ASS-13/CNP ASSURANCES/01.01/ DATABOX

A) 175

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

REUNIDOS

DE UNA PARTE, D. DAVID LATTES, mayor de edad, de nacionalidad francesa, con domicilio a estos efectos en Carrera de San Jerónimo, n.º 21, 28014, Madrid, y con NIE Y-6119145-D, en su condición de representante legal de CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA, en virtud de Escritura de poderes otorgada el 12 de julio de 2018 ante el Notario de Madrid D. Juan Aznar de la Haza con el n.º 2563 de orden de su protocolo e inscrita en el Registro Mercantil de Madrid al Tomo 30.634, Folio 137 Hoja M-73979 (en adelante, "CNP ASSURANCES") (W0013620J) y de CNP CAUTION, SUCURSAL EN ESPAÑA, en virtud de Escritura de poderes otorgada el 19 de febrero de 2021 ante el Notario de Madrid D. Juan Aznar de la Haza con el n.º 728 de orden de su protocolo e inscrita en el Registro Mercantil de Madrid al Tomo 33803, Folio 166, Hoja M-608403 (en adelante, "CNP CAUTION") (W0010754J).

Ambas entidades denominadas conjuntamente como el "Cliente".

Y, DE OTRA PARTE, D. Juan Vicente Fauró García con NIF: 02844329-B con domicilio profesional en la C/ Camino Ancho S/N 28814-Madrid en nombre y representación de DATABOX S.L. (en lo sucesivo y para ese contrato "DATABOX") con domicilio social en C/ Camino Ancho S/N, 28814 Daganzo de Arriba (Madrid) y NIF nº: B83173500. Interviene en virtud de poder otorgado a su favor en escritura de fecha 30-11-2001, ante el Notario D. José María Piñar, con el número 7269 de su protocolo.

Ambas partes se reconocen, en el concepto en que respectivamente intervienen, la capacidad necesaria para el otorgamiento del presente contrato y al efecto,

EXPONEN

1. Que **DATABOX**, tiene entre otros, dentro de su objeto social, la prestación de servicios de custodia, conservación, digitalización y logística de Fondos Documentales, contando para ello con todas las medidas de seguridad necesarias para garantizar la protección de los documentos ante cualquier imprevisto que pueda darse, incluido el fuego.

2. Que **el Cliente**, desea contratar la prestación de estos servicios.

3. Que para el desarrollo de las actividades que constituyen su objeto, **DATABOX**, cuenta, dentro de su organización, con los medios humanos, técnicos y materiales adecuados.

4. Que conforme con los expositivos precedentes, ambas partes han convenido en el otorgamiento del presente CONTRATO DE PRESTACIÓN DE SERVICIOS que se regirá por las siguientes:

ESTIPULACIONES

PRIMERA. -OBJETO DEL CONTRATO:

El objeto del presente contrato es la prestación por parte de DATABOX de los servicios de digitalización de custodia, conservación, digitalización y logística de Fondos Documentales de acuerdo con lo establecido en este documento y en sus Anexos y Apéndices.

A estos efectos se entenderá por logística, los siguientes servicios: recogida, clasificación, almacenamiento de documentos, traslado y digitalización de los mismos a las instalaciones de DATABOX.

SEGUNDA. -INSTALACIONES Y PERSONAL:

Los servicios objeto de este contrato serán prestados en las instalaciones de DATABOX que figuran en el encabezamiento del presente contrato, con desplazamientos al Cliente tantas veces como sea requerido, dentro del horario habitual de ésta y de acuerdo con las condiciones económicas establecidas en el Anexo I al presente contrato.

A estos efectos se entiende como horario habitual del Cliente, el siguiente:
El horario de servicio de DATABOX es de 08:30 horas a 18:00 horas, de lunes a jueves y los viernes de 8:30 horas a 14:30 horas, ambos inclusive, de acuerdo con el calendario laboral de la Comunidad de Madrid y los festivos de Madrid capital.

Durante la vigencia de este contrato, el Cliente estará informada en todo momento de los movimientos de su documentación, a solicitud de la propia empresa o conforme a lo establecido en la estipulación décima relativa a seguimiento y control.

Toda la documentación que el Cliente, entregue a DATABOX tendrá carácter confidencial motivo por el cual DATABOX, manifiesta que todo el personal que, para la prestación de los servicios objeto del presente contrato, tenga que gestionar esta documentación está sujeto al más estricto secreto profesional en relación con la documentación gestionada, comprometiéndose a respetar escrupulosamente esta obligación de confidencialidad y a no revelar, difundir o divulgar por ningún medio, las informaciones de las que hubiera podido tener conocimiento ni a hacer uso de la misma ni de los datos personales recogidos ni en beneficio propio ni de terceros y a cumplir con lo dispuesto por la normativa vigente sobre protección de datos de carácter personal y con lo establecido en el Anexo II al presente Contrato impidiendo su manipulación por parte de toda persona ajena a DATABOX, salvo autorización expresa y por escrito del Cliente.

TERCERA. -DOCUMENTACIÓN Y ALMACENAMIENTO:

La documentación susceptible de ser gestionada y digitalizada por DATABOX será la que conste en:

- ✓ Papel con cualquier tipo de tamaño y formato, impresos tanto por una sola cara como por ambas caras.

CUARTA. -SERVICIOS DE RECOGIDA DE DOCUMENTACIÓN:

La documentación será recogida, siempre que lo solicite el Cliente, en sus instalaciones por la empresa DATABOX para su posterior traslado y almacenamiento en sus instalaciones conforme a lo establecido en el presente contrato. El horario diario, excepto sábados, domingos, y días festivos en Madrid Capital, de recogida de documentación en el Cliente será en las 48 horas (laborables) siguientes a la solicitud de recogida siempre con previa solicitud del Cliente. La solicitud se debe hacer en horario de 9:00 a 14:00 horas si es de carácter Urgente y de 9:00 a 17:30 horas, si es de carácter Normal que se realizará por correo electrónico

Dicha documentación será trasladada a las instalaciones de DATABOX sitas en C/ Camino Ancho s/n 28814 Daganzo de Arriba (Madrid) en unos contenedores propiedad de DATABOX, de un tamaño normalizado de **410 mm x 365 mm** x 295 mm, con un peso no superior en su contenido a 30 Kg.

DATABOX mensualmente enviará al Cliente una relación de la documentación recogida y gestionada en sus instalaciones con un máximo de diez (10) días laborales desde que finaliza el mes, pudiendo ser dicho plazo más reducido según así lo haga constar el responsable del Cliente. Así mismo, a finales de mes, se incluirá en la factura el número de servicios realizados siguiendo las instrucciones de la cláusula duodécima, el tiempo (nivel de servicio) y el número de incidencias.

Las modalidades de almacenamiento que podrá emplear DATABOX serán:

ARCHIVADOR: Es un archivador DEFINICLAS que contiene distinta documentación agrupada según unos criterios de identificación establecidos por el Cliente e identificados exteriormente por un código interno establecido por DATABOX, previamente aceptado por el Cliente. Dichos archivadores serán de un tamaño de **350 mm x 250 mm x 100 mm.**

CONTENEDOR: Es una caja que contiene un máximo de **4 ARCHIVADORES (GIOS)** y tiene un tamaño de **410 mm x 365 mm** x 295 mm establecido por DATABOX.

QUINTA. -SERVICIOS DE DIGITALIZACIÓN DE LA DOCUMENTACIÓN:

La documentación que ha de ser objeto de digitalización será la recogida por DATABOX de conformidad con lo establecido en el apartado anterior y que se encuentre en sus

instalaciones. El Cliente indicará en todo momento a DATABOX qué documentación deberá ser digitalizada.

Una vez digitalizada dicha documentación, la misma permanecerá de nuevo almacenada por **DATABOX** en la forma estipulada en este contrato, salvo que el Cliente por escrito por correo electrónico indique otra cosa.

La empresa **DATABOX** prestará el servicio de digitalización que consiste en:

- **Manipulación**: Se eliminan todos los elementos (grapas, clips, gomas...) que puedan impedir un escaneo correcto, manteniendo una organización y clasificación inicial que permita un control efectivo del procedimiento desde el inicio.
- **Escaneo**: Una vez preparada la estructura de los destinos digitales en los sistemas de información, se escanean todos los documentos en función de los requisitos y parámetros que el cliente especifica. Se utilizan escáneres industriales de alto rendimiento con una tasa de escaneo de 110 a 130 hojas/minuto. Durante este proceso se auxilia cada equipo para solucionar los problemas que puedan producirse.
- **Proceso**: Los archivos digitales se finalizan con el tratamiento digital acordado: renombramiento, OCR, clasificación y análisis de información en su caso, así como cualquier otro tratamiento que las Partes pudieran acordar.
- **Clasificación/Archivo**: Los archivos físicos originales se archivan de nuevo, bien manteniendo la organización original, o reorganizando el archivo físico original de forma que facilite al cliente su archivo o tratamiento físico posterior.
- **Entrega a cliente**: Para finalizar, se entrega el trabajo realizado al cliente por los soportes que nos indique.

Las imágenes serán almacenadas por **DATABOX** en su gestor documental y el Cliente accederá a la consulta a través de contraseña y nombre de usuario.

SEXTA. -SERVICIOS DE CONSULTAS:

La empresa **DATABOX** prestará los siguientes servicios de consulta que se facturarán de acuerdo con lo dispuesto en el Anexo I del presente contrato relativa a condiciones económicas.

TIPOS DE CONSULTAS

- VÍA ORIGINAL
- VÍA ARCHIVADOR (GIO)
- VÍA CONTENEDOR (Contiene 4 GIOS)

En función de la prioridad de dicha petición de consulta, la forma de prestación del servicio de consulta podrá ser:

- NORMAL al siguiente día hábil de la petición de consulta para el resto de la documentación
- URGENTE (con compromiso de entrega de la documentación en un periodo máximo de 3 horas). Considerando siempre, que se refiere este servicio a documentos originales, fotocopia, contenedor o archivador-Gio.

DATABOX realizará informes mensuales, con un máximo de diez (10) días laborales desde que finaliza el mes, en los que se recojan los servicios de consultas realizados por el Cliente y deberán hacerse constar periódicamente a través de informes internos informatizados, que luego se contrastarán según se recoge en la estipulación cuarta referente a los servicios de recogida y digitalización de la documentación y Anexo I referente a condiciones económicas.

Las consultas realizadas a la documentación del Cliente que haya sido digitalizada por DATABOX, podrá ser consultada por el Cliente en todo momento a través del gestor documental y sin coste de consulta.

SÉPTIMA. -OTROS SERVICIOS:

DATABOX será responsable en todo momento de la correcta clasificación, inventario e identificación de los documentos almacenados conforme a los criterios, si hubiera, oportunamente comunicados por el Cliente, no pudiendo alterarlos sin previa autorización expresa y por escrito del Cliente.

Como mínimo DATABOX estará obligada a suministrar una relación general anual de toda la documentación en custodia, así como las actualizaciones correspondientes según se generen.

Además, DATABOX será responsable en todo momento de la adecuada conservación de la documentación en custodia de la compañía, así como de su adecuado manteniendo y comprometiéndose por tanto a mantenerla en buen estado en todo momento. La documentación que se encuentre fuera de las instalaciones de DATABOX en concepto de consulta, se considerará como si estuviera en custodia por la misma.

A tal fin, DATABOX garantiza la seguridad de la documentación depositada mediante el propio sistema de Organización de Archivo LSF que impide a terceros extraños la localización directa de cualquier documento concreto. Al mismo tiempo asegura la integridad física de los contenedores cerrados herméticamente, mediante la instalación de los sistemas adecuados de protección LSF, garantizando el mantenimiento de la documentación en el mismo estado en que ha sido entregado por CNP ASSURANCES.

OCTAVA. -EXPURGO Y DESTRUCCIÓN:

DATABOX, previa solicitud por escrito del Cliente prestará también servicios de destrucción de la documentación entregada por la misma para su custodia.

Dicho proceso deberá ser expresamente autorizado por escrito por el Cliente. La destrucción será realizada siempre con previa comunicación en cada caso, del lugar, día y hora, con posibilidad de ser supervisado por alguna persona responsable de dicho proceso, enviando a continuación un certificado de los documentos destruidos.

DATABOX deberá entregar al Cliente contenedores específicos para que éste pueda depositar la documentación a destruir. Dichos contenedores serán entregados en las oficinas del Cliente previa petición.

DATABOX se obliga durante todo el tiempo en que está vigente este contrato a cumplir con la normativa aplicable en materia de protección de datos y cumpliendo con todas las obligaciones e instrucciones del anexo II y el apéndice 1 del presente Contrato, así como, la normativa medioambiental vigente en cada momento.

Asimismo, DATABOX debe entregar al Cliente el certificado de destrucción dicha documentación que deberá enviar en un plazo máximo de diez (10) días después de la recogida del contendor en las oficinas del Cliente.

NOVENA. -COLABORACIÓN:

Para el desarrollo y ejecución de los trabajos aquí encomendados ambas partes se comprometen a prestar toda la colaboración que sea necesaria y razonable para la realización de los servicios encomendados conforme a lo establecido en el presente contrato.

DÉCIMA. -SEGUIMIENTO Y CONTROL:

Con el fin de realizar una adecuada labor de seguimiento y control de cada uno de los servicios encomendados, las partes designan a los siguientes interlocutores:

Por DATABOX:

D. Charo Moñino

e-mail: charom@databoxsl.es

Por CNP ASSURANCES y CNP CAUTION:

D. Fabrice Alberti

e-mail: fabrice.alberti@cnp.es

Los interlocutores indicados mantendrán, como mínimo, una reunión trimestral con el fin de conocer y determinar el estado de evolución de cada uno de los servicios encomendados. No obstante, podrán celebrarse reuniones de periodicidad inferior a solicitud de cualquiera de las partes.

A tales reuniones asistirán como mínimo los interlocutores antes indicados, pudiendo asistir otras personas involucradas en los trabajos si alguna de las partes lo considera conveniente. De las reuniones celebradas se levantará acta que suscribirán todos los

asistentes y en la cual se dejará constancia de los trabajos en ejecución, su estado de evolución, las incidencias detectadas hasta la fecha y las medidas a adoptar para solventar tales incidencias.

UNDÉCIMA. -RESPONSABILIDAD:

DATABOX manifiesta que 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 Contrato, por daños materiales o personales y sus perjuicios consecuenciales, con un límite máximo de indemnización de 300.000 euros por siniestro.

DATABOX responderá frente al Cliente de cualesquiera daños que, tanto él como las personas de las que deba responder legal o contractualmente, pudieran ocasionar al Cliente, al personal del Cliente o a terceros.

DATABOX responderá directamente de los daños y sanciones administrativas derivados de cualquier accidente sufrido o producido por él o por su personal durante la realización de los trabajos, bien sea al Cliente o a terceros.

DATABOX se obliga a cumplir y hacer cumplir con todo rigor a su personal las obligaciones impuestas por la legislación laboral, incluido el convenio colectivo de aplicación, 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.

DATABOX deberá entregar al Cliente, si así ésta lo 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 contrato 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 contrato. Dichos documentos se aportarán con periodicidad anual.
- ✓ Certificación expedida por **DATABOX** cuando así lo solicite el Cliente, acreditativa del abono de los salarios debidos, con arreglo a La normativa o pactos aplicables, a los trabajadores empleados en La realización de los trabajos objeto del contrato.
- ✓ 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 contrato y para retener el importe de las facturaciones pendientes, en

la cuantía necesaria para cubrir eventuales responsabilidades legales del cliente derivadas de los incumplimientos de **DATABOX** siempre que habiéndose concedido un plazo razonable de quince (15) días para La aportación de La documentación citada, **DATABOX** no la hubiera presentado en el citado plazo.

Para el supuesto de que por resolución judicial el Cliente fuera condenada a hacerse cargo de personal que hubiera pertenecido a la plantilla de DATABOX, DATABOX deberá pagar al Cliente una cantidad igual a la que el Cliente debiera pagar a ese personal en concepto de indemnización por despido improcedente.

DUODECIMA. -CONDICIONES ECONÓMICAS:

I. El precio para pagar por los servicios objeto de este contrato se fija en función de conceptos susceptibles de facturación que figuran en el Anexo I al presente Contrato para los servicios de custodia, conservación digitalización y logística de documentos.

II. 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, DATABOX enviará una factura a cada empresa y ambas facturas serán remitirás al siguiente correo electrónico: facturas@cnp.es

III. Los conceptos facturables están agrupados en fijos y variables. Los fijos estarán separados según la periodicidad de facturación en anuales y mensuales. Los variables estarán en función del tipo y número de consultas realizadas. Si hubiera otros servicios ajenos al objeto del presente contrato, precisarán una propuesta de DATABOX con presupuesto previo y la aprobación del Cliente.

IV. Las facturas por los servicios prestados se emitirán con periodicidad mensual y su forma de pago será a treinta (30) días de la fecha de factura, a partir de la firma del contrato.

V. La facturación del servicio de custodia anual se realizará al principio de cada mes, prorrateando la parte proporcional que le corresponda.

VI. Los precios aquí pactados se revisarán entre noviembre y diciembre de 2022.

VII. La facturación se deberá ajustar en todo momento a los conceptos recogidos en este contrato y corresponder con los informes periódicos según se recoge en las estipulaciones cuarta y quinta referente a servicios de recogida.

DECIMOTERCERA. -DURACIÓN Y RESOLUCIÓN DEL CONTRATO:

El presente contrato entrará en vigor el día 03 de junio de 2022. Su duración será de un (1) año, entendiéndose prorrogado tácitamente por períodos de un (1) año de duración de no existir notificación fehaciente de cualquiera de las partes oponiéndose

a dicha prórroga, con cinco (5) meses de antelación a la fecha de vencimiento del contrato o de cualquiera de sus prórrogas, en su caso.

Las partes acuerdan que el presente contrato podrá ser resuelto en cualquier momento por cualquiera de ellas con el sólo requisito de preavisar a la otra parte con, al menos, cinco (5) meses de antelación a la fecha en la que se vaya a dar por finalizado el presente contrato, sin que ello de derecho a la otra parte a exigir indemnización alguna.

No obstante, lo anterior, cualquiera de las partes tiene derecho a resolver este contrato de forma inmediata y por escrito si la otra parte hubiese incumplido este contrato o partes del mismo y estos incumplimientos no se rectificarán en los treinta (30) días posteriores a su notificación por escrito a la otra Parte.

Simultáneamente a la celebración de este contrato de custodia, conservación y logística de fondos documentales, las Partes han regulado en el anexo 4 un acuerdo de nivel de servicio estando ambos contratos indisolublemente unidos. La resolución de cualquier de ellos, llevará aparejada la inmediata resolución de ambos contratos.

DÉCIMOCUARTA. - PROPIEDAD, DEVOLUCIÓN DE LA DOCUMENTACIÓN Y CONFIDENCIALIDAD:

En caso de extinción del presente contrato, **DATABOX** se compromete a hacer entrega y poner a disposición del Cliente en la dirección que la misma indique toda la documentación que, como consecuencia de la prestación de los servicios objeto de este contrato, obre en su poder, sin que **DATABOX** o sus empleados tengan derecho a retener copia. Dicha entrega será facturada y pagada por el Cliente solo en caso de que el Cliente haya decidido unilateralmente disolver el contrato. En caso contrario, los costes de devolución de la documentación deberán ser asumidos por **DATABOX**. .

En el caso de la documentación que se haya digitalizada, DATABOX se compromete a entregar dicha documentación en un formato CSV a través de un pen drive que será entregado al Cliente.

Las partes estarán obligadas al deber de confidencialidad establecido en el artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, por tanto, deberán cumplir con sus deberes de secreto profesional respecto de la información a la que tengan acceso, subsistiendo dicha obligación incluso una vez acabada la relación contractual que les une de manera indefinida.

DATABOX desarrolla para el Cliente , los servicios consistentes en custodia, conservación, digitalización y logística de Fondos documentales y, para el caso en que tenga acceso a los datos personales de ficheros cuya responsabilidad es del Cliente, , DATABOX se obliga a tratar los datos de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas, es decir, integridad y

confidencialidad y a tal efecto, DATABOX manifiestan expresamente que están obligadas al cumplimiento de lo establecido en el Anexo II y en su Apéndice 1.

DATABOX garantiza que cuenta con los medios humanos y físicos necesarios para cumplir lo establecido en la normativa legal vigente sobre protección de datos personales.

DATABOX se compromete a adoptar las medidas de seguridad de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal, de forma que se evite su alteración, pérdida, y acceso o tratamiento no autorizado de acuerdo con el Anexo II y en su Apéndice 1 del presente Contrato.

DECIMOQUINTA. - PROTECCIÓN DE DATOS

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.

DATABOX 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 contrato.

DECIMOSEXTA. - CESIÓN Y SUBCONTRACIÓN:

Las Partes no podrán ceder el presente Contrato, sin el previo consentimiento por escrito de la otra. DATABOX 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 DATABOX 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, DATABOX 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 manifestaran 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 DATABOX tuviera intención de sustituir a alguno o algunos de sus subcontratistas.

DECIMOSÉPTIMA. - CLÁUSULA DE PREVENCIÓN FRENTE AL FRAUDE

El Cliente tiene tolerancia cero en lo que se refiere a prácticas de soborno y corrupción, así como mantiene un estricto control para prevenir el fraude por lo que cuenta con políticas cuyo objetivo es prevenir estas prácticas en el seno de la entidad y en cualquier relación con terceros. Se adjunta como Anexo 3 inseparable carta sobre los principios éticos que aplican al Cliente y de los que DATABOX debe ser conocedor y respetar en sus relaciones con la misma.

Con base a lo anterior, DATABOX declara contar con políticas y procedimientos internos adecuados aplicables a sus empleados, así como a cualquier tercero que colaboren con el DATABOX 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 acuerdo. Adicionalmente ambas partes declaran que el presente acuerdo 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 DATABOX garantiza, en relación con el presente acuerdo, que no existirán ventajas financieras o de cualquier otro tipo que hayan sido acordadas o que lo sean en el futuro con cualquier persona perteneciente al grupo CNP o terceras partes que colaboren con el mismo.

El incumplimiento de cualquiera de las previsiones anteriores será considerado como un incumplimiento grave del presente acuerdo, y dará derecho al Cliente a su terminación inmediata sin perjuicio de cualesquiera otras acciones legales que le puedan corresponder.

DECIMO OCTAVA. - CLÁUSULA APLICACIÓN SANCIONES FINANCIERAS

El Cliente no realizará pago de cantidad alguna que le puedan exponer o impliquen 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.

El Cliente tendrá 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.

DECIMONOVENA. -DATOS PERSONALES DE LOS FIRMANTES

Los Datos Personales de los representantes de las Partes que firman el presente Contrato serán tratados de acuerdo con la siguiente política de privacidad:

¿Quién es el Responsable del Tratamiento de sus Datos Personales?	Por parte de DATABOX: Dirección postal: Camino Ancho s/n, 28814 Daganzo de Arriba-Madrid Juan Vicente Fauró García Por parte de CNP ASSURANCES y CNP CAUTION: CNP ASSURANCES SUCURSAL EN ESPAÑA Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpspain.eu CNP CAUTION SUCURSAL EN ESPAÑA Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpspain.eu
¿Con qué finalidad se tratan sus Datos personales?	La finalidad del Tratamiento de los firmantes y las personas de contacto es gestionar de forma adecuada la relación contractual objeto de este Contrato. Las Partes tratarán estos datos para satisfacer el interés legítimo que tienen ambas compañías de mantener el contacto entre ellas durante la prestación de los servicios. Los Datos Personales serán conservados mientras sean necesarios para cumplir con las obligaciones contractuales y legales asumidas.
¿Cuál es la legitimación para el Tratamiento de sus Datos Personales?	La base de legitimación deriva del interés legítimo de cada una de las Partes de mantener relaciones de cualquier índole con la otra para cumplir con las condiciones del Contrato.
¿Cuáles son sus derechos cuando facilita sus Datos Personales?	Los sujetos interesados tienen derecho a obtener confirmación sobre si las Partes están tratando Datos Personales que les conciernan, o no. En particular, tienen derecho a: Acceder a sus Datos Personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. En determinadas circunstancias, pueden solicitar la limitación del Tratamiento de sus Datos Personales, en cuyo caso únicamente serán conservados para el ejercicio o la defensa de reclamaciones. Asimismo, también tiene derecho a oponerse al Tratamiento de sus Datos Personales. En tal caso, el responsable del Tratamiento dejará de tratar los Datos Personales, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.

	Los representantes de las Partes pueden ejercer los referidos derechos dirigiendo un correo electrónico a cada una de las direcciones electrónicas designadas en la primera fila de esta tabla. Puede obtener información adicional acerca de sus derechos ante la Agencia Española de Protección de Datos en www.agpd.es Cuando el representante no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Agencia Española de Protección de Datos en www.agpd.es .

VIGÉSIMO. -GENERALIDADES:

1. TOTALIDAD DEL CONTRATO:

El presente contrato contiene la totalidad de lo acordado entre DATABOX y El Cliente sobre las materias objeto del mismo. Las modificaciones y ampliaciones del presente contrato sólo surtirán efecto si se formalizan por escrito con la firma de ambas partes. No existen acuerdos verbales.

2. RENUNCIA:

El hecho de que una de las partes no exigiese a la otra que cumpliese una de las condiciones de este contrato que haya contravenido no supone renuncia futura de aplicación de aquella cláusula, de la que en todo momento podrá exigirse su cumplimiento.

3. NULIDAD:

Si alguna de las cláusulas del presente contrato o de sus partes fuesen nulas de pleno derecho se tendrá por no puesta, manteniendo el resto del contrato toda su fuerza vinculante.

4. LEGISLACIÓN APLICABLE Y ATRIBUCIÓN DE COMPETENCIA:

El presente contrato queda sometido a la legislación española.

Ambas partes se someten expresamente a la jurisdicción de Tribunales y Juzgados de Madrid Capital, con renuncia expresa a cualquier otro fuero o jurisdicción que pudiera corresponder, en todo a su interpretación, validez y cumplimiento.

5. DOMICILIACIÓN:

A todos los efectos que procedan, las dos partes que intervienen en este contrato fijan como domicilios a efectos de notificaciones las direcciones indicadas en el encabezamiento del contrato y toda la correspondencia, documentos, etc., que deban

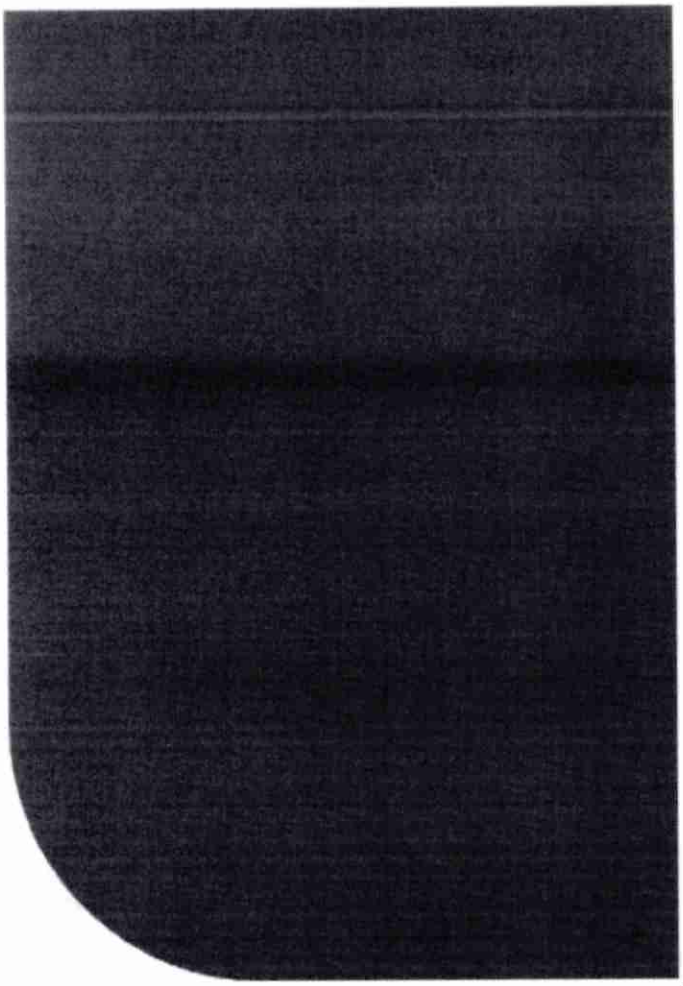
cruzarse entre ellas, para que las obligue y sea válida jurídicamente, deberá necesariamente dirigirse a los domicilios indicados.

Cualquier cambio de domicilio deberá comunicarse por carta certificada con treinta (30) días hábiles de antelación a la otra parte.

Y en prueba de conformidad con lo convenido, ambas partes firman el presente contrato, en duplicado ejemplar y a un sólo efecto.

En Madrid, a 11 de julio 2022.

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España	POR DATABOX, S.L.
Fdo.: David Lattes	Fdo.: Juan Vicente Fauró



ANEXO 1

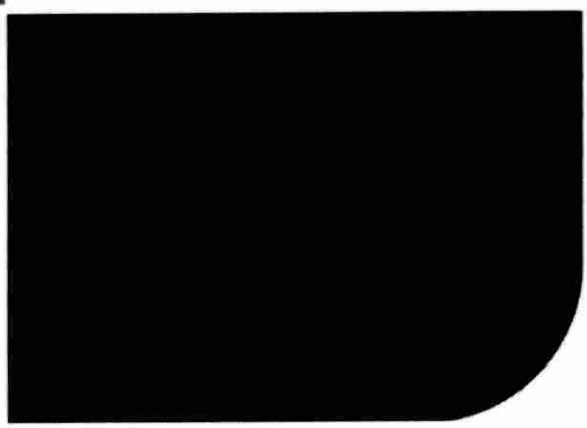
AL CONTRATO DE PRESTACIÓN DE SERVICIOS DE DIGITALIZACIÓN DE CUSTODIA, CONSERVACIÓN, DIGITALIZACIÓN Y LOGÍSTICA DE FONDOS DOCUMENTALES

ENTRE

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

Y

DATABOX, S.L.



ANEXO 1

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

Por medio del presente Anexo se incluyen los Conceptos facturables que se establecen en el marco del contrato de prestación de servicios suscrito entre DATABOX, S.L. y CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA, CNP CAUTION, SUCURSAL EN ESPAÑA y CONVISTA CONSULTING & ADVISORS S.L.U

1. Conceptos Facturables

Custodia mensual	0,2671 €/contenedor
Recogida Nueva Producción	5,63 €/contenedor
Consultas E-mail	
Consulta	4,39€/consulta
Página Adicional	0,40€/página
Consultas Urgente	
Consulta	7,50€/consulta
Página Adicional	0,40€/página
Consulta 24 horas	
Documento original o copia	5,63€/consulta
Archivador	5,63€/consulta
Contenedor	5,63€/consulta
Consultas Urgentes (Entrega en un tiempo máximo de 3 horas)	
Documento original o copia	9,39€/consulta
Archivador	11,25€/consulta
Contenedor	13,92€/consulta
Transporte por Consulta Urgente	50,00€/transporte
Destrucción o expurgo	
Destrucción física	2,00€/contenedor

Certificado de destrucción	Sin Coste
Servicio Ecobox	
Ecobox confidencial	4,89€/contenedor
Transporte	55,00€/transporte
Certificado de destrucción	Sin Coste
Manipulación e inserción	0,16€/documento
Digitalización	
Contratos de Jurídico (incluye manipulación e indexación)	0,046€/página digitalizada
Extractos bancarios y balances (incluye manipulación e indexación):	
1 Página	0,098€/página digitalizada
De 1 A 5 Páginas	0,065€/página digitalizada
De 5 A 10 Páginas	0,059€/página digitalizada
> 10 Páginas	0,054€/página digitalizada

Consultor/Visor Web	
Incluye:	
Logo del cliente	Sin Cargo en 2022
Búsquedas por un máximo de dos filtros	

Operaciones disponibles sobre los ficheros digitalizdos: descargar o mostrar en el visor web y solo para ficheros PDF o imágenes	
Todos los usuarios del sistema tienen los mismos permisos	
Almacenamiento hasta 100 GB y Backup diario con una retención de 2 días	
Permanencia mínima 12 mees	
Puesta en marcha	475 €

Los precios son sin IVA.

Y en prueba de conformidad con lo convenido, ambas partes firman el presente Anexo I, en duplicado ejemplar y a un sólo efecto, en el mismo día que el contrato del que trae causa.

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

POR DATABOX, S.L..

Fdo.: David Lattes

Fdo.: Juan Vicente Fauró

[redacted]

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

(Protección de datos personales)

ENTRE

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

Y

DATABOX S.L.

[redacted]

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, SUCURSAL EN ESPAÑA (en adelante, el CLIENTE).**

'Encargado de tratamiento' significa: **DATABOX 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
☑ Estructuración	☐ Modificación
☑ Conservación	☐ Extracción
☑ Consulta	☐ Comunicación por transmisión
☐ Difusión	☐ Interconexión
☐ Cotejo	☐ Limitación
☐ Supresión	☑ Destrucción
☑ Conservación	☐ Comunicación

☑ Otros: Almacenamiento, organización y utilización

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:

- DNI - Pasaporte – NIE – NIF (cualquier otro documento similar de identificación de la persona física)
- Nombre y apellidos
- Dirección postal
- Email
- Teléfono
- Información financiera
- Información de salud
- Información laboral
- Información sobre antecedentes penales

Estos datos serán relativos tanto de los tomadores/asegurados/ beneficiarios, empleados, administradores, proveedores y distribuidores.

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 seudonimización 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 información, 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 veinticuatro (24) 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. *(Nota aclaratoria: según art. 33.1 del RGPD).*

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	DATABOX, S.L.
Fdo.: David Lattes	Fdo.: Juan Vicente Fauró García

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 y del PROVEEDOR (incluidos los Sistemas del PROVEEDOR) que procesen, almacenen o transmitan información; y
    - 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 periódica.
- 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.

Certificados

EL PROVEEDOR en caso de obtener una certificación de Seguridad, deberá enviar el certificado al CLIENTE a mayor brevedad.

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

La responsabilidad relativa a la gestión de los Incidentes de Seguridad recae en EL PROVEEDOR, salvo en los casos en que tenga impacto sobre las obligaciones legales del CLIENTE o sobre sus procesos de negocio, donde esta responsabilidad será compartida.

EL PROVEEDOR sólo podrá revelar datos sobre un Incidente de Seguridad al Personal del PROVEEDOR cuando sea necesario para cumplir con sus obligaciones derivadas del presente Contrato, o para asegurarse de que su Personal pueda desempeñar sus funciones correctamente a efectos de que EL PROVEEDOR pueda prestar los Servicios.

Si se produce un Incidente de Seguridad, 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.

Valoración de la Seguridad

EL PROVEEDOR contratará, a su costa, a un Tercero Evaluador de la Seguridad que realizará al menos una Valoración de la Seguridad al año durante el período de vigencia del Contrato.

Como parte de la valoración de la seguridad, EL CLIENTE solicitará la realización de pruebas de *hacking* ético y penetration test sobre los sistemas del PROVEEDOR que soporten los servicios prestados.

EL CLIENTE y/o sus Agentes tendrán derecho a realizar una Valoración de la Seguridad en los Sistemas del PROVEEDOR, mediando un preaviso escrito remitido por EL CLIENTE al PROVEEDOR con VEINTE (20) Días Hábiles de antelación. La frecuencia, el ámbito y los métodos empleados para realizar la Valoración de la Seguridad serán comunicados al PROVEEDOR QUINCE (15) Días Hábiles antes del inicio de la Valoración de la Seguridad.

EL CLIENTE o sus Agentes dedicarán todos los esfuerzos razonables para asegurarse de que la Valoración de la Seguridad se lleve a cabo de una forma que cause el menor trastorno posible al funcionamiento de los Servicios y a las demás actividades del PROVEEDOR.

EL PROVEEDOR prestará al CLIENTE toda la asistencia razonable que éste o sus Agentes puedan solicitarle en relación con la Valoración de la Seguridad, y se asegurará de que los acuerdos que alcance con cualquier Tercero proveedor de servicios o Subcontratista al que pueda recurrir para la prestación de los Servicios contienen disposiciones al menos igual de restrictivas que las que se establecen en el presente apartado.

Dentro de los DIEZ (10) Días Hábiles siguientes a la finalización de una Valoración de la Seguridad, la parte que hubiera contratado al Tercero Evaluador de la Seguridad informará por escrito a la otra parte de los resultados de la Valoración de la Seguridad, poniendo de relieve los problemas de seguridad que pudieran haberse detectado.

EL PROVEEDOR, dentro de los DIEZ (10) Días Hábiles siguientes a la recepción de los resultados de la Valoración de la Seguridad, presentará un plan de acciones correctoras en el que se detallarán las medidas a adoptar y las fechas en las que los problemas de seguridad estarán totalmente resueltos.

EL CLIENTE tendrá derecho a aprobar las fechas y las medidas indicadas en el plan de acciones correctoras. Una vez ejecutado el plan, EL PROVEEDOR confirmará por escrito al CLIENTE que ha puesto en práctica todas las medidas establecidas en el plan, y que se han resuelto todos los problemas de seguridad dentro de los plazos acordados.

Tras la implantación completa del plan de acciones correctoras, EL CLIENTE tendrá derecho a contratar, o a exigir al PROVEEDOR que contrate, a un Tercero Evaluador de la Seguridad (en ambos casos, a costa del PROVEEDOR), para que realice una nueva Valoración de la Seguridad que garantice que se han resuelto plenamente los problemas de seguridad previamente identificados. En caso de que se detecte algún fallo adicional, deberá seguirse el mismo proceso establecido en el presente apartado.

Si, después de un Incidente de Seguridad, EL CLIENTE deseara realizar una Valoración de la Seguridad de emergencia en un plazo más corto que el indicado en el apartado anterior, las Partes acordarán un plazo razonable para la realización de dicha Valoración de la Seguridad que, en todo caso, se llevará a cabo dentro de los DIEZ (10) Días Hábiles siguientes a la recepción de la correspondiente notificación escrita remitida por EL CLIENTE.

EL PROVEEDOR probará de forma periódica (y al menos una vez al año) el código de *software* y otros aspectos de los principales componentes que soportan el servicio, para detectar áreas en las que podría producirse una amenaza a la seguridad. Los resultados de dichas pruebas deberán remitirse al CLIENTE de forma proactiva en las reuniones periódicas de seguimiento.

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,Medios Redundantes y Documentos

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 papel, cintas magnéticas, discos, material de escritorio y cualquier otro tipo de soporte de información).

Control de Acceso

Autenticación

EL PROVEEDOR se asegurará de que todos los miembros del Personal del PROVEEDOR que tengan acceso al Sistema del PROVEEDOR sean autenticados mediante identificaciones y contraseñas de usuario, o mediante mecanismos de autenticación de alta fiabilidad (como tarjetas inteligentes, mecanismos biométricos o sistemas de autenticación de dos factores) antes de que puedan acceder a los sistemas y las aplicaciones.

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

- Las credenciales de autenticación del usuario anterior no deben aparecer en el aviso de conexión, ni en ningún otro lugar visible;
- El sistema debe restringir el número de intentos de acceso infructuosos para impedir ataques basados en la adivinación de contraseñas;
- Las sesiones deben restringirse o expirar después de un período de inactividad predefinido, que en ningún caso será superior a los 15 minutos; y
- Los usuarios deberán ser autenticados de nuevo después de la expiración o interrupción de una sesión.

Acceso Privilegiado

EL PROVEEDOR se asegurará de que:

- Las cuentas de Acceso de Usuarios Privilegiados, en caso de no ser nominales, 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 mecanismos de autenticación deben garantizar que no puedan ser eludidos para obtener un acceso no autorizado a los sistemas;
- 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.
- Relativo a las contraseñas para dar servicio al CLIENTE, se podrá pactar la política de contraseñas junto con EL CLIENTE.

Baja de Usuario

- Las bajas de usuarios solicitadas por CLIENTE deben ejecutarse en un plazo de 24 horas.

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.

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

EL PROVEEDOR mantendrá registros de todos los sucesos clave, y en especial de los que sean susceptibles de afectar a la confidencialidad, la integridad y la disponibilidad de los Servicios prestados al CLIENTE que servirán para facilitar la identificación y la investigación de los Incidentes y/o incumplimientos significativos de los derechos de acceso que se produzcan en relación con los Sistemas del PROVEEDOR.

EL PROVEEDOR conservará este registro al menos durante los DOCE (12) meses siguientes a su creación, o durante el período distinto que EL CLIENTE pueda solicitarle razonablemente en cualquier momento, y lo protegerá frente a cualquier cambio no autorizado (lo que incluye la modificación o la eliminación de un registro). EL PROVEEDOR transmitirá el registro al CLIENTE, previa solicitud de éste.

EL PROVEEDOR revisará los registros relativos a todos los sucesos clave que se encuentren en los Sistemas del PROVEEDOR (preferentemente con herramientas automáticas) y, previa identificación de cualquier incidente y/o incumplimiento de los derechos de acceso, se asegurará de que se aplique el Proceso de Gestión de Incidentes.

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

Diseño de la Red

La red del PROVEEDOR se diseñará e implantará de forma que pueda soportar los niveles de tráfico actuales y proyectados, y se protegerá mediante controles de seguridad disponibles e incorporados de fábrica.

Documentación de la Red

La red del PROVEEDOR estará respaldada por diagramas precisos y actualizados y por obligaciones y procedimientos de control documentados.

La red del PROVEEDOR relacionada con la prestación de los Servicios estará respaldada por diagramas precisos y actualizados que incluirán todos los componentes del sistema y las interfaces con otros sistemas.

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.

Acceso inalámbrico

EL PROVEEDOR se asegurará de que el acceso inalámbrico a los Sistemas del PROVEEDOR esté sujeto a protocolos de autorización, autenticación y codificación que cumplan con las Buenas Prácticas de la Industria, y que sólo se permita desde emplazamientos aprobados por EL PROVEEDOR.

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.

Criptografía

Gestión de las Claves Criptográficas

EL PROVEEDOR se asegurará de que las claves criptográficas se gestionan en todo momento de forma segura, de acuerdo con obligaciones y procedimientos de control documentados que se correspondan con las Buenas Prácticas de la Industria, y se asegurará de que los Datos del CLIENTE y la Información Confidencial del CLIENTE sean protegidos frente al riesgo de acceso no autorizado o de destrucción.

Infraestructura de Clave Pública

Si se utiliza una infraestructura de clave pública (PKI), EL PROVEEDOR se asegurará de que esté protegida, 'endureciendo' el (los) sistema(s) operativos subyacentes y permitiendo el acceso únicamente a las Autoridades Certificadoras que puedan operar oficialmente en cada momento.

Protección de la Información Confidencial de CNP

Sin perjuicio de las obligaciones del PROVEEDOR, EL PROVEEDOR, de acuerdo con las Buenas Prácticas de la Industria, deberá codificar (y hacer que sus Subcontratistas codifiquen) toda la Información Confidencial del CLIENTE almacenada en todo tipo de aparatos de almacenamiento portátiles digitales, electrónicos o en *cloud*.

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 los Parches

EL PROVEEDOR desarrollará y pondrá en práctica una estrategia de gestión de parches respaldada por controles de gestión y por procedimientos de gestión de los ajustes y documentos operativos.

Los parches de seguridad y demás actualizaciones relativas a la vulnerabilidad de la seguridad sólo se aplicarán si están disponibles y han sido previamente aprobados, a menos que su utilización suponga un riesgo mayor para el negocio. Se instalarán 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 aprobado.

EL PROVEEDOR dispondrá de un proceso documentado para identificar y subsanar las vulnerabilidades de seguridad que presente el *software* entregado a EL CLIENTE y facilitará al CLIENTE las actualizaciones correspondientes en cuanto estén disponibles. Así como, las

soluciones temporales que sirvan para mitigar el riesgo en caso de no existir un parche oficial disponible.

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.

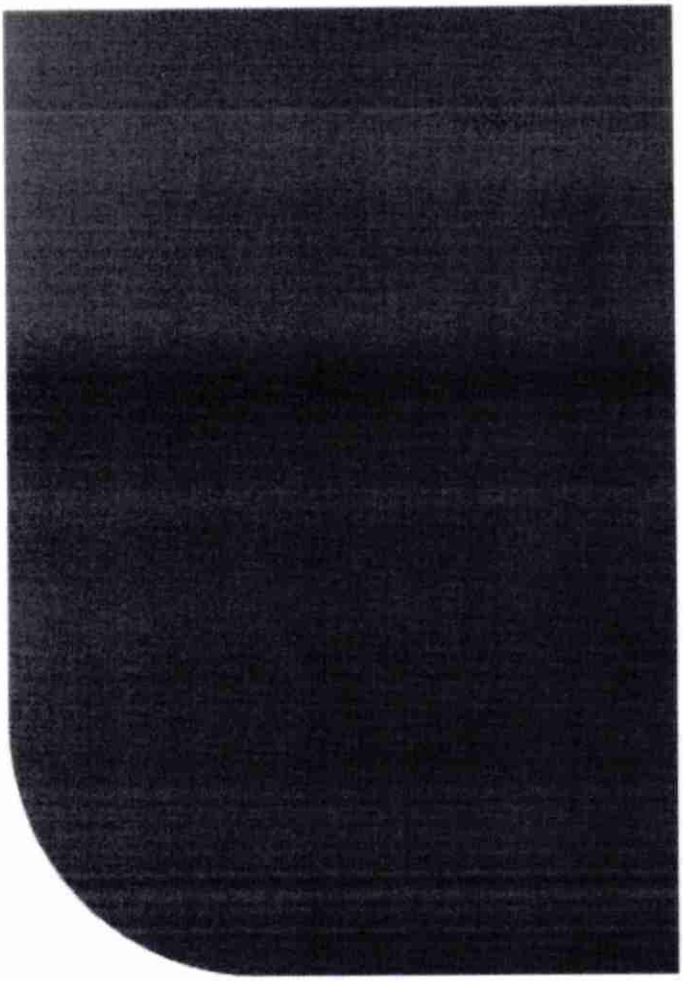
Contratos de servicios

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	DATABOX, S.L.
Fdo.: David Lattes	Fdo.: Juan Vicente Fauró García



ANEXO 3

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

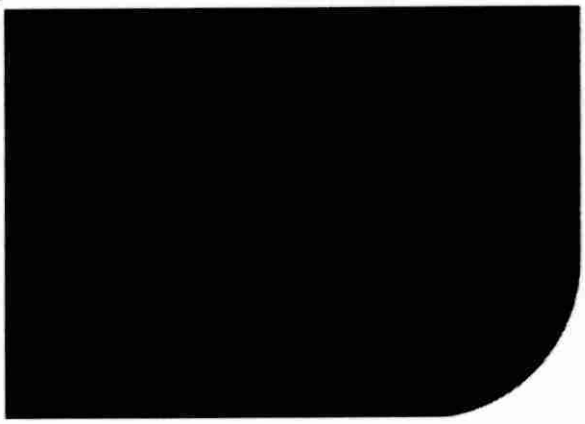
(Principios Éticos Grupo CNP)

ENTRE

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

Y

DATABOX, S.L.



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:

CNP assurances **Insuring a more open world**

ÉTICA DE NEGOCIOS.
EL 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 C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

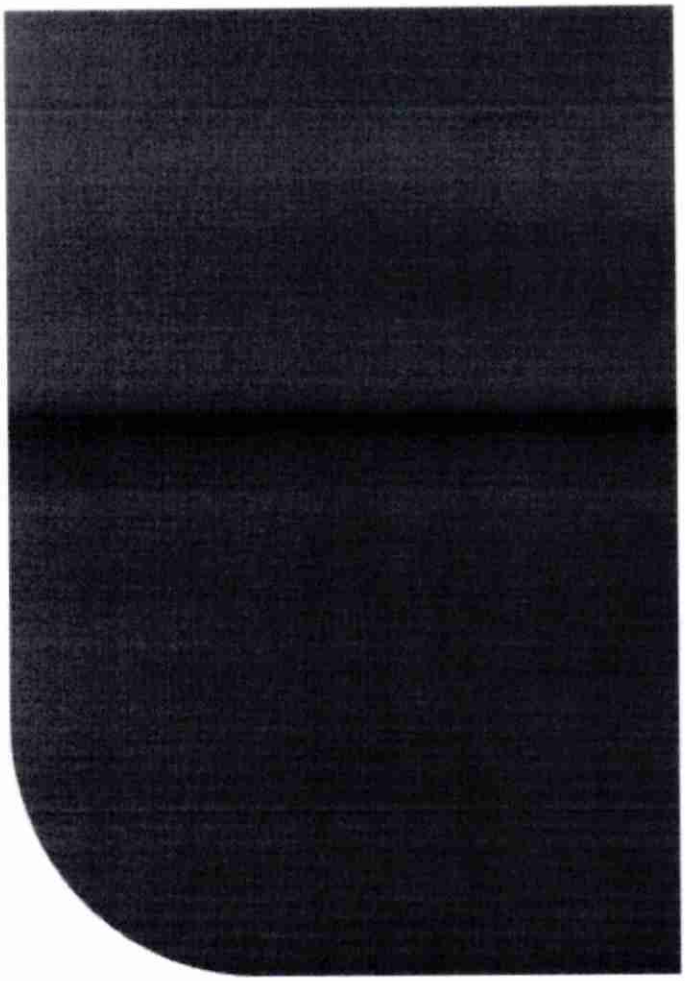
Evelyn TORTOSA
Director Conformidad Grupo

Y en prueba de recepción el suscribiente en el carácter con el que interviene, firma el presente anexo en Madrid a 11 de julio de 2022.

Por duplicado a un solo efecto.

DATABOX, S.L.

Fdo.: Juan Vicente Fauró



ANEXO 4

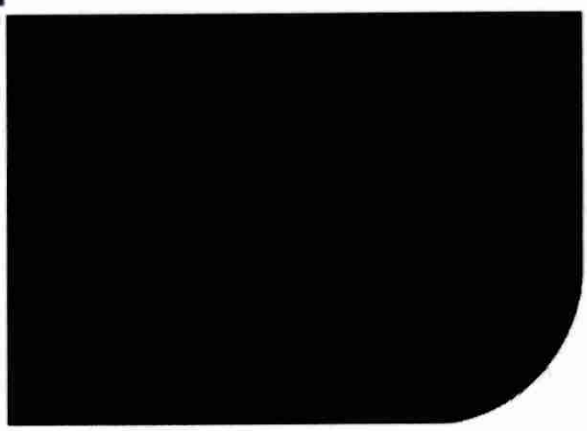
AL CONTRATO DE PRESTACIÓN DE SERVICIOS DE DIGITALIZACIÓN DE CUSTODIA, CONSERVACIÓN, DIGITALIZACIÓN Y LOGÍSTICA DE FONDOS DOCUMENTALES

ENTRE

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

Y

DATABOX, S.L.



Por medio del presente Anexo se incluyen los Acuerdos de Nivel de servicio (en adelante, SLA) que se establecen para medir y seguir el servicio que DATABOX, S.L realizará al Cliente en el marco del contrato de prestación de servicios suscrito entre ASSURANCES, S.A., SUCURSAL EN ESPAÑA, CNP CAUTION, SUCURSAL EN ESPAÑA y CONVISTA CONSULTING & ADVISORS S.L.U

1. Plazos para el cumplimiento

Tarea	Plazo máximo
Recogida de documentación	48 horas (laborales) desde la solicitud de la recogida
Solicitud de carácter normal – Documentación original	En el siguiente día laborable desde la recepción de la solicitud
Solicitud de carácter urgente – Documento original	Máximo 3 horas desde la recepción de la solicitud (con un margen de 30 minutos desde la hora de envío del email)
Expurgo	10 días hábiles desde la confirmación

2. Continuidad

DATABOX se compromete a restablecer los niveles de servicio ofertados ante la materialización de una contingencia grave en un plazo no superior a siete (7) días hábiles.

3. Capacidad

DATABOX se compromete a gestionar la capacidad de los servicios prestados al Cliente de acuerdo con sus necesidades.

Con el fin de garantizar unos niveles de servicios adecuados, DATABOX deberá informar al Cliente de posibles picos relativos al uso de recursos derivados de su actividad empresarial. Dicha notificación deberá realizarse como mínimo con tres (3) días hábiles de antelación.

4. Penalizaciones por incumplimiento

Todas las desviaciones a la baja en el nivel de cumplimiento del servicio estarán asociadas a una compensación por parte de DATABOX al Cliente.

Para establecer la compensación se definen dos niveles de incumplimiento: (i) Leve y; (ii) Grave.

Incumplimiento	Desviación leve	Desviación grave
Tiempo de entrega excedido en Solicitud Normal Documento Original	Entre 2 y 5 horas de retraso	Más de 5 horas de retraso
Tiempo de entrega excedido en Solicitud Urgente Documento Original	Entre 1 y 2 horas de retraso	Más de 2 horas de retraso
Incumplimiento	Desviación leve	Desviación grave
Tiempo de entrega excedido en Solicitud Normal Documento Original	Abono 50% coste del servicio	Abono 100% coste del servicio
Tiempo de entrega excedido en Solicitud Urgente Documento Original	Abono 50% coste del servicio	Abono 100% coste del servicio

Y en prueba de conformidad con lo convenido, ambas partes firman el presente Anexo I, en duplicado ejemplar y a un sólo efecto, en el mismo día que el contrato del que trae causa.

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

Fdo.: David Lattes

DATABOX, S.L.

Fdo.: Juan Vicente Fauró García

Hoja de Control: Documentación a Firmar

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

Fecha:	13 de julio de 2022						
Sociedad:	CNP ASSURANCES						
Tipo de documento:	Contrato /Anexos ☐	Presupuesto/ Proyecto ☐	Doc. Consejo ☐	Doc. Hacienda ☐	Doc. DGSFP ☐	Doc. Planes/EPSV ☐	Otro: OFERTA
Solicitado por: *(Director del CODIR)*	DAVID LATTES						
Contenido / Objetivo: Principal Acuerdo, entregables y descripción del servicio	DATABOX SL ARCHIVO DOCUMENTAL						

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

Denominación del Documento:	CONTRATO			
Apoderado/s de CNP: *(según importe económico del contrato)* [1]	DAVID LATTES			
Contraparte: *(proveedor, o interviniente)*				
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)*	Fecha:	Firma:	
Comentarios Asesoría Jurídica:			
Verificación de Compras:	Fecha: 14-07-22	Firma:	
Director General o Directora Operativa o Directora Financiera:	Fecha:	Firma:	
Director General o Directora Operativa:	Fecha: 14.07.2022	Firma:	

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

Creación 17/02/2022