anterior, LIS Data Solutions concede a favor del Cliente una licencia de uso no exclusiva, por tiempo indefinido, de la propiedad intelectual que se desarrolle para el Proyecto, sin que se autorice la explotación, ingeniería inversa, comercialización, cesión o publicación de todo o parte de la misma sin la previa, escrita y expresa autorización, otorgada a tal efecto por LIS Data Solutions.

7.2. Derechos de propiedad intelectual de terceros
El Cliente será el titular de las licencias de uso de los derechos de propiedad intelectual de terceros necesarias para el correcto funcionamiento del Proyecto. Correrá de su cuenta el pago de las mismas, y será el único responsable frente al tercero titular de los derechos afectados en cualquier reclamación que éste pudiera ejercitar derivada de una violación de la licencia de uso o sus derechos de propiedad intelectual.
8.3 Derechos de propiedad intelectual del Cliente
El Cliente será titular en exclusiva de todos los derechos de explotación derivados de la Propiedad Intelectual del programa de ordenador o parte del programa que resulte de desarrollos específicos que puedan ser objeto de la prestación de los servicios contratados, a cuyo efecto LIS Data cede a favor del Cliente su uso, y no pudiendo no pueden reutilizarse por parte de LIS Data en otros clientes salvo consentimiento previo, expreso y por escrito del Cliente.
LIS Data garantiza que los trabajos y servicios prestados al Cliente en la ejecución de este Proyecto no infringen derechos de Propiedad Intelectual o Industrial o cualesquiera otros derechos de terceros, haciéndose LIS Data, en todo caso, plena e individualmente responsable de toda clase de reclamaciones y/o indemnizaciones por razón de este concepto frente a todo tipo de terceros.

En ambos casos, se deberá cesar inmediatamente en el uso de los signos distintivos de la otra Parte.

Condiciones de Contratación

lis data solutions

8. **CONFIDENCIALIDAD, SECRETO EMPRESARIAL Y PROTECCIÓN DE DATOS**

8.1. Confidencialidad y Secreto Empresarial

Las Partes se comprometen a mantener en estricta confidencialidad toda información (escrita o verbal) transmitida, que puedan obtener como consecuencia del Proyecto. Tendrán también consideración de secreto empresarial los algoritmos empleados por LIS Data Solutions para el desarrollo del Proyecto, los cuales tienen un alto valor empresarial y no son generalmente conocidos ni fácilmente accesibles.

8.2. Protección de Datos Personales

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la normativa nacional sobre protección de datos aplicable (incluyendo las disposiciones específicas sobre protección de datos incluida en la normativa del sector seguros de aplicación en cada momento) y/o cualquier otra legislación que las modifique o sustituya en un futuro, será de obligado cumplimiento para cada una de las partes.

LIS Data tendrá la condición de Encargado del Tratamiento del Cliente de los datos de carácter personal y estará obligado a cumplir las condiciones estipuladas en el Anexo 2 al presente Proyecto.

9. **COMPROMISOS Y RESPONSABILIDAD**

LIS Data Solutions garantiza que los trabajos serán realizados por profesionales con cualificación y experiencia suficientes, y que los desarrollos objeto del Proyecto son fruto de su autoría o, que en todo caso, cuenta con los derechos suficientes para su utilización en el marco de este Proyecto.

El Cliente se compromete a utilizar el Proyecto conforme a las necesidades y finalidades previstas, excluyéndose expresamente cualesquiera otras aplicaciones, fines, usos, modificaciones o resultados no indicados, no resultando LIS Data Solutions responsable por ningún concepto que pudiera derivarse en caso de incumplimiento de tales exclusiones.

De igual manera, el Cliente acepta y reconoce que nunca podrá garantizarse el funcionamiento impecable de una configuración de hardware-software, ya sea debido a factores externos (fallo de alimentación o interrupción de corriente, tormentas eléctricas, etc.) o debido a factores específicos de la configuración del conjunto (defectos, fallos de red, fallos ocultos en el sistema y/o software empleados, etc.) y, en consecuencia, existe el riesgo de la pérdida inesperada de, entre otras cosas, (incluso todos) los software y/o datos. El Cliente asume que dichos elementos y consecuencias quedan fuera de la responsabilidad de LIS Data Solutions y se compromete a instalar los mecanismos adecuados para la seguridad, el almacenamiento y la restauración de los datos.
En consecuencia, LIS Data Solutions responderá de los daños directos o indirectos atribuibles a la misma en relación con el Proyecto.

9.1 Proyectos que incluyen elementos de Inteligencia Artificial

Las sugerencias, planificaciones o predicciones que ofrecen los proyectos que cuentan con elementos de Inteligencia Artificial surgen del análisis, mediante algoritmos, de los datos facilitados por el Cliente. En todo caso, la información resultante de la Inteligencia Artificial debe ser utilizada para ayudar a las personas a la toma de decisiones, no debiendo ser empleadas, en ningún caso, para sustituir el criterio humano.

El Cliente se compromete a contar con supervisión humana que valore y cuestione el funcionamiento del Proyecto, las sugerencias y resultados ofrecidos, así como el uso que debe hacerse de las sugerencias y predicciones en función de las circunstancias concretas. Así mismo, el Cliente se compromete a notificar a LIS Data Solutions, a la mayor brevedad posible, cualquier comportamiento fuera de lo esperado por parte del Proyecto.

Los conjuntos de datos, procesos y algoritmos integrados en el sistema de Inteligencia Artificial, así como las acciones o decisiones que contribuyen a un determinado resultado, podrán ser consultadas en la documentación del Proyecto.

9.2 Proyectos que incluyen conexión de sensores y otros hardware de captura de datos

Los servicios de LIS Data Solutions no incluyen el montaje del hardware de captura de datos, ni la manipulación, reparación o modificación de instalaciones o bienes del Cliente a los que deba conectarse el hardware, limitándose el trabajo de LIS Data Solutions a la correcta conexión del hardware a los bienes del Cliente mediante conectores.

El Cliente se compromete a facilitar a LIS Data Solutions cualquier información necesaria para la correcta conexión del hardware, especialmente en lo relativo a componentes autorizados por el fabricante de los bienes donde deban instalarse.

En todo caso, el Cliente garantiza a LIS Data Solutions que está autorizado por el fabricante de los bienes a conectar hardware de captura de datos, exonerando a LIS Data Solutions de los perjuicios o responsabilidades que pudieran derivarse como consecuencia de la falta de autorización, así como de cualquier otra responsabilidad derivada de la conexión de los mismos, salvo en aquellos casos en que exista dolo o culpa grave por parte de LIS Data Solutions.

Como regla general, será el Cliente quien adquiera el hardware. En el supuesto en que el Cliente encargue a LIS Data Solutions la compra del hardware, el Cliente exonera expresamente a LIS Data Solutions del saneamiento por vicios ocultos en los productos adquiridos, y asume la obligación de reclamar directamente al fabricante o proveedor del hardware.

9.3 Fuerza Mayor

Ninguna de las Partes será responsable del incumplimiento de sus obligaciones cuando sea debido a causas de Fuerza Mayor. En cualquier caso, para que pueda ser aplicable una fuerza mayor, la Parte afectada deberá comunicar por escrito a la otra la ocurrencia del suceso a la mayor brevedad posible y en todo caso con un máximo de 48 horas desde que se iniciara. Mientras dure la situación de Fuerza Mayor, la parte que declaré su concurrencia adoptará las medidas necesarias para minorar sus efectos.

10. **EXTINCIÓN DEL CONTRATO**

El Proyecto se extinguirá por las causas generales de extinción de los contratos.

Las Partes podrán interrumpir la realización del Proyecto y/o resolver el Proyecto en los supuestos previstos en estas condiciones y, en especial, por incumplimiento grave del de las obligaciones que se derivan de las mismas.

Se entenderá por incumplimiento grave, a título enunciativo:

- La declaración del concurso de acreedores de cualquiera de las Partes.
- El retraso reiterado en el pago de facturas.
- La no realización o la realización defectuosa de los servicios estipulados en el presente Proyecto por parte de LIS Data dará derecho al Cliente a resolver el Proyecto, pudiendo en su caso solicitar a LIS Data la pertinente indemnización por los daños y/o perjuicios ocasionados al Cliente por razón de su acción u omisión.
- Cualquier incumplimiento relativo a la Información Confidencial

Cuando tenga lugar el incumplimiento de las obligaciones previstas en el Proyecto, la Parte perjudicada que decida invocar la facultad de resolución que en los mismos se contempla, deberá comunicar su decisión a la Parte incumplidora, entendiéndose que el Proyecto queda resuelto en el plazo de siete (7) días naturales desde el envío de dicha comunicación, siempre que, en caso de que se pueda subsanar dicho incumplimiento, la Parte incumplidora no hubiese subsanado el incumplimiento dentro de ese plazo.

En cualquiera de los supuestos de resolución por incumplimiento, la Parte incumplidora estará obligada al pago de la indemnización a la Parte cumplidora de los daños y perjuicios sufridos.

Condiciones de Contratación

Sin perjuicio de lo dispuesto en las anteriores cláusulas, el Proyecto podrá extinguirse por mutuo acuerdo de las Partes, quedando ambas Partes libres de cualquier obligación aquí recogida.

11. SEGURO DE RESPONSABILIDAD CIVIL

LIS Data Solutions cuenta con un Seguro de Responsabilidad Civil Profesional que cubre las reclamaciones del Cliente y terceros cuyo origen sea la ejecución de las obligaciones que se deriven del Proyecto, por daños materiales o personales y sus perjuicios consecuenciales, con un límite máximo de indemnización de 1.500.000 euros por siniestro.

12. RELACIÓN ENTRE LAS PARTES

Ninguna de las Partes, ni sus empleados, podrán (i) actuar como representante, agente o mandatario de la otra, ni (ii) crear obligaciones a la otra parte frente a terceros. Asimismo, ni el perfeccionamiento ni el cumplimiento del Proyecto, podrán interpretarse como una relación laboral por las Partes aquí intervinientes.

El Cliente reconoce que el equipo humano de LIS Data Solutions tiene, por sus características, un alto valor, y en consecuencia se obliga a no contratar a ningún empleado de LIS Data Solutions durante el desarrollo del Proyecto ni hasta que haya transcurrido un año desde su finalización, debiendo indemnizar a LIS Data Solutions por los daños y perjuicios que ocasione el incumplimiento de la presente cláusula.

La naturaleza de este Proyecto es la propia de un arrendamiento de servicios de carácter exclusivamente mercantil. Por lo expuesto, no se deriva relación o vínculo laboral alguno entre las Partes, ni entre el Cliente y el personal o colaboradores de LIS Data que, eventualmente, pudieran estar prestando alguno de los servicios que constituyen el objeto del Proyecto.
En ningún caso los empleados de LIS Data se consideran personal del Cliente, no dependiendo ni funcional ni orgánicamente y no asumiendo el Cliente responsabilidad alguna en materia laboral respecto de los mismos.

LIS Data se obliga a cumplir y hacer cumplir con todo rigor a su personal las obligaciones impuestas por la legislación laboral, especialmente en materia de Seguridad Social y Prevención de riesgos laborales, lo que justificará en cualquier momento a petición del Cliente y deberá disponer de una persona encargada de la vigilancia y cumplimiento de tales obligaciones.
LIS Data deberá entregar al Cliente, si así se le solicita, y mantener actualizada la siguiente documentación:

- Certificación negativa por descubiertos en la Seguridad Social expedida por el Órgano competente de la Administración. Dicha certificación, acreditativa de estar al corriente en el pago de las cuotas, se entregará antes del inicio de los servicios y se actualizará trimestralmente. La eficacia y validez del Proyecto queda condicionada al cumplimiento de aportar inicialmente el mencionado certificado.
- Justificantes de pago de las cuotas de Seguridad Social, correspondientes a los trabajadores empleados en la realización de los trabajos objeto del Proyecto. Dichos documentos se aportarán antes del comienzo del servicio pactado.
- Certificación expedida por LIS Data cuando así lo soliciten el Cliente, acreditativa del abono de los salarios debidos a los trabajadores empleados en la realización de los trabajos objeto del Proyecto.
- En el caso de intervención de personal extranjero, las autorizaciones pertinentes para residir y trabajar en España.

El incumplimiento de cualquiera de las obligaciones especificadas facultará al Cliente para resolver el Proyecto siempre que, habiéndose concedido un plazo razonable de un (1) mes para la aportación de la documentación citada, LIS Data no la hubiera presentado.
Asimismo, para el supuesto de que por resolución judicial CNP ASSURANCES o CNP CAUTION fuera condenada a hacerse cargo de personal que hubiera pertenecido a la plantilla de LIS Data, LIS Data deberá pagar al Cliente una cantidad igual a la que el Cliente debiera pagar a ese personal en concepto de indemnización por despido improcedente.

La aceptación de la Propuesta y estas cláusulas sustituye todas las propuestas y acuerdos, escritos u orales, anteriores a la fecha de la Propuesta, que existieran entre las Partes con el mismo objeto. Las Partes renuncian expresamente a hacer valer otras condiciones generales. El Proyecto no es asignable, transmisible ni transferible, salvo por acuerdo por escrito entre ambas Partes.

13. PREVENCIÓN FRENTE AL FRAUDE, SOBORNO Y CORRUPCIÓN

CNP ASSURANCES y CNP CAUTION tienen tolerancia cero en lo que se refiere a prácticas de soborno y corrupción, así como mantienen un estricto control para prevenir el fraude por lo que cuentan con políticas cuyo objetivo es prevenir estas prácticas en el seno de ambas entidades y en cualquier relación con terceros. Se adjunta como Anexo 1 carta sobre los Principios Éticos que aplican a CNP ASSURANCES y CNP CAUTION y de los que LIS Data debe ser conocedor y respetar en sus relaciones con CNP ASSURANCES y CNP CAUTION.
Con base a lo anterior, LIS Data declara contar con políticas y procedimientos internos adecuados aplicables a sus empleados, así como a cualquier tercero que colaboren con ella, para prevenir y evitar la participación en actividades relacionadas con el fraude, la corrupción y el soborno y que serán de aplicación en el desarrollo del presente Proyecto.
Adicionalmente las Partes declaran que el Proyecto se celebra única y exclusivamente para desarrollar objetivos de negocio, y que en ningún caso atiende a intereses particulares de cualesquiera de las Partes o al propósito de obtener una ventaja indebida para una de las Partes, uno de sus empleados o directivos.
En concreto, LIS Data garantiza, en relación con el presente Proyecto, que no existirán ventajas financieras o de cualquier otro tipo que hayan sido acordadas o que lo puedan ser en el futuro con cualquier persona perteneciente a CNP ASSURANCES y CNP CAUTION.
El incumplimiento de cualquiera de las previsiones anteriores será considerado como un incumplimiento grave del Proyecto y dará derecho a CNP ASSURANCES y a CNP CAUTION a su terminación inmediata sin perjuicio de cualesquiera otras acciones legales que les puedan corresponder.

14. APLICACIÓN DE SANCIONES FINANCIERAS

CNP ASSURANCES y CNP CAUTION no realizarán pago de cantidad alguna que les pueda exponer o implique cualquier sanción, prohibición o aplicación de medidas restrictivas, en virtud de resoluciones de cualquier organismo internacional y, en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

CNP ASSURANCES y CNP CAUTION tendrán derecho a rescindir los acuerdos o contratos suscritos en el caso de que su contraparte adquiera la categoría de persona sancionada o se le aplique una medida restrictiva, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

15. CESIÓN Y SUBCONTRATACIÓN

Las Partes no podrán ceder el presente Contrato, sin el previo consentimiento por escrito de la otra.
LIS Data no podrá subcontratar a una tercera parte para la prestación de los servicios establecidos en el Contrato salvo que medie previo consentimiento y por escrito del Cliente.

En el caso de que LIS Data recurra a subcontratistas para llevar a cabo los servicios descritos en el presente contrato deberá obtener autorización previa y por escrito del Cliente. A tal efecto, LIS Data informará por escrito al CLIENTE con carácter previo de las subcontrataciones previstas facilitando los datos de los terceros a los que pretenda subcontratar.

Si el Cliente no manifestara por escrito su oposición a dicha subcontratación en el plazo de CINCO (5) días hábiles desde la recepción de la notificación correspondiente, se entenderá que no se oponen a la misma. Los mismos términos y obligaciones resultarán aplicables en el supuesto de que LIS Data tuviera intención de sustituir a alguno o algunos de sus subcontratistas.

16. LEGISLACIÓN Y RÉGIMEN JURÍDICO APLICABLE

La relación contractual establecida entre LIS Data Solutions y el Cliente se regirá en todo caso por la legislación española común aplicable en el momento de la ejecución del Proyecto. En caso de que algún juez o tribunal competente considere alguna cláusula o parte de ellas inválida o inaplicable, dicha invalidez o inaplicabilidad no afectará a la integridad del resto de la cláusula o del Proyecto.

Las Partes, con renuncia expresa a cualquier otro fuero que pudiera corresponderles, se someten al de los Juzgados y Tribunales de Madrid Capital para cualquier controversia que pudiera derivarse del presente Proyecto.

17. FIRMA Y PERFECCIÓN DEL PROYECTO - CONTRATO

Cualquier facsímil, documento firmado electrónicamente o copia firmada y digitalizada de esta Propuesta vinculará a las Partes de igual manera que un documento original.

Las Partes acuerdan que el presente Contrato podrá perfeccionarse mediante firma electrónica de la oferta, por lo ambas aceptan que la utilización de tales medios tendrá la misma validez que la utilización de una firma manuscrita.

Para garantizar la eficacia jurídica de este procedimiento, las Partes podrán designar a cualquier proveedor de servicios digitales certificado que proceda a certificar y a consignar la fecha y la hora en la firma ha tenido lugar.

lis data solutions

Get In Touch

info@lisdatasolutions.com

☎ +34 945 06 59 50

ANEXO 1

AL CONTRATO DE PRESTACIÓN DE SERVICIOS

(Principios Éticos Grupo CNP)

ENTRE

CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA Y CNP CAUTION, SUCURSAL EN ESPAÑA

Y

LIS DATA SOLUTIONS, S.L.

ANEXO 1 AL CONTRATO DE PRESTACIÓN DE SERVICIOS
(Principios Éticos Grupo CNP)

Por medio del presente Anexo se incluyen los principios éticos del Grupo CNP Assurances al que pertenecen CNP ASSURANCES, S.A., Sucursal en España y CNP CAUTION, Sucursal en España

insuring
a more
open world

ETICA DE NEGOCIOS
E. GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in CodEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

Y en prueba de recepción el suscribiente en el carácter con el que interviene, firma el presente anexo en Madrid a 29 de Junio de 2022

Por duplicado a un solo efecto.

LIS DATA SOLUTIONS, S.L.

lis data solutions
LIS SOLUTIONS S.L - B01507938
www.lisdatasolutions.com
Fdo.: Manuel Coterillo

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

(Protección de datos personales)

ENTRE

CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA Y CNP CAUTION, SUCURSAL EN ESPAÑA

E

LIS DATA SOLUTIONS S.L.

DC

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS DE DIGITALIZACIÓN DE CUSTODIA, CONSERVACIÓN, DIGITALIZACIÓN Y LOGÍSTICA DE FONDOS DOCUMENTALES

Por medio del presente Anexo se recogen las obligaciones de las partes en relación con la actual regulación de protección de datos de carácter personal así como la requerida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, "**RGPD**").

A los efectos de esta cláusula:

'**Responsable de tratamiento**' significa: **CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA Y CNP CAUTION, SURCURSALEN ESPAÑA (en adelante, el CLIENTE).**

'**Encargado de tratamiento**' significa: **LIS DATA SOLUCITONS, S.L. (en adelante, PROVEEDOR).**

1. Objeto del encargo del tratamiento

Por acuerdo de las Partes se habilita al encargado de tratamiento para tratar por cuenta del responsable del tratamiento, los datos de carácter personal necesarios para prestar los servicios recogidos en el Contrato. El tratamiento consistirá en:

☐ Recogida	☐ Registro
X Estructuración	☐ Modificación
☐ Conservación	☐ Extracción
X Consulta	☐ Comunicación por transmisión
☐ Difusión	X Interconexión
☐ Cotejo	☐ Limitación
☐ Supresión	☐ Destrucción
☐ Conservación	☐ Comunicación

☐ Otros: .....

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, EL CLIENTE, responsable del tratamiento, pone a disposición del PROVEEDOR, encargada del tratamiento, la información que se describe a continuación:

- Fecha de nacimiento
- Número de póliza
- Sexo
- IBAN

3. Duración

La duración del Encargo de tratamiento se vincula a la duración del Contrato suscrito entre el CLIENTE y el PROVEEDOR.

Una vez finalice dicho Contrato, el Encargado del tratamiento deberá devolver al Responsable o, si el responsable así lo solicita, entregar a otro encargado que designe el responsable, los datos personales y suprimir cualquier copia que esté en su poder.

4. Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

   Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión Europea o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

   1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos (éste último, en el caso de que sea obligatoria su designación de acuerdo a lo dispuesto en la normativa).

   2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

   3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49.1 párrafo segundo del RGPD, la documentación de garantías adecuadas. En todo caso, queda prohibido realizar una transferencia internacional de los datos propiedad del CLIENTE, a un tercer país que no cuente con unas garantías adecuadas.

4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

   i) La seudoanimización y el cifrado de datos personales.

   ii) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

   iii) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

   iv) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

   El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

   Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión Europea o de los Estados miembros que sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Subcontratación

   No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

   Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de treinta (30) días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista, localización, y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

   El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección: dpd@cnpspain.eu. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. Derecho de información

Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos

El encargado del tratamiento notificará al responsable del tratamiento inmediatamente, sin dilación indebida, y en cualquier caso antes del plazo máximo de doce (12) horas, y a través de dpd.es@cnpspain.eu las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

En caso de que el responsable decida comunicar la violación de la seguridad de los datos a la Autoridad de Protección de Datos, el encargado del tratamiento deberá cooperar en el proceso siempre que el responsable del tratamiento lo requiera, aportando información sobre la violación de seguridad, en particular, sobre las cuestiones indicadas en la presente cláusula.

En caso de que el responsable decida comunicar la violación de la seguridad de los datos a los interesados, el encargado del tratamiento deberá cooperar en el proceso siempre que el responsable del tratamiento lo requiera, aportando información sobre la violación de seguridad, en particular, sobre las cuestiones que se incluyan en la comunicación.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implementar las medidas de seguridad siguientes:

El PROVEEDOR estará sujeto a unas medidas de seguridad que serán adecuadas para la protección de los datos personales y demás información que deberá llevarse a cabo por el PROVEEDOR. Las medidas de seguridad, serán las contenidas en el Apéndice 1 al presente Anexo, de acuerdo con la evaluación de riesgos realizada por el responsable de tratamiento con fecha de firma del presente Anexo.

En todo caso, deberá implementar mecanismos para:

(i) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

(ii) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

(iii) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento.

(iv) Seudonimizar y cifrar los datos personales, en su caso.

q. Tener designado un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable (en el caso de que esté obligado a designarlo de acuerdo a lo dispuesto en la normativa).

r. Destino de los datos

Una vez cumplida la prestación, el encargado del tratamiento, de conformidad con las instrucciones del responsable del tratamiento y según le indique éste, deberá:

a) Devolver al responsable del tratamiento o al encargado designado por escrito por el responsable, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado; o

b) Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, en cualquier caso, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.

b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

c) Realizar las consultas previas que corresponda.

d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

f) Facilitar al encargado la descripción de las medidas de seguridad que debe implementar.

6. Responsabilidad

En caso de incumplimiento por una de las Partes de la normativa aplicable o las obligaciones establecidas en el presente Anexo / Cláusula, la Parte incumplidora deberá mantener indemne a la otra Parte. Si, como resultado de negligencia o incumplimiento, una de las Partes tuviera que hacer frente a una sanción, gasto o pérdida de cualquier tipo, la Parte incumplidora se compromete a reembolsar el importe de la sanción, gasto o pérdida, en el plazo de los dos meses siguientes al requerimiento formulado por la otra Parte.

7. Inspección de la Agencia Española de Protección de Datos

En caso de que inspectores de la Agencia Española de Protección de Datos (AEPD) se personaran en las instalaciones del PROVEEDOR al objeto de ejercer su potestad inspectora, EL PROVEEDOR se compromete a comunicar esta circunstancia a CNP ASSURANCES, S.A., Sucursal en España y CNP CAUTION, Sucursal en España en el menor tiempo posible.

8. Obligación de cumplimiento

Todo el personal del PROVEEDOR, en su caso, colaboradores y/o subcontratistas, que puedan tener acceso a datos de carácter personal cuyo responsable es CNP ASSURANCES, S.A., Sucursal en España y CNP CAUTION, Sucursal en España deberán cumplir lo establecido en la presente cláusula, cuya obligación subsistirá incluso hasta después de finalizar las relaciones contractuales entre las Partes.

Y para que así conste firman las partes el presente Anexo por duplicado ejemplar y a un solo efecto

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España

Fdo.: David Lattes

POR DATA LIS SOLUTIONS, S.L.

lis data solutions
LIS SOLUTIONS S.L. - B01507938
www.lisdatasolutions.com

Fdo.: Manuel Coterillo

APÉNDICE 1: MEDIDAS DE SEGURIDAD APLICABLES A LA PRESTACIÓN DEL SERVICIO

Introducción

1. EL PROVEEDOR se compromete firmemente a mantener la confidencialidad, la integridad y la disponibilidad de toda la información que utilice o almacene en función de su valor, su sensibilidad y de los riesgos a los que esté expuesta, de una forma que cumpla con todas las obligaciones regulatorias y contractuales aplicables.

2. EL PROVEEDOR se asegurará de que, en relación con la prestación de los Servicios, los campos siguientes estén protegidos frente a daños o abusos deliberados o accidentales:

   - los Datos del CLIENTE; incluida la Información Confidencial del CLIENTE.
   - toda información relativa a EL CLIENTE.
   - cualquier otra información utilizada en la prestación de los Servicios;
   - los sistemas informáticos del CLIENTE
   - el código informático utilizado para procesar Datos del CLIENTE incluida la Información Confidencial del CLIENTE.

Funciones y Responsabilidades

Cumplimiento

- Se establecerán reuniones de seguimiento para comprobar el cumplimiento de sus obligaciones establecidas en el presente contrato de forma mensual.
- Sin perjuicio de las demás acciones y vías de reparación a las que pueda recurrir al CLIENTE, todo incumplimiento comunicado por EL PROVEEDOR al CLIENTE de acuerdo con lo dispuesto en el apartado Cumplimiento, dará lugar a una valoración del riesgo por parte del CLIENTE que indicará al PROVEEDOR en el plazo de tiempo del que dispondrá para poner en práctica las medidas correctoras que resulten necesarias.
- EL PROVEEDOR llevará a cabo una Auditoría Independiente anual interna para confirmar que cumple con los términos del presente Contrato, y entregará al CLIENTE los resultados de la misma y copias de todos los certificados e informes dentro de los TREINTA (30) días siguientes a la fecha en que EL PROVEEDOR los hubiera recibido.

Valoración del riesgo

EL PROVEEDOR valorará los riesgos de forma periódica y, en todo caso, al menos una vez cada SEIS (6) meses y pondrá en práctica cuantas acciones y medidas de control resulten necesarias para mitigar los riesgos identificados. Si un riesgo relacionado con los Servicios o con los Sistemas del PROVEEDOR no pudiese ser mitigado, EL PROVEEDOR informará de ello al CLIENTE inmediatamente después de haber completado la valoración (informándole también de las medidas que EL PROVEEDOR haya tomado o tenga la intención de tomar), y EL CLIENTE y EL PROVEEDOR acordarán, en su caso, las medidas adicionales que puedan adoptarse para mitigar el riesgo en cuestión.

Personal del PROVEEDOR

- EL PROVEEDOR definirá claramente las funciones y responsabilidades del Personal del PROVEEDOR relacionadas con la Seguridad Informática, incluidas las limitaciones de cada función y el nivel de formación exigido, además de disponer de mecanismos que permitan asegurar la confiabilidad de los empleados, con carácter previo a su incorporación a la organización del PROVEEDOR.

- La actividad de todo el Personal del PROVEEDOR que trabaje en los locales del CLIENTE podrá ser supervisada por EL CLIENTE.

- EL PROVEEDOR se asegurará de que todos los miembros de su Personal tengan acceso únicamente a los sistemas que estén autorizados a utilizar, y que realicen su actividad dentro del ámbito definido de sus funciones y responsabilidades.

- Se identificará un 'titular' respecto de las aplicaciones, las instalaciones informáticas y las redes, y se asignarán las responsabilidades relacionadas con las tareas clave a personas capacitadas para desempeñarlas.

- EL PROVEEDOR obtendrá y registrará cada año un reconocimiento emitido por cada uno de los miembros de su Personal por el que confirmen que comprenden sus responsabilidades relacionadas con la Seguridad Informática en relación con la prestación de los Servicios.

Educación, Formación y Sensibilización

EL PROVEEDOR debe asegurarse de que se ofrezca una formación a todos los miembros de su Personal que participen en la prestación de los Servicios, que deberá abordar al menos los temas siguientes:

- la naturaleza de los Datos del CLIENTE y de la Información Confidencial del CLIENTE

- las responsabilidades de su Personal respecto de la gestión de los Datos del CLIENTE y de la Información Confidencial del CLIENTE, o que incluye una revisión de las obligaciones de confidencialidad de los empleados;

- obligaciones aplicables a la gestión correcta de los Datos del CLIENTE y de la Información Confidencial del CLIENTE en un formato físico, lo que incluye su transmisión, almacenamiento y destrucción;

- métodos adecuados para proteger los Datos del CLIENTE y la Información Confidencial del CLIENTE en el Sistema del PROVEEDOR, lo que incluye la aplicación de una política sobre contraseñas y accesos seguros;

- otras cuestiones relacionadas con la Seguridad Informática;

- la seguridad en el lugar de trabajo, lo que incluye el acceso al edificio, la comunicación de incidentes y cuestiones similares; y

- las consecuencias que acarrearía un incumplimiento del deber de proteger adecuadamente la información, que incluyen entre otros la posible pérdida del empleo, perjuicios a las personas cuyos archivos privados sean divulgados y posibles sanciones de ámbito civil, económico o penal.

La formación incluirá una prueba de conocimientos para comprobar si el Personal del PROVEEDOR comprende el significado de la sensibilización en materia de seguridad y la importancia de proteger

la confidencialidad, la integridad y la disponibilidad de los Datos del CLIENTE y de la Información Confidencial del CLIENTE, así como los Sistemas del PROVEEDOR.

- EL PROVEEDOR se asegurará de que dicha Formación en Sensibilización sobre Seguridad se imparte a su Personal en el primero de los dos hitos siguientes:
    - durante el mes siguiente a la fecha en que hayan empezado a intervenir en la prestación de los servicios; o
    - antes de que tengan acceso a los Datos del CLIENTE y a la Información Confidencial del CLIENTE.
- Cada uno de los miembros del Personal del PROVEEDOR recibirá anualmente una nueva certificación por parte del PROVEEDOR, actualizándose como corresponda el registro de formación de cada uno de ellos.
- La documentación relativa a la Formación en Sensibilización sobre Seguridad debe:
    - ser conservada por EL PROVEEDOR, para acreditar que dicha formación y las nuevas certificaciones posteriores se hayan llevado a cabo respecto de cada miembro de su Personal que intervenga en prestación de los Servicios; y
    - ser puesta a disposición del CLIENTE para su revisión, previa solicitud.
- En caso de que EL CLIENTE o EL PROVEEDOR identifique cualquier error u omisión en los registros, los materiales o la impartición de la Formación en Sensibilización sobre Seguridad, EL PROVEEDOR corregirá dicho error u omisión durante el mes siguiente a su identificación.

Responsable de Seguridad del PROVEEDOR

EL PROVEEDOR, antes de la Fecha de Arranque, nombrará a un miembro de su Personal para que actúe como Responsable de Seguridad.

El Responsable de Seguridad del PROVEEDOR deberá:

- tener conocimientos sobre asuntos relacionados con la Seguridad de la Información;
- ser capaz de responder a consultas del CLIENTE en materia de Seguridad de la información;
- asegurarse de que EL PROVEEDOR cumple con todas sus obligaciones relativas a la Seguridad de la Información establecidas en el presente Contrato; y
- en relación con los Servicios, actuar como única persona de contacto del CLIENTE en cuestiones relacionadas con la seguridad.

Incidentes de Seguridad

Notificación de los Incidentes de Seguridad

Si un Incidente de Seguridad real o potencial que afecte a los Sistemas del PROVEEDOR ha provocado, o sería susceptible de provocar, un acceso no autorizado a los Datos del CLIENTE, a la Información Confidencial del CLIENTE a los Sistemas del CLIENTE o a los Sistemas del PROVEEDOR utilizados por EL PROVEEDOR, por EL CLIENTE o por sus Agentes, o la revelación de éstos, o pudiera tener un efecto negativo sustancial sobre los mismos, EL PROVEEDOR realizará todos los esfuerzos razonables para informar inmediatamente EL CLIENTE de dicho

Incidente de Seguridad real o potencial, quedando en todo caso obligado a realizar dicha notificación dentro de las veinticuatro (24) horas naturales siguientes al momento en que EL PROVEEDOR hubiese tenido conocimiento de dicho Incidente de Seguridad.

La Notificación de Incidente de Seguridad contendrá al menos los siguientes datos:

- la fecha y la hora del Incidente de Seguridad
- un resumen de todos los hechos relevantes conocidos en relación con el Incidente de Seguridad;
- las acciones llevadas a cabo por EL PROVEEDOR para subsanar el Incidente de Seguridad y los fallos que dieron lugar a dicho Incidente de Seguridad; y
- las medidas adicionales cuya adopción sea propuesta por EL PROVEEDOR para subsanar los efectos del Incidente de Seguridad.

Incidentes de Seguridad

Si se produce un Incidente de Seguridad en los sistemas del PROVEEDOR que pudiera afectar a la información o los sistemas del CLIENTE, EL PROVEEDOR pondrá inmediatamente en marcha los mecanismos vinculados a su Proceso de Gestión de Incidencias y adoptará todas las medidas que sean necesarias para garantizar la seguridad y la integridad de los Sistemas del PROVEEDOR y restaurar la seguridad e integridad de los Datos del CLIENTE, la Información Confidencial del CLIENTE y las redes y sistemas afectados por el Incidente de Seguridad.

Respuesta de Emergencia
EL PROVEEDOR establecerá un proceso de respuesta de emergencia respaldado por un equipo de respuesta de emergencia, que describirá las acciones que pondrá en práctica su Personal en caso de que se produzca un Ataque Significativo.

Este proceso deberá tener definidos los interfaces adecuados con el plan de continuidad del servicio vigente.

Investigaciones Forenses
EL PROVEEDOR se asegurará de que se instaura un proceso para gestionar los incidentes que den lugar a una investigación forense. A través de dicho proceso, EL PROVEEDOR deberá ser capaz de analizar y de conservar las pruebas de una forma aceptable desde el punto de vista forense, para facilitar el desarrollo de cualquier proceso penal que pueda tramitarse.

Terceros y subcontratistas
EL PROVEEDOR se asegurará de que todos los contratos firmados con subcontratistas y otros terceros que cuenten con la confianza del PROVEEDOR para la prestación de los Servicios establezcan el derecho del PROVEEDOR y del CLIENTE (o de sus agentes) a realizar de forma conjunta e independiente una comprobación de la seguridad, para asegurarse de que estén cumpliendo con las obligaciones asumidas por EL PROVEEDOR en virtud del presente Contrato.

Si, en opinión del CLIENTE, un subcontratista o cualquier Tercero Proveedor fuese considerado no apto tras la correspondiente revisión de la seguridad, EL CLIENTE podrá exigir al PROVEEDOR (en el plazo de tiempo que EL CLIENTE considere apropiado) que deje de recurrir a dicho Subcontratista o a ese Tercero, y que encuentre un sustituto que EL CLIENTE considere aceptable. Alternativamente, y únicamente a instancias del CLIENTE, EL CLIENTE podrá aceptar un

compromiso del Subcontratista por el que se obligue a acordar con EL PROVEEDOR un plan correctivo legalmente vinculante, en el que deberán indicarse las acciones y los plazos necesarios para subsanar las deficiencias puestas de manifiesto a través de la revisión, y cuya finalización exitosa deberá ser aprobada por EL CLIENTE.

Derecho de inspección del CLIENTE
Sin perjuicio de lo previsto en el apartado Terceros y subcontratistas, EL CLIENTE podrá, con un preaviso escrito de no menos de DIEZ (10) Días Hábiles, inspeccionar la seguridad de cualquier centro o instalación que esté siendo utilizado, o que deba ser utilizado, por EL PROVEEDOR o por sus Subcontratistas o Terceros para desarrollar, probar, mejorar, mantener o hacer funcionar los Sistemas del PROVEEDOR utilizados en la prestación o la recuperación de los Servicios, con el fin de comprobar si EL PROVEEDOR cumple con las obligaciones asumidas por éste en virtud del presente Contrato.

EL CLIENTE podrá realizar una inspección de acuerdo con lo dispuesto en el presente apartado inmediatamente después de que se produzca un Incidente de Seguridad.
Al realizar cualquier inspección, EL CLIENTE deberá causar el menor trastorno posible al funcionamiento de los Servicios.

EL PROVEEDOR prestará toda la asistencia que EL CLIENTE pueda solicitarle razonablemente en relación con toda inspección y, sin perjuicio de lo indicado en el apartado anterior, deberá asegurarse de que los acuerdos que alcance con cualquier Tercero proveedor de servicios o Subcontratista contienen disposiciones al menos igual de restrictivas que las que se establecen en el presente apartado.

Sin perjuicio de los demás derechos y vías de reparación que correspondan al CLIENTE, el riesgo de cualquier incumplimiento identificado será evaluado por EL CLIENTE y EL CLIENTE establecerá el plazo de tiempo concedido al PROVEEDOR para poner en práctica cualquier medida correctora.

Gobierno de la seguridad de la información

Gobierno de la Seguridad de la Información
EL PROVEEDOR documentará su Marco de Gestión de la Seguridad.

EL PROVEEDOR se asegurará, al cumplir con los requisitos y las obligaciones indicadas en el presente contrato que aplicará en todo momento Buenas Prácticas de la Industria, lo que implica que deberá emplear tecnologías y procesos de seguridad disponibles y probados.

Importancia de la Gestión de la Seguridad de la Información
EL PROVEEDOR se asegurará de que la función de seguridad de la información, por su importancia para las actividades del PROVEEDOR, esté representada al más alto nivel de dirección dentro de la organización del PROVEEDOR, y de que el Marco de Gestión de la Seguridad sea aprobado por la alta dirección.

Función de Seguridad de la Información
EL PROVEEDOR dispondrá de una función especializada en seguridad de la información, que se encargará de integrar sistemáticamente la seguridad de la información en la actividad del PROVEEDOR. Esta función de cara a EL CLIENTE se materializará en la figura del Responsable de Seguridad, quien se designará en la Fase de Arranque.

Política de Seguridad de la Información

Política de Seguridad de la Información
EL PROVEEDOR dispondrá de una Política de Seguridad de la Información exhaustiva y documentada que comunicará a todos los miembros del Personal del PROVEEDOR y a cualesquiera Terceros que tengan acceso a los Datos del CLIENTE a la Información Confidencial del CLIENTE o a la información y sistemas del PROVEEDOR (incluidos los Sistemas del PROVEEDOR) (cuando tales Terceros hayan sido previamente aprobados por EL CLIENTE antes de haberles concedido dicho acceso).

Arquitectura de la Seguridad de la Información
EL PROVEEDOR dispondrá de una estructura correctamente documentada relativa a la Arquitectura de la Seguridad de la Información, que establecerá una metodología, herramientas y procesos de Buenas Prácticas de la Industria que permitan la aplicación de controles de seguridad en toda la empresa del PROVEEDOR.

Gestión de Activos

Gestión de los Medios Informáticos
EL PROVEEDOR se asegurará de que todos los datos del CLIENTE y la Información Confidencial del CLIENTE conservados o transportados en medios de almacenamiento de datos (lo que incluye ordenadores portátiles, discos duros portátiles, cintas magnéticas, almacenamiento *cloud*) sean codificados y protegidos frente al riesgo de corrupción, pérdida o revelación. Dicha codificación se aplicará de acuerdo con lo previsto en el apartado Criptografía.

Todos los archivos y sistemas de seguridad que contengan datos del CLIENTE e Información Confidencial del CLIENTE u otros datos utilizados para prestar los Servicios, deben conservarse en zonas de almacenamiento seguras y controladas desde el punto de vista medioambiental, que deberán pertenecer al PROVEEDOR o ser gestionadas o contratadas por éste.

Destrucción de Equipos y Medios Redundantes
EL PROVEEDOR se asegurará de que todos los equipos y medios informáticos redundantes sean destruidos de forma segura, lo que incluye el borrado seguro de todos los datos almacenados en dichos equipos y medios informáticos antes de su destrucción, de una forma que imposibilite su recuperación.

La destrucción segura de equipos y medios informáticos redundantes a efectos de lo dispuesto en el apartado "Gestión de los Medios Informáticos" incluirá el borrado seguro de la información que ya no sea necesaria, de una forma que imposibilite su recuperación (lo que incluye cintas magnéticas, discos, material de escritorio y cualquier otro tipo de soporte de información).

Control de Acceso

Autenticación
EL PROVEEDOR se asegurará de que el Sistema del PROVEEDOR prevea de forma efectiva las siguientes medidas de seguridad:

- Los usuarios deben siempre solicitar cuentas personales.
- No está permitido compartir credenciales ni cuentas.

Acceso Privilegiado
EL PROVEEDOR se asegurará de que:

- Las cuentas de Acceso de Usuarios Privilegiados deben tener una persona definida para su custodia como responsable.
- Las cuentas de Acceso de Usuarios Privilegiados no puedan utilizarse en operaciones día a día;
- los usuarios que disfruten de Acceso de Usuarios Privilegiados dejarán de disponer de este tipo de acceso lo antes posible cuando dejen de trabajar para EL PROVEEDOR, y en todo caso dentro de las 24 horas siguientes al momento de su salida; y
- el Acceso de Usuarios Privilegiados a la producción por parte de los desarrolladores sólo puede concederse para la prestación de asistencia en casos de cambios planificados o urgentes.

Gestión de las contraseñas
EL PROVEEDOR se asegurará de que el Sistema del PROVEEDOR prevea los siguientes controles para la gestión de las contraseñas:

- los datos de autenticación, incluidas las contraseñas, no deben almacenarse de una forma que permita que los mismos puedan ser recuperados en un formato legible o descifrable; y
- las contraseñas deben ser complejas e incluir una combinación de distintos tipos de caracteres y tener una longitud suficiente para evitar ataques exhaustivos o de diccionario.

Entorno Compartido
Si EL PROVEEDOR presta los Servicios al CLIENTE desde un emplazamiento que comparte con uno o varios Terceros, EL PROVEEDOR desarrollará y aplicará procesos, sujetos a la aprobación previa del CLIENTE que restrinjan el acceso físico e informático a los sistemas de dicho entorno compartido. En consecuencia, sólo podrán acceder a la parte del entrono compartido dedicado a los Servicios los empleados, subcontratistas o agentes del PROVEEDOR que intervengan en la prestación de los Servicios.

Bajas de usuario

Si un usuario de PROVEEDOR que da servicios al CLIENTE causa baja de la compañía, el PROVEEDOR debe notificarlo a CLIENTE con 72 horas de antelación.

Configuración del Sistema

Diseño del Sistema
EL PROVEEDOR identificará y pondrá en práctica todos los controles que sean necesarios, de acuerdo con las Buenas Prácticas de la Industria, para proteger la confidencialidad, la integridad y la disponibilidad del sistema.

Configuración de Sistemas Anfitriones y Redes
EL PROVEEDOR se asegurará de que los sistemas anfitriones y las redes que formen parte de los Sistemas del PROVEEDOR se configuren de forma que respondan a Buenas Prácticas de la Industria, a las especificaciones y a los requisitos de funcionalidad aplicables, e impidan la instalación de actualizaciones incorrectas o no autorizadas en dichos sistemas y redes.

Monitorización de los sistemas

Registro de Sucesos

Detección de Intrusos
EL PROVEEDOR desplegará herramientas de detección de intrusos en los Sistemas del PROVEEDOR, para identificar ataques reales o potenciales y responder de una forma acorde con las Buenas Prácticas de la Industria.

Filtración de Datos
EL PROVEEDOR desplegará herramientas contra la filtración de datos, de acuerdo con las Buenas Prácticas de la Industria, para detectar cualquier transmisión no autorizada de Datos del CLIENTE y de Información Confidencial del CLIENTE dentro de los Sistemas del PROVEEDOR, así como cualquier transmisión externa no autorizada de Datos del CLIENTE y de Información Confidencial del CLIENTE.

Seguridad de la Red

Conexiones Externas
EL PROVEEDOR se asegurará de que todas sus conexiones externas a las redes y aplicaciones sean identificadas, comprobadas, registradas y aprobadas individualmente por EL PROVEEDOR de acuerdo con la Política de Seguridad de la Información del PROVEEDOR y las Buenas Prácticas de la Industria.

Cortafuegos
EL PROVEEDOR se asegurará de que todas las redes de tráfico que no pertenezcan al PROVEEDOR ni sean gestionadas por éste sean enrutadas a través de un cortafuegos, antes de que se conceda el acceso a la red del PROVEEDOR.

A efectos de lo dispuesto en el punto anterior de esta sección Cortafuegos, los cortafuegos deben garantizar conexiones seguras entre los sistemas internos y externos, y se configurarán de forma que sólo pueda pasar a través de éstos el volumen de tráfico necesario.

Comunicaciones Electrónicas
E-mail: EL PROVEEDOR se asegurará de que sus sistemas de correo electrónico estén protegidos por una combinación de políticas (incluida una política de utilización que EL CLIENTE considere aceptable), formación y controles de seguridad técnicos y procedimentales documentados.

Mensajería Instantánea: EL PROVEEDOR se asegurará de que sus servicios de mensajería instantánea estén protegidos mediante la instauración de una política de gestión, el despliegue de controles de la aplicación de Mensajería Instantánea y la configuración de todos los controles de seguridad disponibles que sean aplicables a la infraestructura de Mensajería Instantánea del PROVEEDOR.

Protección Contra Código Malicioso

Protección Contra Virus y Ataques
EL PROVEEDOR establecerá y mantendrá medios actualizados de protección contra Código Malicioso, (EDR o XDR y antivirus) en toda su organización y en los sistemas que den servicio al CLIENTE.

EL PROVEEDOR dispondrá de sistemas que eviten la transferencia de Códigos Maliciosos a los Sistemas del CLIENTE, y a otros Terceros que utilicen Sistemas del CLIENTE (y el Sistema), utilizando para ello métodos actualizados habituales en el sector.

Cuando no sea posible actualizar los métodos de protección de un sistema, EL PROVEEDOR deberá desplegar las medidas de seguridad adicionales y compensatorias que sean necesarias para proteger dicho sistema vulnerable.

Gestión de los cambios y parches

Gestión de los Cambios
EL PROVEEDOR se asegurará de que los cambios que afecten a cualquier parte de los Sistemas del PROVEEDOR sean probados, revisados y aplicados a través del Proceso de Gestión de Cambios.

Soluciones de Emergencia
EL PROVEEDOR se asegurará de que sólo se apliquen soluciones de emergencia si están disponibles y han sido previamente aprobadas, a menos que su utilización suponga un riesgo mayor para el negocio. Se instarán medidas de seguridad adicional en los Sistemas del PROVEEDOR que, por cualquier motivo, no puedan actualizarse, para que el sistema vulnerable quede totalmente protegido. Todos los cambios deben realizarse de acuerdo con el proceso de gestión de cambios del PROVEEDOR.

Gestión de Terceros

Acuerdos con Terceros
EL PROVEEDOR se asegurará de que las conexiones de Terceros se sometan a una valoración del riesgo, y de que sean aprobadas y acordadas por ambas partes a través de un acuerdo documentado, como puede ser un contrato.

Contratos de servicios
EL PROVEEDOR se asegurará de que los servicios necesarios para respaldar la prestación de los Servicios sean suministrados exclusivamente por prestatarios de servicios capaces de ofrecer controles de seguridad que sean al menos igual de rigurosos que los que EL PROVEEDOR está obligado a aplicar en virtud del presente contrato. Dichos servicios se prestarán en virtud de los correspondientes contratos.

EL PROVEEDOR se asegurará de que los requisitos de servicio de los usuarios se estructuren de una forma que identifique su criticidad para el negocio.

Y para que así conste firman las partes el presente documento por duplicado ejemplar y a un solo efecto

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España

Fdo.: David Lattes

POR DATA LIS SOLUTIONS, S.L.

lis data solutions
LIS SOLUTIONS S.L - B01507938
www.lisdatasolutions.com

Fdo.: Manuel Coterillo

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS DE DIGITALIZACIÓN DE CUSTODIA, CONSERVACIÓN, DIGITALIZACIÓN Y LOGÍSTICA DE FONDOS DOCUMENTALES

Hoja de Control: Documentación a Firmar

(Esta hoja deberá ser entregada junto con la Ficha de Selección de Proveedor)

Fecha:	29 de junio de 2022						
Sociedad:	CNP ASSURANCES						
Tipo de documento:	Contrato /Anexos ■	Presupuesto/ Proyecto ☐	Doc. Consejo ☐	Doc. Hacienda ☐	Doc. DGSFP ☐	Doc. Planes/EPSV ☐	Otro:
Solicitado por: *(Director del CODIR)*	DAVID LATTES						
Contenido / Objetivo: Principal Acuerdo, entregables y descripción del servicio	CONTRATO LIS						

Cumplimentar en caso de contrato, presupuestos, proyectos, u obligaciones de pago

Denominación del Documento:	CONTRATO + ANEXOS		
Apoderado/s de CNP: *(según importe económico del contrato)* (1)	DAVID LATTES		
Contraparte: *(proveedor, o interviniente)*	LIS: Manuel COTERILLO		
Fecha de inicio del contrato:			
Fecha de vencimiento del contrato:			
Transferencia de datos:	☐ S/N Tipo de Tratamiento: Encargado ☐ Responsable ☐ Corresponsable ☐		
Renovación Tácita:	☐ SI ☐ NO		
Preaviso Cancelación:	☐ SI ☐ NO	Especificar preaviso:	
Penalización por cancelación:	☐ SI ☐ NO	Importe:	
Actualización precio por IPC, etc.:	☐ SI ☐ NO		
Delegación actividades críticas:	☐ SI ☐ NO	Especificar:	
KPI / SLA:	☐ SI ☐ NO		
Presupuestado:	☐ SI ☐ NO	Importe (IVA incluido):	
Código CECO:			
Código PEP:			
Activable:	☐ SI ☐ NO		
Periodicidad del pago:	Mensual ☐	*Trimestral* ☐	*Anual* ☐ *Pago único* ☐

- OBLIGATORIO-

Responsable del Departamento y Director del CODIR correspondiente:	Fecha:	Firma:	Firma:
Verificación de Control Financiero: *En el caso de que el gasto sea activable.*	Fecha:	Firma:	
Verificación de Control de Gestión: *En el caso de que el gasto esté presupuestado y el pedido o la factura no superen el presupuesto, no será necesaria la firma del Control de Gestión.*	Fecha:	Firma:	
Revisión Asesoría Jurídica: *(persona del equipo legal que ha revisado el contrato y verificado que cumple con todos los requerimientos solicitados)* V. H.	Fecha: 04-07	Firma:	
Comentarios Asesoría Jurídica: N.C			
Verificación de Compras:	Fecha: 04.07.22	Firma:	
Director General o Directora Operativa o Directora Financiera:	Fecha:	Firma:	
Director General o Directora Operativa:	Fecha: 04.07.22	Firma:	

(1) Véase rangos de importes económicos según hoja de pedido.

Creación 17/02/2022