AJ 359

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

Fecha:	28/07/2023						
Sociedad:	**CNP ASSURANCES S.A. SUCURSAL EN ESPAÑA/ CNP CAUTION SUCURSAL EN ESPAÑA**						
Tipo de documento:	Contrato /Anexos ☐	Presupuesto/ Proyecto ☐	Doc. Consejo ☐	Doc. Hacienda ☐	Doc. DGSFP ☐	Doc. Planes/EPSV ☐	Otro:
Solicitado por:							
Contenido / Objetivo: Principal Acuerdo, entregables y descripción del servicio	**Project Neptune - TSA – signed (SERVICES AGREEMENT)**						

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

Denominación del Documento:	**Project Neptune**		
Apoderado/s de CNP: *(según importe económico del contrato)* (1)	DAVID LATTES		
Contraparte: *(proveedor, o interviniente)*	**MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS, S.A. (SOCIEDAD UNIPERSONAL)**		
Fecha de inicio del contrato:			
Fecha de vencimiento del contrato:			
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 correspondiente:	Fecha: 28/07/2023	Firma:	Firma:
Verificación de Control Financiero: *En el caso de que el gasto sea activable.*	Fecha: 28/07/2023	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: 28/07/2023	Firma:	
Revisión Asesoría Jurídica: *(persona del equipo legal que ha revisado el contrato y verificado que cumple con todos los requerimientos solicitados)* ***Nereida Guardiola/Ernesto Thode***	Fecha: 28/07/2023	Firma: Ernesto Thode	
Comentarios Asesoría Jurídica: ☐ CORRESPONSABLE **X** ENCARGADO ☐ RESPONSABLE ☐ N/A			
Verificación de Compras: ***Thierry Vasquez***	Fecha: 28/07/2023	Firma:	
Representante Legal o Director Financiero ***David Lattes***	Fecha: 28/07/2023	Firma:	

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

Última versión 17/10/2019

DocuSign

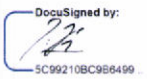
Certificate Of Completion

Envelope Id: 4443758A8A9E44BBAA709D3E4C6F4A37
Status: Completed
Subject: [Signature required] Project Neptune - TSA
a) Hogan Lovells reference:
Source Envelope:
Document Pages: 81
Signatures: 3
Certificate Pages: 4
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC) Dublin, Edinburgh, Lisbon, London

Envelope Originator:
Boris Urquizu
Atlantic House
Holborn Viaduct, London EC1A 2FG
boris.urquizu@hoganlovells.com
IP Address: 193.104.164.123

Record Tracking

Status: Original
7/27/2023 11:38:56 AM
Holder: Boris Urquizu
boris.urquizu@hoganlovells.com
Location: DocuSign

Signer Events	Signature	Timestamp
David Lattes david.lattes@cnp.es Director General Security Level: Email, Account Authentication (None)	DocuSigned by:  8AD39B55E982422...	Sent: 7/27/2023 11:46:24 AM Viewed: 7/27/2023 11:55:19 AM Signed: 7/27/2023 11:55:34 AM
	Signature Adoption: Pre-selected Style Using IP Address: 212.0.102.218	
Electronic Record and Signature Disclosure: Accepted: 7/27/2023 11:55:19 AM ID: 2fdbc112-a7b0-48b4-aa57-fead2bdc8351		
Jaime Kirkpatrik jaime.kirkpatrick@medvidapartners.com Security Level: Email, Account Authentication (None)	DocuSigned by:  5C99210BC9B6499...	Sent: 7/27/2023 11:46:24 AM Viewed: 7/27/2023 3:05:00 PM Signed: 7/27/2023 3:05:31 PM
	Signature Adoption: Drawn on Device Using IP Address: 80.28.210.230	
Electronic Record and Signature Disclosure: Accepted: 7/27/2023 3:05:00 PM ID: bc7e74a5-0b7b-48c5-b9dc-5c8275a06d5a		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Boris Urquizu boris.urquizu@hoganlovells.com Junior Associate HLI Security Level: Email, Account Authentication (None)	COPIED	Sent: 7/27/2023 11:46:25 AM
Electronic Record and Signature Disclosure: Not Offered via DocuSign		

Carbon Copy Events	Status	Timestamp
Ernesto Thode ernesto.thode@cnp.es Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:25 AM
Francisco de León Francisco.DeLeon@simmons-simmons.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:26 AM
Jaime Sánchez jsanchez@medvida.es Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:26 AM
Montse Sánchez msanchez@medvida.es Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:27 AM
Paloma Sánchez-Fayos paloma.sanchez-fayos@simmons-simmons.com Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:27 AM
Thierry Vasquez thierry.vasquez@cnp.es Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:28 AM
Zaira Santano Barriga zsantano@medvida.es Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Not Offered via DocuSign	COPIED	Sent: 7/27/2023 11:46:28 AM Viewed: 7/27/2023 2:27:37 PM

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/27/2023 11:46:29 AM
Certified Delivered	Security Checked	7/27/2023 3:05:00 PM
Signing Complete	Security Checked	7/27/2023 3:05:31 PM
Completed	Security Checked	7/27/2023 3:05:31 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

Electronic Record and Signature Disclosure created on: 6/8/2021 3:18:38 PM
Parties agreed to: David Lattes

LEGAL NOTICES

Hogan Lovells makes the DocuSign facility available as a service for its clients. However, the technology and the platform are not under its direct control, and accordingly it cannot accept any liability for any loss or damage arising out of or in connection with any use of the DocuSign facility.

For information on DocuSign's terms of use, click here.

For information on DocuSign's privacy policy, click here.

You may be asked to provide certain personal data for the purposes of use of the DocuSign facility. These may include names, signatures, email addresses, mobile phone numbers, identification documentation and visual images. These are used with the object of assisting in the execution of transaction documentation, including the verification of the identity of signatories and witnesses. Personal data provided to us in connection with the DocuSign facility will be used only for the purposes of the relevant transaction, and not for any other purpose. A full description of the rights which individuals enjoy in relation to their personal data while under our control can be found in our privacy policy, available here.

Electronic Record and Signature Disclosure created on: 9/11/2019 12:12:35 PM
Parties agreed to: Jaime Kirkpatrik

LEGAL DISCLAIMER

"Hogan Lovells makes the DocuSign facility available as a service for its clients. However, the technology and the platform are not under its direct control, and accordingly it cannot accept any liability for any loss or damage arising out of or in connection with any use of the DocuSign facility."

For information on DocuSign's terms of use, click here.

For information on DocuSign's privacy policy, click here.

Execution version

SERVICES AGREEMENT

Between

MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS, S.A. (SOCIEDAD UNIPERSONAL)

(as Service Provider)

CNP ASSURANCES, S.A., acting through CNP ASSURANCES SUCURSAL EN ESPAÑA

And

CNP CAUTION, S.A., acting through CNP CAUTION SUCURSAL EN ESPAÑA

(as Assignees)

Madrid, 27 July 2023

CONTENTS

In Madrid, on 27 July 2023.

THE PARTIES

On the one part,

MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS, S.A. (SOCIEDAD UNIPERSONAL), Spanish insurance company with registered office at Carrera de San Jerónimo, 21, 28014 Madrid, registered with the Madrid Commercial Registry at volume 4.467, page (*folio*) 140, sheet number M-73979 and with the special administrative Registry of Insurance and Reinsurance Undertakings held by the General Directorate for Insurance and Pension Funds ("**DGSFP**") under number C-0559, with Tax Identification Number (NIF) A-28534345 ("**MVP**" or "**Service Provider**").

MVP is herein duly represented by Mr. Jaime Kirkpatrick de la Vega, of legal age and Spanish nationality, whose address for these purposes is Carrera de San Jerónimo, 21, 28014 Madrid, holding Spanish National Identification Document (DNI) no. 05420369-M, currently in force, in his capacity as General Manager (*Director General*) and attorney of MVP.

On the other part,

CNP ASSURANCES SUCURSAL EN ESPAÑA, Spanish branch office of the French insurance company CNP Assurances, S.A., with registered office at Calle Cedaceros 10, fifth floor, 28014 Madrid, registered with the Madrid Commercial Registry at volume 20.063, page (*folio*) 48, sheet number M-353.978 and with the special administrative Registry of Insurance and Reinsurance Undertakings held by the DGSFP under number E-0160, with Tax Identification Number (NIF) W-0013620-J ("**CNP Assurances**").

CNP Assurances is herein duly represented by Mr. David Lattes, of legal age and French nationality, whose address for these purposes is Calle Cedaceros 10, fifth floor, 28014 Madrid, holding Spanish Foreigners Identity Name (N.I.E.) no. Y6119145D, currently in force, in his capacity as legal branch representative (*representante legal permanente*) of CNP Assurances.

And on the other part,

CNP CAUTION SUCURSAL EN ESPAÑA, Spanish branch office of the French insurance company CNP Caution, S.A., with registered office at Calle Cedaceros 10, fifth floor, 28014 Madrid, registered with the Madrid Commercial Registry at volume 33.803, page (*folio*) 166, sheet number M-608.403 and with the special administrative Registry of Insurance and Reinsurance Undertakings held by the DGSFP under number E-0221, with Tax Identification Number (NIF) W-0010754-J ("**CNP Caution**").

CNP Caution is herein duly represented by Mr. David Lattes, of legal age and French nationality, whose address for these purposes is Calle Cedaceros 10, fifth floor, 28014 Madrid, holding Spanish Foreigners Identity Name (N.I.E.) no. Y6119145D, currently in force, in his capacity as legal branch representative (*representante legal permanente*) of CNP Caution.

CNP Assurances and CNP Caution shall be jointly referred to as the "**Assignees**" and each of them individually as an "**Assignee**". The Service Provider and the Assignees shall be jointly referred to as the "**Parties**" and each of them individually as a "**Party**".

RECITALS

I. MVP is a Spanish insurance undertaking that has the required administrative authorisation to carry out insurance activities in Spain in the life (0), accident (1), sickness (2) and miscellaneous financial loss (16) insurance classes, carrying out insurance activities in Italy under the right of establishment regime and in France and Portugal under the freedom to provide services regime.

II. CNP Assurances is the branch office of a French insurance undertaking (CNP Assurances, S.A.) that has the required administrative authorisations to carry out insurance activities in the life, accident and sickness insurance classes, being entitled to carry out those activities in Spain under the right of establishment regime, carrying out insurance activities in Portugal through CNP Assurances under the freedom to provide services regime.

III. CNP Caution is the branch office of a French insurance undertaking (CNP Caution, S.A.) that has the required administrative authorisation to carry out insurance businness in the miscellaneous financial loss insurance class, being entitled to carry out those activities in Spain under the right of establishment regime, carrying out insurance activities in Portugal through CNP Caution under the freedom to provide services regime.

IV. On 29 June 2023 MVP and the Assignees have entered into an insurance portfolio assignment agreement in order to transfer the PPI Business of MVP, including its PPI portfolio, to the Assignees ("**Insurance Business Transfer Agreement**" or "**IBTA**").

V. The Assignees consider essential MVP to provide certain services in connection with the PPI Business (as this term is defined in the IBTA), as part of the assigned business under the IBTA, for a certain period of time after the transfer.

VI. Consequently, the Parties agree to enter into this services agreement ("**Agreement**"), in accordance with the following

CLAUSES

1 DEFINITIONS AND INTERPRETATION

1.1 Capitalised terms shall have the meaning given to them throughout this Agreement or in **Annex 1.1**. Capitalized terms used but not otherwise defined herein shall have the meanings ascribed to such terms in the IBTA.

1.2 Unless the context requires otherwise, the provisions of this Agreement shall be construed as provided in **Annex 1.2**.

2 PURPOSE OF THE AGREEMENT

2.1 The purpose of this Agreement is the provision to the Assignees of services in connection with the PPI Business, to be executed by the Service Provider in exchange for the Fees set out in Clause 5 below (the "**Services**").

2.2 The Services to be rendered by the Service Provider shall be those detailed in **Annex 2.2**.

2.3 Additionally to the Services detailed in Annex 2.2, the Parties may agree that the Service Provider provides other services which are needed to operate the PPI Business after the Closing Date (the "**Omitted Services**").

2.4 At the request of the Assignees, the Service Provider shall provide, or procure the provision of, the Omitted Services as part of the Services, provided that the Parties agree on the terms and conditions according to which those services will be provided and the additional fees to be paid to the Service Provider for the provision of such services.

For these purposes, and subject to what is set forth in previous paragraph, both Parties undertake to (a) cooperate in good faith to try to determine the scope of the Services, the Fees, the start date and other terms for such Omitted Services, taking into account any reasonable views of the Assignees and the Service Provider and (b) make the necessary amendments to the Agreement, as provided for in clause 2.5 below.

2.5 Annex 2.2 and Annex 5.1 shall be updated to include the relevant details of the Omitted Services, including the fees to be paid by the Assignees to the Service Provider.

2.6 During the period between the signing of this Agreement and its termination, MVP shall share, upon request by the Assignees, with the Assignees and/or the service provider(s) appointed by them (the "**TPA Service Provider(s)**") (in all cases subject to and within the limits of applicable law, including, without limitation, competition law, intellectual property and personal data protection) such information, documentation, data and files relating to the PPI Business as may be deemed necessary by the Parties for the correct continuation of the PPI Business following termination of this Agreement.

2.7 Such process of communication of the Shared Information to the Assignees and/or their TPA Service Provider(s) shall be referred to as the "**Migration Process**". The Migration Process shall ensure a timely and effective transition of the PPI Business into the Assignees and/or the TPA Service Provider(s), so that the Assignees and/or the TPA Service Provider is able to provide, completely and independently, the corresponding Services from the first day they must provide said Services.

2.8 The Shared Information to be communicated by MVP to the Assignees and/or to the TPA Service Provider(s) appointed by the Assignees may include, to the extent necessary to complete the Migration Process, Personal Data related to the PPI Business, contained in files for which the Service Provider is responsible, in accordance with the provisions of article 21 LOPD and any other applicable provisions under the GDPR and the LOPD.

2.9 The Parties shall make its best efforts to agree and incorporate into this Agreement, by 30 September 2023 at the latest, key performance indicators for the work to be carried out by the Parties in connection with the Migration Process, with an aim to complete the Migration Process within the first three (3) months of the term of this Agreement and, if not, to provide for the development of work plans, with a view to completely agree the terms and conditions of the Migration Process as soon as possible and, in no case, later than the Closing Date (as this term is

defined in the Insurance Business Transfer Agreement). In any event, the provisions of Clause 3 with regard to the Term of this Agreement shall apply.

2.10 The activities to be carried out pursuant to these Clauses 2.6 to 2.9 shall in no case oblige MVP to vary the current format or content of the information and documentation relating to the PPI Business, which shall be provided to the Assignees and/or the TPA Service Provider(s) in the state, with the content and format in which it is currently held by MVP (it being specified that such information and documentation shall include all the updated information and documentation used by MVP to effectively manage the PPI Business), without any obligation for MVP to adapt or vary the same and without any guarantee with regard to the compatibility of the same with the systems and platforms used by the Assignees or the TPA Service Provider(s), MVP not being obliged to make any expense or investment in this regard. Therefore, the Shared Information shall be provided in the form in which it is currently stored in the Service Provider's systems ("AS IS" and "AS AVAILABLE").

2.11 If the Insurance Business Transfer Agreement is terminated for any reason, without the transfer of the PPI Business to the Assignees being completed, the Assignees shall immediately remove or destroy, and/or cause the TPA Service Provider(s), to whom MVP has provided the Shared Information provided for in Clause 2.6, to remove or destroy, all the Shared Information. Likewise, in this event, should the Shared Information include any physical files or documentation, the Assignees shall return and/or cause the TPA Service Provider(s) to return the physical files or documentation in their original condition to MVP at the address and to the attention of the contact details set out in Clause 16.

2.12 For clarification purposes, it is noted that in no event shall MVP provide any of the services that constitute the subject matter of the PPI TPA Agreement (as this term is defined in the IBTA), which, should such agreement be finally executed, shall be solely provided to the Assignees, as of the Closing Date, by one or more service providers, under their sole responsibility.

3 TERM

3.1 Except as provided in clauses 2.6 to 2.11 which shall be effective from the signing of this Agreement, this Agreement shall become effective on the Closing Date (as this term is defined in the Insurance Business Transfer Agreement) and will continue in full force, subject to what it is stated in this Agreement, for six (6) months following the Closing Date, in no event extending its term beyond 30 June 2024, as foreseen in Clause 2.2(f) of the IBTA (the "**Term**").

3.2 Each Party irrevocably waives any right it may have under any applicable law to terminate or bring about the end of this Agreement other than as provided for in this Agreement or in mandatory legal provisions and agrees that the foregoing is reasonable having regard to all relevant circumstances at the time of entering into this Agreement.

4 PROVISION OF SERVICES

4.1 Services

The Service Provider shall provide (or, when applicable, procure the provision of) the Services,

making available the premises, personnel and equipment required for the performance of such Services, whether they are rendered directly by the Service Provider or by a third party.

4.2 Standard of Services

In the performance of the Services under this Agreement, the Service Provider shall meet the following general standards:

(a) provide the Services to the Assignees in a timely manner during the term of the Agreement;

(b) act in accordance with usual industry practices and standards;

(c) exercise the skill and diligence to be expected of a supplier of similar services, having regard to the size, scope and complexity of the Services;

(d) provide to the Assignees, at the request of the latter, with up-to-date information in relation to the Services; and

(e) supply the Services with a level of risk-management and internal control, and implement the core measures and controls, which are reasonably adequate to manage the risks associated with the performance of the Services.

4.3 Service Provider as independent contractor

(a) The Service Provider's personnel will be under the organizational direction of the Service Provider only, so that all personnel employment related matters, including, but not limited, to hiring, discipline, working time, compensations of any kind, performance appraisal, remuneration, social benefit payments and administration shall be the sole responsibility of the Service Provider. The Service Provider shall:

(i) discharge all payroll, benefits, and employment-related obligations regarding its personnel;

(ii) comply with applicable legal obligations towards its personnel in relation to remuneration, Social Security contributions, employment conditions foreseen in collective bargaining agreements, other collective agreements and internal policies applicable, health and safety measures, tax, pensions and any benefit entitlement, being therefore liable for any breach of the employment, Social Security, health and safety, tax and pension obligations caused by the Service Provider in relation to itself and its personnel. In this regard, the Service Provider undertakes to ensure that its personnel is sufficiently qualified and reliable to perform the Services provided by the Service Providers' personnel; and

(iii) have the right to designate, at its discretion, which of its employees it will assign

to perform the Services, and to remove any person from the Service Provider's personnel at any time.

(b) In addition to the above, upon request of the Assignees, the Service Provider undertakes to deliver to the Assignees, certificates (including any of its Sub-Contractors) confirming no defaults on payment issued by the Spanish General Secretary of the Social Security, as well as to present any documentation that the Assignees may deem appropriate, acting reasonably, for the purpose of evidencing the fulfilment of the above-mentioned legal obligations *vis-à-vis* the staff providing the Services.

4.4 Provision of the Services by Sub-Contractors

The Service Provider will be entitled to subcontract the Services, provided that (i) any breach of the obligations under this Agreement caused by a Sub-Contractor shall be treated as a breach by the Service Provider under this Agreement; and (ii) the Service Provider notifies it beforehand (within a reasonable period of time), in writing, to the Assignees; all without prejudice to the application of Clause 10.5.

The Service Provider shall remain responsible for the provision the Services as if such Services were performed by the Service Provider's employees, without being released from its obligations and responsibilities under the Agreement.

For the avoidance of doubt, any service provider under the PPI TPA Agreement, should this agreement be finally executed, shall not be considered a Sub-contractor of the Service Provider in any event, nor shall the Service Provider assume any liability with respect to the service provider(s)' acts and omissions.

5 FEES

5.1 Fees payable

Subject to what is stated in this Agreement, in consideration for the provision of the Services by the Service Provider to the Assignees in accordance with Clause 4, the Assignees shall pay to the Service Provider the Fees detailed in **Annex 5.1** with regard to the Services.

The amount of the Fees payable under this Agreement shall be distributed among the Assignees in the following proportion: 39% CNP Assurances and 61% CNP Caution.

5.2 Reimbursement of costs and expenses

In no event shall MVP be obliged to advance the payment of claims in respect of PPI policies from its own funds or advance the payment of any expenses on behalf of the Assignees.

Notwithstanding the foregoing, in the event that MVP anticipates the payment of any costs, expenses or disbursements on behalf of any of the Assignees, the Assignees shall be obliged to reimburse the Service Provider for those.

The Parties may agree, at the Management Meetings provided for in Clause 11, the mechanisms they deem appropriate for the advance of certain amounts by the Assignees to the Service Provider.

5.3 Invoices and payment

(a) The Service Provider shall submit an invoice to the Assignees to cover the Services rendered monthly, including the relevant information and formalities set forth in Royal Decree 1619/2012, of November 30th ("*Reglamento por el que se regulan las obligaciones de facturación*") and all information necessary for tax and accounting purposes.

(b) Where the Service Provider has incurred costs, expenses and disbursements on behalf of the Assignees which are payable by the Assignees according to Clause 5.2 above these will also be included in the invoice to be paid by the Assignees.

(c) The Assignees shall pay the invoice within twenty (30) Business Days of its receipt by means of a bank transfer to the Service Provider's account at the following bank account or to any other bank account which the Service Provider may notify the Assignees at a later date pursuant to Clause 16 (Notices):

Account holder: MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS SAU

Bank: BANCO SANTANDER

IBAN: ES45 0049 1182 3523 1008 0762

BIC: BSCHESMMXXX

(d) The Assignees shall not be obliged to pay a sum which is in dispute (a "**Disputed Amount**"), either in respect of a Service or of Fees, costs, expenses or disbursements paid by the Service Provider for the provision of the Services.

In case there is a Disputed Amount, the Assignees will notify the Service Provider, and in no event later than fifteen (15) Business Days following receipt of such invoice, of any objection of the Service Recipient with regard to such invoice and the Parties will discuss in good faith to resolve such disagreement.

If the relevant Parties do not reach an agreement within ten (10) Business Days, either Party may submit the dispute in writing to the Management Meeting (as these term is defined in Clause 11.2) and the Management Meeting shall hold a meeting promptly to examine the dispute, and in any event, in the next monthly meeting.

If the relevant Management Meeting has not settled the dispute, the Parties shall refer all disputes in respect of a Disputed Amount to the procedure set out in Clause 18.

Notwithstanding all the foregoing, the Assignees shall be obliged to pay, within the same invoice, those amounts that are not in dispute.

(e) If the Services are not rendered for a full calendar month, as it may happen in the initial month of this Agreement and in the final month if terminated, then the payable Fees shall be pro-rated on a daily basis to reflect the number of days the Agreement has been in effect during such calendar month.

(f) Fees shall be subject to the taxes applicable to the Services from time to time. In particular, all the fees to be paid by the Assignees to the Service Provider pursuant to this Agreement shall be subject to VAT at the applicable VAT rate from time to time.

(g) Fees may be revised (upwards or downwards) annually by the Parties, without being possible to change the Fees without the unanimous agreement of the Parties.

5.4 Default Interest

Save for any Disputed Amounts, the Parties will pay interest on any amounts that are not paid by the due date for payment. Interest will accrue and be calculated on a daily basis at the annual rate of 4,0625%, for the period from (but excluding) the due date for payment to (and including) the date of actual payment.

6 WARRANTIES AND OBLIGATIONS

6.1 Mutual Warranties

Each Party warrants to the other that:

(a) it is duly constituted, organised and validly existing under the laws of the country of its incorporation;

(b) it has the legal right and full power and authority to execute and deliver, and to exercise its rights and perform its obligations under this Agreement; and

(c) nothing contained in this Agreement will result in a breach of any provision of its constitutional documents or result in a breach of any agreement, licence or other instrument, order, judgment or decree of any court, governmental agency or regulatory body to which it is bound.

6.2 Service Provider Warranties:

The Service Provider warrants to the Assignees that:

(a) it has necessary authorisation required by Law to provide the Services;

(b) it has sufficient organizational and contractual measures in place to provide the Services in accordance with this Agreement; and

(c) it has the financial resources to perform the Services.

6.3 Mutual Obligations

The Service Provider shall, and the Assignees shall:

(a) participate in discussions regarding the provision of the Services where reasonably required by the other Party in order to facilitate decision making in relation to the Services;

(b) maintain reasonable security measures to protect the other's systems from third parties, including from any virus or other software intended or designed to:

(i) permit access or use of information technology systems by a third party other than as expressly authorised; or

(ii) disable, damage, erase, disrupt or impair the normal operation of any information technology systems; and

(c) notify the other Party of any breach of this Clause 6.2 or any other event relating to it that is likely to materially affect the security of the other Party's systems.

6.4 Service Provider's obligations

The Service provider shall:

(a) render the Services or any other services under Clause 2 as determined in this Agreement and as agreed by the Parties;

(b) undertake not to disclose the Confidential Information of the Assignees to which they have access on the occasion of this Agreement with regard to systems, methodology, equipment, programs and technical information;

(c) comply with the security obligations foreseen in **Annex 6.4(c)**.

(d) use reasonable endeavours to respond promptly to any request, instruction or information from the Assignees in relation to the Services; and

(e) fulfil any other obligation expressly set forth in this Agreement.

6.5 Assignees' obligations

The Assignees shall:

(a) in consideration for the provision of the Services, pay the Fees according to the provisions of this Agreement;

(b) undertake not to disclose the Confidential Information of the Service Provider to which they have access on the occasion of this Agreement with regard to systems, methodology, equipment, programs and technical information;

(c) ensure that all suitably authorised personnel of the Service Provider have such access to any information or records kept by or under the control of the Assignees in relation to the Services as may be necessary to enable the Service Provider to provide the Services; and

(d) use reasonable endeavours to respond promptly to any request for guidance, instruction or information from the Service Provider in relation to the Services; and

7 TERMINATION

7.1 Termination events

This Agreement shall terminate:

(a) upon expiry of the Term provided for in Clause 3 above;

(b) by mutual written agreement of the Parties;

(c) by the Assignees' decision, subject to a prior one (1) month written notice given by the Assignees to the Service Provider;

(d) by the Assignees' decision, subject to the procedure regulated under Clause 7.2 below; or

(e) by the Service Provider's decision, subject to the procedure regulated under Clause 7.3 below.

7.2 Termination by the Assignees

The Assignees shall be entitled to terminate this Agreement forthwith upon written notice to the Service Provider:

(a) if the Service Provider commits a material breach of this Agreement which either (i) cannot be remedied or (ii) has not been effectively remedied within thirty (30) Business Days of the date upon which the Assignees serve written notice on the Service Provider specifying the breach and requiring its remedy; or

(b) to the extent permitted by the applicable law, if the Service Provider ceases, or is likely to cease, to carry on its business.

7.3 Termination by the Service Provider

The Service Provider shall be entitled to terminate this Agreement forthwith upon written notice to the Assignees:

(a) If any of the Assignees fails to pay any amount (save for any Disputed Amount) when due in accordance with this Agreement and such default continues for a period of more than ten (10) Business Days after written notice of such failure is given to the Assignees;

(b) if any of the Assignees commits a material breach of this Agreement (different from that set out in (a) above) which either (i) cannot be remedied or (ii) has not been effectively remedied within thirty (30) Business Days of the date upon which the Service Provider serves written notice on the Assignees specifying the breach and requiring its remedy; or

(c) to the extent permitted by the applicable law, if the Service Provider ceases, or is likely to cease, to carry on its business.

7.4 For the purpose of Clauses 7.2(a) and 7.3(b), a breach shall be considered as capable of being remedied if the Party in breach can still comply with the provision in question and it can be done, *vis-à-vis* third parties, in time and form in all material respects and without generating any damages for the Assignees.

7.5 If the Service Provider fails to provide any of the Services, this will not be considered a breach of its obligations under the terms of this Agreement, to the extent that the failure to provide such Service or obligation in question is caused by:

(a) A prior breach by the Assignees of their obligations under this Agreement;

(b) the Assignees failing, without reasonable cause, to grant or procure any approvals required pursuant to this Agreement;

(c) the Assignees preventing the Service Provider in its performance of the Services;

(d) the Assignees not supplying to the Service Provider such information which is in their possession or control, or instructions, as may reasonably be requested by the Service Provider, and which are essential for the Service Provider to perform the Services; or

(e) an act or omission of the Service Provider in circumstances where, prior to such act or omission:

(i) the Service Provider has advised in writing to the Assignees:

(A) that such act or omission would cause a breach of the Service Provider's obligations under this Agreement; and

(B) of the likely negative consequences of such act or omission; and

(ii) the Assignees have, following receipt of such advice, instructed the Service Provider in writing to so act or refrain from acting.

7.6 The termination of this Agreement shall be enforceable only towards the defaulting Assignee and the termination right exercised by the relevant Party shall neither be binding upon, nor affect the rights of the non-defaulting Assignee under this Agreement.

8 CONSEQUENCES OF TERMINATION

8.1 If the Agreement is terminated the Assignees shall pay to the Service Provider all accrued but unpaid amount for the Services provided until the date of termination of this Agreement, save for any Disputed Amount. For the avoidance of doubt the Parties acknowledge that if termination takes place in accordance with Clause 7.2(a) the Assignees will not be obliged to pay any amounts to the Service Provider under this Agreement.

8.2 Subject to what is stated in the next paragraph, upon termination of this Agreement, the Service Provider shall:

(a) return to the Assignees any documents produced, received or kept in connection with the provision of the Services; and

(b) transfer to the Assignees (if agreed by it) to the extent reasonably possible (if any), any agreements between the Service Provider and third parties, including third party agreements relating to the provision of the Services.

8.3 Termination or expiry of this Agreement shall not affect any rights, liabilities, remedies or obligations which may have accrued prior to termination or expiry. The obligations of each Party set out in any Clause intended to survive such termination or expiry, including, without limitation, Clauses 4 (Provision of Services), 5 (Fees), 6 (Warranties and Obligations), 9 (Liability), 12 (Audit and Information), 13 (Confidentiality), 15 (IP Rights), 17 (Ancillary Provisions) and 18 (Governing Law and Arbitration), shall continue in full force and effect notwithstanding termination or expiry of this Agreement.

9 LIABILITY

9.1 The Service Provider's liability for breach of its obligations under this Agreement shall be limited to an amount equal to the Fees effectively received by the Service Provider under this Agreement for the Services provided during the six (6) months immediately preceding the date on which the Services Provider was notified of the occurrence of the breach by any of the Assignees. This

limitation of liability shall not apply in cases of wilful misconduct (*dolo*) of the Service Provider and in cases where a limitation of liability is not permitted by law.

9.2 In no event shall any of the Parties assume any liability for loss of profit.

9.3 For clarification purposes, MVP shall not incur any liability with respect to the services to be provided under the PPI TPA Agreement, should this agreement be finally executed pursuant to the terms of the IBTA.

9.4 In order to submit any claim for damages, the Party who suffered the damages shall notify the other Party about the facts giving rise to such a claim within a maximum period of thirty (30) Business Days from the date on which they were effectively known by the Party claiming the damages.

9.5 The liability of the Assignees for breach of their obligations under this Agreement shall be joint (*mancomunada*).

10 BUSINESS CONTINUITY AND DISASTER RECOVERY AND FORCE MAJEURE

10.1 The Service Provider shall provide business continuity and disaster recovery in respect of the Services in accordance with the plans in existence as at the date of this Agreement, as these may be modified from time to time (the "**Business Continuity and Disaster Recovery Plans**").

10.2 The Service Provider shall provide reasonable information, to the Assignees in relation to the Business Continuity and Disaster Recovery Plans.

10.3 The Service Provider may unilaterally make changes to its Business Continuity and Disaster Recovery Plans from time to time, provided that it does not significantly affect the quality of the Services.

10.4 Following the declaration of a disaster or the occurrence of a Force Majeure Event:

(a) the Service Provider shall implement the Business Continuity and Disaster Recovery Plans;

(b) the Service Provider shall continue to provide, to the extent reasonably possible, those Services which are not affected by the disaster or Force Majeure Event in accordance with the provisions of this Agreement;

(c) the Service Provider shall, to the extent reasonably possible, continue to provide those Services which are affected by the disaster or Force Majeure Event with a reasonable

degree of continuity in accordance with the Business Continuity and Disaster Recovery Plans; and

(d) the Assignees shall comply with all reasonable obligations given to it in the Business Continuity and Disaster Recovery Plans so long as the Service Provider has provided written notice of any such obligations.

10.5 Neither Party shall be liable for any delay or total or partial non-performance of its obligations under this Agreement arising directly from a Force Majeure Event, provided that the Party seeking to rely on this Clause 10.5 has enacted, to the extent reasonably possible, any Business Continuity and Disaster Recovery Plans relevant to the Force Majeure Event.

10.6 If a Force Majeure Event occurs, the affected Party shall promptly (and, in no case, later than three (3) Business Days) notify the other Party in writing of the cause of the delay or non-performance and the likely duration of the delay or non-performance.

10.7 The Assignees may, without prejudice to its other rights or remedies, terminate this Agreement if, as a result of a Force Majeure Event, the Service Provider's obligations under this Agreement are not resumed within one (1) month after a notice from the Assignees to the Service Provider.

11 RELATIONSHIP MANAGERS

11.1 Relationship Managers

The principal point of contact between the Assignees and the Service Provider in relation to issues arising out of this Agreement or the performance of the Services will be the Relationship Managers.

Either Party may change the identity of its Relationship Manager at any time by giving notice to the other.

11.2 Meetings

(a) Every month (or at such other frequency as the Parties may agree) the Parties shall procure that their respective Relationship Managers meet (each such meeting a "**Management Meeting**") for the purposes of:

(i) considering any issues arising out of the performance of the Services; and

(ii) considering any other issues arising under or in connection with this Agreement.

(b) Within a reasonable timeframe prior to each such Management Meeting, the Service Provider shall provide the Assignees with such information as is reasonably required for the Assignees to assess and monitor the performance of the Services.

12 AUDIT AND INFORMATION

12.1 The Service Provider shall, and shall procure that any Sub-Contractor:

(a) permit the Assignees' supervisory authority or its designated representatives to access the facilities of the Service Provider that the supervisory authority has requested to audit, in order to access to the data, information and documentation that such supervisory authority may require in the exercise of its supervisory functions over the Assignees' activity and the PPI Business, including the possibility for the relevant supervisory authority to conduct on-site inspections; and

(b) provide such information and assistance as the supervisory authority may reasonably require, including by attending meetings requested by the supervisory authority.

12.2 The Service Provider shall, and shall procure that any Sub-Contrator shall:

(a) permit the employees, or auditors and/or any other person duly appointed by the Assignees to access the facilities and/or to have access to any information it may reasonably require of Service Provider that the Assignees has requested to audit; and

(b) provide such information and assistance (including a right to use a copy of the relevant information and/or documentation) as the Assignees may reasonably require.

12.3 An audit pursuant to Clauses 12.1 and 12.2:

(a) may be made subject to the employees or auditors or any other person duly appointed by the Assignees of the Assignees signing appropriate duties of confidentiality;

(b) may not unreasonably interfere with the operations of the Party subject to such audit;

(c) shall be paid for by the Assignees; and

(d) shall be notified in writing to the Service Provider reasonably in advance.

12.4 Except for serious reasons that are reasonably justified, the number of audits to be carried out under this Clause upon the Assignees' request shall be limited to one per year, without such audits interfering with the normal functioning of the activity of the various departments and business units of MVP.

12.5 Without prejudice to the aforementioned right of audit the Parties acknowledge that it is an essential part of this Agreement that the Assignees, advisors, reinsurers and/or any other party duly appointed by the Assignees can have access to (including, without limitation, a right to copy)

records, systems contracts, documents, books, ledgers and other materials and Data related to the PPI Business.

12.6 Under this Clause 12 the Assignees (or any person acting under its behalf) shall not be entitled to access information which would cause the Service Provider to be in breach of any applicable law, regulation or supervisory authority.

13 CONFIDENTIALITY

The terms and conditions set forth in this Agreement and the Confidential Information shall be kept strictly confidential by the receiving Party.

Each Party agrees to limit the distribution of the Confidential Information received (including this Agreement) to those of its officers, shareholders, employees, agents, professional advisors and auditors as far as such distribution is necessary for the completion, enforcement and performance of this Agreement and for audit, accounting or internal compliance purposes of each Party.

Notwithstanding the foregoing:

(a) each Party will be entitled to disclose the Confidential Information to the following persons to the extent that they reasonably require to know the Confidential Information:

(i) its Affiliates; and/or

(ii) its and its Affiliates:

(iii) financiers and re-financiers (including prospective financiers and re-financiers);

(iv) employees, administrators, agents, consultants and professional advisers, including its auditors and legal advisers;

(v) co-investors (including potential direct or indirect investors in the relevant Party); and/or

(vi) reinsurance companies and retrocessionaires, including any potential reinsurers and retrocessionaires, to the extent the Confidential Information is necessary for the execution or performance of the relevant reinsurance and retrocession agreements,

provided that the disclosing Party will assume the responsibility for the use, dissemination or transfer of the Confidential Information to third parties in those cases where said use, dissemination or transfer is in breach of the terms of this Clause; and

(b) a Party may disclose Confidential Information if and to the extent that:

(i) such disclosure is required by any applicable Law, administrative or judicial order, or by the rules or regulations of any stock exchange or other regulatory body to

which such Party is subject. In this case, the Party bound to disclose all or any part of the Confidential Information shall inform the other Party before disclosing Confidential Information, to the extent legally permitted, in order to take appropriate measures to prevent the disclosure. If the disclosure cannot be prevented the disclosing Party shall disclose only that portion of the Confidential Information legally and validly required and shall make commercially reasonable efforts to ensure that the Confidential Information so disclosed will be given confidential treatment;

(ii) such disclosure is required to complete any actions, perform any obligations or enforce any rights set forth hereunder); or

(iii) the disclosed Confidential Information became part of the public domain through no breach of a confidentiality undertaking, has been independently developed by the relevant Party without using any parts of the Confidential Information or has been legally provided by a third party without breaching any confidentiality undertaking.

14 PROCESSING OF PERSONAL DATA

14.1 Processing of Personal Data by the Service Provider as Processor.

As a consequence of rendering the Services, the Service Provider will process Personal Data of which Assignees are Data Controller and linked to the relevant Services, acting as Processor in accordance with the regulations contained in the GDPR. For these purposes, the Parties will enter into a data processing agreement according to article 28 of the GDPR, in the terms and conditions that are set out in **Annex 14.1**.

14.2 Processing of Personal Data by the Parties as Data Controllers

(a) Notwithstanding the processing of Personal Data of the Assignees by the Service Provider as Processor as described in Clause 14.1 above, the Parties agree to share with each other certain Personal Data (such data received by the other Party: "**Shared Data**") on the basis of Article 6 par. 1 (c) and (f) of the GDPR for purposes of the performance of the Agreement and the fulfilment of legal obligations only ("**Permitted Purpose**").

No special categories of Personal Data (sensitive data) will be transferred and processed. The Party receiving Shared Data from the other shall be referred to herein as the "**Data Receiver**" and the Party transferring Shared Data to the Data Receiver shall be referred to herein as the "**Data Discloser**". Details of the Shared Data:

(i) Categories of data subjects concerned: individuals (signatories hereof, representatives and contact persons of the Parties) involved in the execution of the Agreement.

(ii) Categories of Shared Data: Contact details (such as name, position, location, telephone number or other communication channel data), professional details and data related to the management of HHRR and management of services (including verification of the registration with the Social Security system, certificates proving that they are up to date in the payment of their remuneration, etc. only when required by law to provide the services).

(b) The Data Receiver shall at all times process Shared Data in a professional manner in compliance with applicable law, the Agreement and this clause, exercising due skill, care and diligence and shall implement and apply appropriate, state of the art level of technical and organizational data security standards.

(c) Any disclosure or transfer of Shared Data by the Data Receiver to a third party is only admissible if required for the Permitted Purpose and must comply with applicable laws.

(d) Data Discloser shall inform data subjects concerned about the sharing of Shared Data under this clause in accordance with arts. 13 and 14 of the GDPR (for this purpose, Assignees' DPO can be contacted here: dpd.es@cnp.es). Where permitted under applicable laws, the Data Receiver shall promptly notify the Data Discloser of any requests, objections or any other enquiries of data subjects under applicable laws regarding the processing of Shared Data ("Data Subject Requests") which may give rise to any legal obligation or liability or otherwise concern the legitimate interests of the Data Discloser.

(e) The Data Receiver shall promptly delete Shared Data once they are no longer required for the Permitted Purposes unless the Data Receiver is required or legally permitted under applicable law to continue processing the Shared Data.

15 IP RIGHTS

15.1 Each Party (the "**First Party**") shall grant, or shall procure the grant to, the other Party (the "**Second Party**") a non-exclusive, royalty-free, fully paid-up, non-transferable, irrevocable during the Term licence to use the Intellectual Property Rights owned by, or licensed to, the First Party solely to the extent (also in terms of duration and territory) necessary for the purpose of performing or receiving (and enjoying the benefit of) any of the Services in accordance with this Agreement and to otherwise receive the full benefit of this Agreement.

15.2 The Second Party acknowledges and agrees that:

(a) any Intellectual Property Rights licensed to it pursuant to Clause 15.1 will remain the sole property of the First Party or the relevant member of the First Party's Group, or their licensors (as appropriate); and

(b) the First Party or their licensors (as appropriate) owning such Intellectual Property Rights or materials, shall own all Intellectual Property Rights subsisting in any and all

adaptations of, modifications and enhancements to and works derived from such materials or Intellectual Property Rights.

16 NOTICES

All notices and other communications required or permitted to be given or made pursuant to this Agreement shall be in writing in the English language and shall be: (a) delivered by hand against an acknowledgement of delivery dated and signed by the recipient; (b) sent by an overnight courier service of recognized international standing (all changes paid); or (c) sent by e-mail, and, except if receipt is not confirmed by the recipient at the latest of the second (2nd) Business Day, confirmed by registered mail (postage prepaid, return receipt requested) posted no later than the third (3rd) Business Day (it being specified that any time period set forth under this Agreement being extended by three (3) additional Business Days in this case) (provided that any notice or communication which is received after 6 p.m. -local time in the place of receipt- on a Business Day or on any day which is not a Business Day shall be deemed received only at 9 a.m. -local time in the place of receipt- on the next Business Day) to the relevant Party at its address set forth below:

If to the Assignees, to:

Att.: Mr David Lattes, Mr Thierry Vasquez and Mrs Nereida Guardiola

With copy to Mr Ernesto Thode

Address: Calle Cedaceros 10, fifth floor, 28014 Madrid

Email: david.lattes@cnp.fr; thierry.vasquez@cnp.es; and nereida.guardiola@cnp.es

With copy to: ernesto.thode@cnp.es; and legal@cnp.es

If to the Service Provider, to:

Att.: Mr Jaime Kirkpatrick, Mr Santiago Domínguez and Mrs. Begoña Peña

With copy to Mr Jaime Sánchez

Address: Carrera de San Jerónimo, 21, 28014 Madrid

Email: jkirkpatrick@medvida.es; santiago.dominguez@medvidapartners.com; and begona.pena@medvidapartners.com

With copy to: jsanchez@medvida.es

or to such persons or at such other addresses as hereafter may be furnished by either Party by like notice to the other. Any such notice or other communication shall be effective only upon actual receipt thereof by its intended recipient.

17 ANCILLARY PROVISIONS

17.1 Waiver

The delay or failure by either Party to exercise any of its powers, rights or remedies under this Agreement shall not operate as a waiver of them, nor shall any single or partial exercise of any such powers, rights or remedies preclude any other or further exercise of them. The remedies provided in this Agreement are cumulative and not exclusive of any remedies provided by law.

17.2 Assignment

The Parties shall be entitled to assign this Agreement to any entity belonging to their respective Groups, provided that the relevant Party obtains prior written consent to the assignment from the other Party, such consent not to be unreasonably withheld.

17.3 Severability

If any part of this Agreement is found by any court or other competent authority to be invalid, unlawful or unenforceable then such part shall be severed from the remainder of this Agreement which shall continue to be valid and enforceable to the fullest extent permitted by law.

17.4 Costs and expenses

Each Party shall pay its own legal expenses incurred in the preparation and execution of this Agreement.

17.5 Entire agreement

This Agreement supersedes any agreements made or existing between the Parties before or simultaneously with this Agreement (all of which shall be deemed to have been terminated by mutual consent with effect from the commencement date of this Agreement) and constitutes the entire understanding between the Parties in relation to the subject matter of this Agreement. Except as otherwise permitted by this Agreement, no change to its terms shall be effective unless it is in writing and signed by or on behalf of both Parties.

This Agreement is subject to its own terms and to the provisions foreseen in the IBTA. In case of contradiction between the IBTA and this Agreement, this Agreement shall prevail.

18 GOVERNING LAW AND ARBITRATION

18.1 This Agreement shall be governed by Spanish common law (*legislación común española*).

18.2 The Parties expressly waive the jurisdiction of the courts and agree that any litigation, dispute, issue or claim arising from the performance or interpretation of this Agreement or related thereto, whether directly or indirectly, shall be finally resolved by arbitration according to law, in accordance with the Spanish Arbitration Act (Law 60/2003 of 23 December) in the framework of the Court of Arbitration of the Official Chamber of Commerce, Industry and Services of Madrid, to which is entrusted the administration of the arbitration proceedings and the appointment of the arbitrators in accordance with its rules and by-laws.

18.3 The arbitration proceedings shall be heard and decided by an arbitral tribunal formed by three arbitrators belonging to the International Chamber of Commerce who shall be appointed at the time the dispute arises as follows: (1) one arbitrator shall be appointed by MVP; (2) one arbitrator shall be jointly appointed by the Assignees; and (3) one arbitrator, who shall chair the Tribunal, shall be appointed by mutual agreement of MVP and the Assignees, or, in the event such agreement is not reached, by the Court of Arbitration of the Court of Arbitration of the Official Chamber of Commerce, Industry and Services of Madrid in accordance with its by-laws.

18.4 The arbitral proceeding shall be held in Madrid (Spain).

18.5 The arbitral tribunal shall include in its final award the distribution among MVP and the Assignees of the arbitration fees and expenses, of the legal costs of the Parties (including reasonable fees of lawyers), the cost of the service provided by the arbitral institution and all other expenses arising in the arbitration proceedings, it being the intention of the Parties that such fees, expenses and costs are distributed in accordance with their relative fault (where relevant), to the extent to which such default may be duly determined in the arbitration, according to the specific circumstances of the dispute.

18.6 The Parties expressly place on record their commitment to comply with the final arbitral award, and any partial awards which may be issued in the arbitral proceedings.

19 ELECTRONIC SIGNATURE

19.1 This Agreement is signed by each of the Parties using an advanced electronic signature (AES) process implemented by a third party service provider, DocuSign, which guarantees the security and integrity of digital copies in accordance with Regulation (EU) n°910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trusted services for electronic transactions within the internal market.

19.2 The Agreement is drawn up in a single original digital copy, a copy of which shall be delivered to each of the Parties directly by DocuSign, which is in charge of implementing the advanced electronic signature solution under the conditions required by applicable Laws.

19.3 Electronically executed on 27 July 2023 by way of DocuSign.

[Signatures on the last page]

LIST OF ANNEXES

Annex	Title
Annex 1.1	Definitions
Annex 1.2	Rules of interpretation
Annex 2.1	Services
Annex 5.1	Fees
Annex 6.4(c)	Security
Annex 14.1	Data Processing Agreement

Annex 1.1
Definitions

In this Agreement the following words and expressions shall have the following meanings:

"**Agreement**" means this services agreement and all its annexes;

"**Business Continuity and Disaster Recovery Plans**" shall have the meaning set out in Clause 10.1;

"**Business Day**" means a day (other than a Saturday, Sunday or public holiday) when banks are open for business in the city of Madrid and/or Paris;

"Data" means, without limitation, all data, contract, recordings of telephone conversations, document, information (including historical information) or other content in any format or medium, and whether stored electronically or otherwise, in connection with the PPI Business;

"**Data Controller(s)**" shall have the meaning set forth in the article 4 of the GDPR.

"Data Discloser" shall have the meaning set out in Clause 14.2(a);

"Data Protection Regulations" means the GDPR and LOPD and all other applicable regulations and recommendations whatsoever relating, from time to time, to the processing of personal data and privacy in Spain.

"Data Receiver" shall have the meaning set out in Clause 14.2(a);

"**Data Subject Requests"** shall have the meaning set out in Clause 14.2;

"Disputed Amount" shall have the meaning set out in Clause 5.3(d);

"Extended Term" shall have the meaning set out in Clause 3.1;

"Fees" means the amounts payable to the Service Provider pursuant to Clause 5.1;

"Final PPNC" shall have the meaning set out in Annex 5.1;

"First Party" shall have the meaning set out in Clause 15.1;

"Force Majeure Event" means any event of extraordinary character which the non-performing Party is unable to prevent, such as for instance labour strikes of any nature, pandemic and epidemic diseases, revolutions, riots, rebellions, sabotage, curfews, acts of terrorism, civil wars, fires, floods, earthquakes, storms, acts of god, equipment or software failure (including computer virus, cyberattacks and malicious acts on any Information Systems), internet suspension, electricity outages, telecommunication outages or acts or omissions of governmental authorities, provided that (i) such event makes impossible or not feasible or materially negatively impacts the ability to fulfil any material obligation set out in this Agreement, (ii) the non-performing Party is without fault in causing or failing to prevent such occurrence, and (iii) such event may not be avoided by the use of precautions commonly adopted (i.e. should the Party involved, using the common care, have taken all such precautions adopted in order to avoid, minimize such event).

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

"Group" shall in respect of any company mean that company and any and all companies that are in the same group of companies (as such term is defined in Article 42 of Royal Decree dated 22 August 1885, by which the Code of Commerce is published) from time to time as that company;

"Initial PPNC" shall have the meaning set out in Annex 5.1;

"Insurance Business Transfer Agreement" or **"IBTA"** means the insurance portfolio assignment agreement for the transfer of the PPI Business, entered into between MVP, as Cedant, and CNP Assurances and CNP Caution, as Assignees;

"Intellectual Property Rights" means all industrial and intellectual property rights (including but not limited to those rights of a personal and economic character such as author's rights (including reproduction, transformation, distribution and public communication, amongst others, and authorization to exercise any of such author´s rights with respect to any derivative work), as well as the right to use) which are recognized by or arise under Spanish intellectual or industrial property laws or laws of any other jurisdiction as the case may be and will include but will not be limited to trademarks, service marks, trade names, domain names, get-up, logos, patents, inventions, registered and unregistered design rights, copyrights, software, database rights and all other similar rights in any part of the world including, where such rights are obtained or enhanced by registration, any registration of such rights and applications and rights to apply for such registrations;

"LOPD" means Organic Law 3/2018 of 5 December on the Protection of Personal Data and the guarantee of digital rights.

"Management Meeting" shall have the meaning set out in Clause 11.2(a);

"month "n"" shall have the meaning set out in Annex 5.1;

"**Omitted Services**" shall have the meaning set out in Clause 2.3;

"Parties" shall have the meaning given in the introductory paragraph;

"Party" shall have the meaning given in the introductory paragraph;

"Permitted Purpose" shall have the meaning set out in Clause 14.2(a);

"Personal Data" shall have the meaning set out in article 4 of the GDPR;

"PPNC" shall have the meaning set out in Annex 5.1;

"**PPI TPA Agreement**" shall have the meaning given to this term in the IBTA;

"Processor" means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of a Controller, as defined in Article 4 of the GDPR;

"Relationship Manager" means Mr Santiago Domínguez Vacas in relation to the Service Provider, and Mr Thierry Vasquez together with Mrs Nereida Guardiola, in relation to the Assignees;

"Second Party" shall have the meaning set out in Clause 15;

"Services" shall have the meaning given to this term in Clause 2.1, and includes, for the avoidance of doubt all (i) services specified in Annex 2.2, and (ii) Omitted Services;

"**Service Provider**" shall have the meaning given to this term in the headings of this Agreement;

"Shared Data" shall have the meaning set out in Clause 14.2(a);

"Shared Information" shall have the meaning set out in Clause 2.62.6;

"Sub-contractor" means any person engaged by the Service Provider from time to time as may be permitted by Clause 17.2 (Sub-contracting and assignment) to procure the provision of the Services (and "Sub-contractor" shall mean any one of them);

"Term" shall have the meaning set out in Clause 3.1; and

"TPA Service Provider(s)" shall have the meaning set out in Clause 2.6.

Annex 1.2
Rules of interpretation

In this Agreement, unless otherwise specified, reference to:

(a) "includes" and "including" shall mean including without limitation;

(b) a "party" means a party to this Agreement and includes its permitted assignees (if any) and/or the successors in title to that part of its undertaking which includes this Agreement;

(c) a "person" includes any natural or legal person, individual, company, firm, corporation, government, state or agency of a state or any undertaking (whether or not having separate legal personality and irrespective of the jurisdiction in or under the law of which it was incorporated or exists);

(d) "Clauses", "paragraphs" or "Annexes" are to Clauses and paragraphs of and Annexes to this Agreement;

(e) "writing" or "written" (or similar terms) includes any methods of representing words in a legible form (other than writing on an electronic or visual display screen) or other writing in non-transitory form;

(f) the terms "best efforts", "reasonable efforts", any of their equivalents or derivatives, or any other references to "reasonable" actions, assistance, steps, matters or similar, shall be construed to those efforts that, in light of all relevant circumstances and contractual obligations, can reasonably be expected to try to achieve an envisaged result, without such Party being required to incur any unreasonable liability, costs and expenses or obtain any specific result.

(g) words denoting the singular shall include the plural and vice versa, and words denoting either gender shall include both genders;

(h) expressions and phrases in other languages: this Agreement is made in the English language and, therefore, the English language version shall prevail over any translation of this Agreement. However, the meaning of the Spanish expressions and phrases (or other expressions and phrases in other languages) used in this Agreement shall prevail over the meaning of the English expressions and phrases to which they relate.

Annex 2.2
Services

The Parties agree to execute the Services Annex in Spanish, with the terms and conditions set forth hereto:

Por medio del presente Anexo 2.2, las Partes establecen el detalle de los Servicios, las condiciones en las que deben ser prestados dichos Servicios, así como los niveles de servicio ("**SLA's**") objeto del presente Contrato.

El Proveedor (o "**MVP**" a los efectos de este Anexo 2.2) prestará a los Cesionarios (o "**CNP**" a los efectos de este Anexo 2.2), los Servicios de gestión y administración del Negocio PPI que se relacionan a continuación, en relación con los siguientes seguros y coberturas.

I. **Seguros**:

(a) Seguro de protección de pagos:

1. Pérdida Involuntaria de Empleo (desempleo);
2. Incapacidad Temporal por enfermedad o accidente;
3. Hospitalización por enfermedad o accidente;
4. Fallecimiento por enfermedad o accidente;
5. Incapacidad Permanente Absoluta por enfermedad o accidente;
6. Nacimiento múltiple;
7. Divorcio; y
8. Traslado profesional.

(b) GAV:

1. Secuelas Permanentes por accidente en la vida privada; y
2. Fallecimiento por accidente en la vida privada.

(c) Seguro de hospitalización:

1. Hospitalización;
2. Hospitalización Accidente;
3. Fallecimiento Accidente; y
4. Fallecimiento Accidente Circulación.

II. **Índice de Servicios:**

1. Legal;
2. Ficheros de Producción (Altas/bajas/Gestión de errores);
3. Gestión a través de Front-End (Altas);

4. Atención telefónica y/o por correo (postal o electrónico);
5. Tarificadores;
6. Modificaciones no económicas;
7. Modificaciones económicas;
8. Desistimientos o Cancelaciones por decisión unilateral del tomador/asegurado;
9. Gestión de cobros/impagados;
10. Renovaciones;
11. Gestión de siniestros;
12. Gestión, guarda y custodia de la documentación;
13. Gestión de quejas y reclamaciones;
14. Gestión del Ministerio de Justicia (pólizas con garantía de fallecimiento);
15. Gestión de fichero EIAC (pólizas, recibos, comisiones y siniestros);
16. Ejercicio de derechos de protección de Datos Personales;
17. Prevención de Blanqueo de Capitales y de la Financiación del Terrorismo (PBC/FT);
18. Gestión de Comisiones;
19. Gestión apuntes contables;
20. Gestión modelos fiscales;
21. Informes de actuarial;
22. Gestión documentación contractual;
23. Servicios adicionales;
24. Informes periódicos;

III. Descripción de los Servicios:

Todos los periodos en días descritos en este Anexo 2.2 están expresados en Días Hábiles.

1. Legal

El Proveedor se hará cargo de:

(a) Adaptación a la normativa en vigor en todo momento;
(b) Dar soporte a CNP en relación con las peticiones realizadas por los auditores externos e internos poniendo a disposición de la misma la información que dichos auditores requieran para la realización de los pertinentes informes, siempre y cuando dicha información obre en poder del Proveedor.
(c) Generar la información necesaria de CNP relativa a Protección de Datos bajo la supervisión del DPO de CNP.
(d) Remitir a CNP cualquier tipo de requerimiento o notificación que reciba por parte de un organismo público o privado o de supervisión o cualquier otra persona física o jurídica en relación con la cartera de productos del presente contrato.
(e) Colaborar con CNP en la aportación de información necesaria para cumplimentar los requerimientos de los organismos públicos o privados, supervisores, y demás personas físicas o jurídicas siempre que dicha información obre en poder del Proveedor.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Cumplimiento de las obligaciones derivadas de cambios normativos.	Implementación de las medidas en todo caso, antes de su entrada en vigor.	Mensual	100%	2
Remitir a CNP los requerimientos y notificaciones recibidas de organismos públicos o privados y/o de supervisión en relación con la cartera de productos objeto del presente Contrato.	Envío del documento en el plazo de 1 día desde su recepción	N/A	100%	5
Colaborar con el envío de documentación que se requiera por parte de auditores internos, externos, DPO, organismos oficiales y supervisores demás personas cuya finalidad sea cumplir con obligaciones legales	Envío de la información requerida en 3 días desde la recepción de la solicitud de información. Dicho plazo podrá ser ampliado a 7 días si por la naturaleza de la documentación requerida, no pudiera obtenerse en el citado plazo de 3 días.	Mensual	100%	2

Quedan excluidas de este apartado las quejas y reclamaciones interpuestas ante el Servicio de Atención al Cliente, ante la DGSFP, así como las demandas y litigios, que se encuentran reguladas en el apartado 13 siguiente.

2. Ficheros de Producción (Altas/bajas/Gestión de errores)

MVP recibirá a través de SFTP los ficheros de producción emitidos por cada mediador/distribuidor, de forma diaria (altas, cobros, impagados y bajas).

MVP procesará en un máximo de 2 días, dichos ficheros implementando los procesos de validación necesarios para garantizar que los datos enviados y los capitales/primas son correctos.

En un máximo de 2 días, en caso de errores, enviará notificación al mediador/distribuidor indicando los registros erróneos con el motivo del error para su corrección y solicitará nuevo envío con los registros corregidos.

En caso de no recibir contestación, cada 5 días y hasta un máximo de 3 recordatorios, reclamará al mediador/distribuidor el envío en el SFTP del fichero corregido. En caso de no recibir contestación, lo notificará al responsable de Negocio, para que realice las acciones necesarias con el mediador/distribuidor.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo de Respuesta	N.º de ficheros procesados en plazo / ficheros recibidos en el mes	Mensual	90%	1
Tiempo de Respuesta de los errores	N.º de comunicaciones de errores en plazo / ficheros de errores generados	Mensual	90%	1

3. Gestión a través de Front-End (Altas)

Los Front-End, para aquellos productos/AM, que así lo contemplen, podrán ser utilizados para la gestión del alta, tanto por MVP, como por los mediadores. El alta a través de Front-End, es muy residual, ya que la gran mayoría de la producción se gestiona a través de ficheros.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo de grabación de la póliza en el Front-End	Tiempo de la grabación entre la recepción del formulario con la documentación requerida y lo que indica la póliza.	Diaria	90%	1

4. Atención telefónica y/o correo (postal o electrónico)

MVP proporcionará un Servicio de atención telefónica, por correo postal o por correo electrónico, a los tomadores/asegurados y beneficiarios para la gestión de sus pólizas y de los siniestros que pudieran derivarse de las mismas:

(a) Información sobre las características del producto y/o pólizas a los clientes.
(b) Envío de duplicados (solo en el caso de que sea CNP quién se encargue de realizar la documentación contractual).
(c) Gestión de modificaciones no económicas.
(d) Gestión de modificaciones económicas.
(e) Gestión de cancelaciones de pólizas.
(f) Gestión de siniestros.

(g) Atención a las consultas, quejas, reclamaciones y derechos de los interesados con relación a la protección de sus datos personales de conformidad con lo establecido en el presente contrato.

Los medios de comunicación habilitados para tal fin serán facilitados por CNP un mes antes del inicio de la prestación de los Servicios y serán los siguientes:

- Teléfono[1].
- Correo electrónico.
- Dirección postal: Calle Cedaceros, 10 - 28014 MADRID

Cualquier documentación recibida por MVP será registrada, archivada y custodiada, en un formato fácilmente recuperable, quedando a disposición de CNP en el momento que esta lo solicite.

Todos los documentos recibidos por MVP serán almacenados teniendo en cuenta las medidas de seguridad correspondientes a la naturaleza de los datos que dichos documentos pudieran contener y siempre teniendo en cuenta lo establecido en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

MVP deberá tener una locución de GDPR para las llamadas entrantes. Asimismo, dispondrá de locuciones de fuera de horario y vacaciones. El contenido de las locuciones será consensuado por ambas partes, antes del inicio de la prestación de servicios.

MVP deberá grabar y almacenar las llamadas atendidas y emitidas en un formato que sea recuperable y las pondrá a disposición de CNP.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo de respuesta	Número de llamadas respondidas en 30 segundos (tras el mensaje de bienvenida) / número total de llamadas respondidas, expresado en valor porcentual.	Mensual	>= 90%	1

[1] La atención telefónica deberá prestarse a través de un teléfono de tarificación gratuita para los clientes.

Ratio de abandono abandonadas tras 30 segundos después del mensaje de bienvenida"	Número de llamadas abandonadas tras 30 segundos (después del mensaje de bienvenida) / número total llamadas recibidas, expresado en valor porcentual.	Mensual	<= 5%	1
Tiempo de disponibilidad de la línea telefónica	Número de horas disponibles por mes / Total de número de horas por mes, expresado en valor porcentual	Mensual	95%	1
Información a facilitar al Cliente	Información correcta y completa facilitada a los Clientes (Auditoría semestral hasta un volumen máximo de 20 llamadas / semestre)	Mensual	100%	1
Correo electrónico, para consultas	Número de correos contestados en 3 días (excluyendo documentación relacionada con siniestros y reclamaciones) / número total de correos recibidos, expresado en valor porcentual	Mensual	>= 90%	1

5. Tarificadores

MVP facilitará los tarificadores de cada producto, utilizados para el cálculo de la prima en el sistema.

A efectos enumerativos no limitativos, se considerarán incidencias, entre otras la siguiente:

(a) No resolución de incidencias del tarificador en tiempo y forma.
(b) No cumplimiento del plazo establecido para actualizaciones o modificaciones del tarificador

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo de respuesta si incidencia en el tarificador	Máximo de 2 días desde la fecha de comunicación de la incidencia	Mensual	100%	1

6. Modificaciones no económicas

El tomador/asegurado podrá realizar modificaciones que no supongan variaciones económicas en su póliza:

Modificaciones no económicas	Teléfono	Correo postal/ electrónico	documentación requerida
Nombre/apellidos (errores ortográficos)	no	sí	NIF en vigor
Sexo	sí	sí	n/a
Estado civil	sí	sí	n/a

Dirección fiscal y postal	sí	sí	n/a
Beneficiarios	no	sí	Comunicación escrita y firmada con copia del NIF en vigor
Teléfono fijo y móvil	sí	sí	n/a
Correo electrónico	sí	sí	n/a
NIE por DNI	no	sí	NIE y DNI en vigor
IBAN	no	sí	Comunicación escrita y firmada con copia del NIF en vigor y justificante de la titularidad bancaria

Las modificaciones no económicas tomarán efecto inmediato. CNP facilitará a MVP un formulario para la solicitud de modificaciones no económicas, antes del inicio de la prestación de servicios.

La solicitud de modificación por parte del tomador podrá llegar por correo electrónico/correo postal o por teléfono a MVP:

(a) Teléfono: La identificación del tomador/asegurado y de la petición se llevará a cabo con la grabación de la llamada y 3 preguntas de seguridad (NIF, fecha de nacimiento, código postal).
(b) Correo postal / correo electrónico: El tomador deberá enviar escrito firmado (nombre completo, DNI y descripción de la petición) y adjuntar la copia del DNI en vigor. En el supuesto de que la documentación enviada sea incompleta o incorrecta, MVP deberá informar el tomador/asegurado y solicitarle la documentación que falta.

Algunas modificaciones en póliza podrían implicar, si el cliente así lo solicita, el envío de un suplemento o certificado, según corresponda, vía correo electrónico al tomador/asegurado, o vía correo postal si así lo requiere de manera expresa el tomador/asegurado y solo en el caso de que sea CNP quién se encargue de realizar la documentación contractual. En caso contrario deberá ser el mediador quién emita dicho suplemento o certificado en cuyo caso MVP se los comunicará a CNP.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo para efectuar la modificación no económica y envío del suplemento si procede	Número de modificaciones no económicas gestionadas como máximo 3 días / número total de modificaciones no económicas recibidas, expresado en valor porcentual	Mensual	>= 90%	1

7. Modificaciones económicas

a) Seguro de Protección de Pagos

Para los seguros vinculados a préstamos, el tomador podrá solicitar un extorno en caso de amortización parcial del préstamo asegurado (efecto inmediato):

(a) Si es una prima única: implicará la devolución o extorno de la parte de la prima no consumida correspondiente a la parte amortizada anticipadamente del préstamo menos el importe correspondiente a los recargos e impuestos satisfechos.
(b) Si es una prima anual: también dará lugar a extorno si la amortización parcial se produce antes de la renovación anual.
(c) Si es una prima mensual: no se realizarán extornos y la siguiente prima mensual se calculará con el nuevo capital pendiente del préstamo asegurado.

Para los Seguros de Protección de Pagos y atendiendo a lo que indique el condicionado en cada caso, el tomador podrá solicitar un extorno total del seguro, tanto en caso de amortización total del préstamo asegurado o por decisión unilateral (efecto inmediato):

(d) Si es una prima única: implicará la devolución o extorno de la parte de la prima no consumida correspondiente menos el importe correspondiente a los recargos e impuestos satisfechos.
(e) Si es una prima anual: también dará lugar a extorno si la amortización se produce antes de la renovación anual.
(f) Si es una prima mensual: no se realizarán extornos y el seguro quedará cancelado al vencimiento de la mensualidad.

Estas peticiones tienen que venir por comunicación escrita y firmada junto con copia del NIF en vigor, justificante de titularidad bancaria si procede abono y justificante de la fecha de la cancelación parcial o total del préstamo si el seguro está vinculado a préstamo y la solicitud es por finalización o desaparición del riesgo. En el caso de amortización parcial deberán informar del saldo antes de la amortización, el capital amortizado y el saldo después de la amortización.

b) GAV

Las peticiones que se indican a continuación tienen que venir por comunicación escrita y firmada junto con copia del NIF en vigor.

(a) Cambio de opción de personal a familiar o viceversa (próxima renovación).
(b) Cambio periodicidad de pago de las primas (próxima renovación).

c) Seguro de Hospitalización

Las peticiones que se indican a continuación tienen que venir por comunicación escrita y firmada junto con copia del NIF en vigor.

(a) Cambio de modalidad y tarifa (Down grade – Próxima renovación).

La solicitud de modificación por parte del tomador/asegurado podrá llegar por correo electrónico/correo postal.

El tomador/asegurado deberá enviar escrito firmado/formulario (nombre completo, DNI y descripción de la petición), adjuntar la copia del DNI en vigor, certificado de amortización del préstamo y justificante de titularidad bancaria, si procede. En el supuesto que la documentación enviada sea incompleta o incorrecta, MVP deberá informar el tomador/asegurado y solicitarle la documentación que falta.

Cualquier modificación en póliza implicará el envío de un suplemento o nuevo certificado, según corresponda, vía correo electrónico con al tomador/asegurado, o vía correo postal si así lo requiere de manera expresa el tomador/asegurado y solo en el caso de que sea CNP quién se encargue de emitir la documentación. En caso contrario deberá ser el mediador quién emita dicho suplemento o certificado en cuyo caso MVP se los comunicará a CNP.

CNP facilitará a MVP un formulario para la solicitud de modificaciones económicas antes del inicio de la prestación de servicios.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo para efectuar la modificación económica y pago del extorno y suplemento (Si corresponde)	Número de modificaciones económicas gestionadas como máximo 3 días / número total de modificaciones económicas recibidas, expresado en valor porcentual	Mensual	>= 90%	2

8. Desistimientos o cancelaciones por decisión unilateral del tomador/asegurado

a) **Seguro de protección de pagos**: efecto inmediato
b) **GAV:** a la renovación
c) **Seguro de hospitalización**: inmediato, tomará efecto fin de la última mensualidad pagada.

El periodo legal de desistimiento de una póliza son 15 días o 30 días, según las condiciones del producto, pero el tomador podrá cancelar la póliza en cualquier momento.

MVP se encargará de realizar las cancelaciones de pólizas solicitadas por los tomadores/asegurados.

En caso de desistimiento se solicitará la devolución de la prima cobrada y una vez recibida, se procederá a la cancelación del seguro sin efecto.

En caso de solicitud de cancelación una vez ha transcurrido el periodo de desistimiento y dependiendo de la forma de pago del seguro el tomador podrá tener derecho a la devolución o extorno de prima:

(a) Si es una prima única: implicará la devolución o extorno de la parte de la prima no consumida menos el importe correspondiente a los recargos e impuestos satisfechos.
(b) Si es una prima anual: también dará lugar a extorno si la solicitud se produce antes de la renovación

anual (mínimo 1 mes antes)

(c) Si es una prima mensual: no se realizarán extornos.

La petición de modificación por parte del tomador podrá llegar por correo electrónico/correo postal:

Correo electrónico/correo postal: El tomador deberá enviar escrito firmado solicitando la cancelación junto con la copia del DNI en vigor (Si da lugar a extorno, se debe solicitar siempre justificante de titularidad bancaria). En el supuesto que la documentación enviada sea incompleta o incorrecta, MVP lo comunicará al tomador y le solicitará la documentación que falta.

MVP enviará al tomador comunicación de la cancelación de la póliza a través de correo electrónico o correo postal si el tomador así lo indica, indicando en la misma, si así fuera el caso, el importe de abono del extorno y el plazo para dicho abono.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo para efectuar desistimiento/cancelación (sin extorno)	Número de cancelaciones gestionadas como máximo 3 días / número total de solicitud de cancelación recibidas, expresado en valor porcentual	Mensual	>= 90%	1
Tiempo para efectuar desistimiento/cancelación y pago del extorno	Número de cancelaciones con extorno gestionadas como máximo 3 días / número total de solicitud de cancelación con extorno recibidas, expresado en valor porcentual	Mensual	>= 90%	2

No se podrá realizar solicitud de cancelación, cuando estas sean enviadas por el tomador/asegurado por correo electrónico o postal, sin la petición firmada y sin la documentación obligatoria requerida en cada caso.

9. Gestión de cobros/impagados

MVP generará automáticamente un proceso diario de cobros/recobros/renovaciones a través de la generación de ficheros de cobros (formato estándar SEPA), para todos aquellos productos que no se gestionen por ficheros de producción.

En caso de primer impago, la cobertura del tomador/asegurado queda suspendida temporalmente y MVP enviará al mediador/distribuidor y al tomador/asegurado comunicación del impago de la prima a través de correo electrónico informando del primer impago.

En caso de falta de pago de una de las primas siguientes, la cobertura del tomador queda suspendida temporalmente y en el caso de falta de pago de un segundo intento de cobro, la póliza quedará finalizada

por el impago consecutivo de la prima. MVP enviará al tomador/asegurado comunicación de cancelación de su póliza por impago consecutivo de la prima.

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío diario de los ficheros sin incidencias	Número de ficheros enviados sin incidencias / número total de ficheros enviados	Mensual	>= 90%	1
Tiempo de envío de las comunicaciones de impago/ cancelaciones	Número de comunicaciones enviadas en plazo / número total de comunicaciones enviadas	Mensual	>= 90%	1

10. Renovaciones

Las renovaciones de las pólizas se realizan de forma anual en cada aniversario de la póliza.

MVP, con dos meses de antelación, deberá comunicar a los tomadores la renovación de su póliza e informar de la nueva prima a pagar. Dicha comunicación se realizará a través de correo electrónico o a través de correo postal.

Los indicadores para medir el nivel de cumplimiento del presente Servicio será el que se indica a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío comunicación de renovación	Número total de comunicados enviados a los tomadores en plazo / número total de renovaciones mensuales, expresado en valor porcentual	Mensual	100%	1

11. Gestión de los siniestros

MVP realizará en nombre de CNP la gestión integral de los siniestros que pudieran derivarse, hasta su correcta liquidación y cierre:

(a) Atención telefónica, vía correo electrónico o por correo postal.
(b) Información del producto y sus coberturas.
(c) Declaración, tramitación y pago de los siniestros.
(d) Provisión de los siniestros.
(e) Comunicación de apertura del siniestro al tomador y/o beneficiario.
(f) Información sobre el estado de tramitación del siniestro.
(g) Control contra listas de los Asegurados/beneficiarios antes del pago del siniestro.
(h) Atención de quejas y reclamaciones.
(i) Escaneo, archivo y custodia de la documentación cumpliendo con las medidas de seguridad para la protección de los datos personales.
(j) Almacenamiento de ficheros de comunicación.

(k) Informes periódicos de acuerdo con los formatos estándar de MVP.
(l) Información *ad hoc* a CNP o a las autoridades competentes que CNP requiera.
(m) Gestión de los profesionales pertinentes: investigación médica, asesoramiento legal, etc.
(n) Realizar todas las comprobaciones de diligencia debida del cliente y cualquier otra comprobación necesaria en relación con el pago de los importes de los siniestros a los beneficiarios (herederos en el caso de un siniestro de vida o el beneficiario individual en relación con otros siniestros), incluidos, en su caso, los requisitos de lucha contra el blanqueo de capitales (AML) en virtud de la legislación y las políticas de CNP, según proceda.

MVP dispondrá de controles para vigilar la gestión de los siniestros con el fin de detectar a tiempo las conductas que constituyan o puedan constituir un fraude por parte de un cliente en relación con un siniestro e informará inmediatamente a CNP por correo electrónico relacionando datos del asegurado/beneficiarios, producto/A.M., siniestros y describiendo la conducta detectada.

La gestión de los siniestros se realizará siempre a través del departamento de siniestros de MVP y a través de la herramienta MVP CLAIMS, permitiendo a los usuarios que CNP designe, realizar consultas de los siniestros.

El tomador/asegurado o beneficiario se pondrán en contacto con MVP para declarar un siniestro. La comunicación podrá llegar también a través del mediador.

MVP incluirá el número del expediente del siniestro abierto en el asunto de todos los correos electrónicos enviados.

MVP enviará, correo electrónico, al beneficiario informando la documentación necesaria (que consta en la póliza según el producto comercializado) para la gestión del siniestro.

Dicha documentación es variable según Producto/A.M./Garantía.

CNP entregará a MVP la documentación a solicitar según corresponda, antes del comienzo de la prestación de servicios.

Si fuera procedente el rechazo de un siniestro con posterioridad a haberse efectuado pagos con cargo al mismo, el Asegurador podrá reclamar a su elección contra el Asegurado o el Beneficiario por las sumas indebidamente satisfechas más los intereses legales que correspondan. En ese caso MVP se pondrá en contacto en CNP informando de la incidencia y solicitando instrucciones para su resolución.

El pago de la Prestación sólo se llevará a cabo una vez que se haya recibido la documentación y las pruebas requeridas, por parte del Asegurado o el Beneficiario. En caso de que no se recibiese dicha documentación, el Asegurador no estará obligado a pagar Prestación alguna.

Una vez que se hayan recibido las pertinentes pruebas de que el Asegurado/Beneficiario se halla en alguna de las situaciones fijadas en la póliza, se pagará la suma asegurada en los términos y límites establecida en la misma y sin perjuicio de que el Asegurado pueda iniciar el procedimiento de reclamación desde el momento en que se encuentre en alguna de las contingencias previstas en la póliza.

Toda la documentación a solicitar al Asegurado/Beneficiario para la declaración y tramitación del seguro, se adecuará a la documentación indicada en la póliza de cada producto.

MVP procederá a la declaración del expediente en un máximo de 2 días desde la recepción de la comunicación, comprobando todos los datos personales, de dirección fiscal/postal, teléfonos y correo electrónico de contacto y recabando la mayor información posible. Tras la declaración del expediente, enviará la carta de solicitud de documentación necesaria para el trámite del expediente.

Si en el plazo de 30 días naturales no recibe documentación alguna, procederá a enviar una carta recordatoria, denominada AVISO. Si en el plazo de otros 30 días naturales se sigue sin recibir documentación, procederá a enviar una nueva carta de aviso y si a los siguientes 30 días naturales, sigue sin recibir documentación, procederá al cierre administrativo del expediente, sin perjuicio de que pueda ser activado en cualquier momento teniendo en cuenta los plazos legales de prescripción (2 años para desempleo y 5 años para el resto de las coberturas).

Una vez recibida la documentación, MVP procederá a realizar el análisis del expediente en un plazo máximo de 5 días. Tras el análisis pueden darse las siguientes situaciones:

- **Falta documentación**: MVP emite comunicación solicitando la documentación pendiente;
- **Se rechaza:** No cumple con las condiciones del seguro. MVP emite comunicación de rechazo;
- **Se acepta:** Cumple con los requisitos del Seguro. En su caso, MVP enviará la carta de aceptación y en caso de fallecimiento, si procede, emitirá una certificación para que el/los beneficiario/s tributen el Impuesto de Sucesiones y Donaciones (ISD). Además, si procediera, realizará el pago correspondiente.

MVP, en el caso de fallecimiento con ISD, quedará a la espera del envío de la justificación acreditativa del pago del ISD correspondiente para realizar el pago y finalizar el trámite del siniestro.

En el caso de pagos recurrentes, MVP quedará a la espera de recibir la documentación justificativa solicitada en la aceptación y realizará dichos pagos a medida que vayan justificando el mantenimiento de la situación declarada y solicitada según los plazos indicados en las pólizas.

Ante de realizar cualquier pago se deberá efectuar comprobación contra listas de PEP/SIP (Sancionados/Terroristas/e información adversa...) de el/los beneficiario/s que reciben el pago de la prestación.

En el supuesto que el/los Beneficiario/s diera positivo contra listas, antes del pago del siniestro, se deberá informar con carácter inmediato a la UPBC de CNP a la siguiente dirección de correo: mailto:upbc@cnp.es. La UPBC de CNP una vez revisado comunicará a MVP en el plazo máximo de 24 horas, si se procede al pago o si es necesario cualquier tipo de documentación adicional.

MVP enviará las órdenes de pago en un máximo de 3 días, una vez que se ha recibido toda la documentación requerida y generando el fichero de pago correspondiente y enviándolo a la depositaria de CNP a la cuenta bancaria que figura a continuación.

Banco: **CECABANK, S.A.**
IBAN: **ES69 2000 0002 21 8800351910**
Divisa / Currency : EUR / EURO
Swift-Code: **CECAESMM**

Normas de delegación:

CNP establece las siguientes normas de delegación para el pago de siniestros:

- Importes de prestación hasta 25.000€, MVP podrá aceptar y realizar pagos de siniestro.
- Importes de prestación a partir de 25.001€, MVP deberá solicitar la aceptación y autorización de pago a CNP enviado toda la documentación del expediente a la dirección de correo electrónico operaciones@cnp

MVP pondrá a disposición de CNP toda la documentación/información para la consulta de todos los procesos de siniestros y soporte para la toma de decisión de aquellos siniestros que estén fuera de las normas de delegación.

CNP tendrá acceso de consulta a la plataforma de MVP.

La forma y contenido de las comunicaciones por escrito con el tomador serán el estándar de MVP.

MVP enviará mensualmente un fichero a CNP con la información de todos los siniestros, declarados, tramitados y pagados, así como con la información de provisiones y pagos para su contabilización.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo para la apertura de un siniestro (siniestros declarados sin documentación)	Número de siniestros abiertos como máximo 2 días / número total de siniestros comunicados, expresado en valor porcentual	Mensual	>= 90%	1
Tiempo para la tramitación de un siniestro (incluyendo la comunicación de aceptación, petición de documentación pendiente, rechazo)	Número de tramitaciones en máximo 5 días / número total de tramitaciones, expresado en valor porcentual	Mensual	>= 90%	1
Tiempo para el pago de un siniestro (3 días desde la fecha de aceptación)	Generación del fichero de pagos realizado en máximo 3 días desde la fecha de aceptación /número total de pagos	Mensual	>= 90%	1

12. Gestión, guarda y custodia de documentación

MVP realizará la guarda y custodia de la documentación en un periodo que dure la prestación de servicios y que se acuerde por contrato.

TIPO	Nombre
Correo electrónico	Correo electrónico Modificación económica
Correo electrónico	Correo electrónico Modificación no-económica
Correo electrónico	Correo electrónico Impago
Correo electrónico	Correo electrónico Carta cancelación por impago
Correo electrónico	Correo electrónico carta cancelación
Correo electrónico	Carta de comisiones al mediador I
PDF	Carta de bienvenida (nuevas altas)
PDF	Nota informativa
PDF	Nota informativa mediador
PDF	Condicionado
PDF	Mandato SEPA
PDF	Carta de cancelación impago
PDF	Carta de cancelación
PDF	Carta de impago
PDF	Carta de modificación + suplemento si procede
PDF/Correo electrónico	Carta de Declaración del siniestro
PDF/Correo electrónico	Carta de Tramitación del siniestro
PDF/Correo electrónico	Carta de Aceptación del Siniestro/ISD (si fuera necesario)
PDF/Correo electrónico	Carta de Rechazo del Siniestro
PDF/Correo electrónico	Comunicación del pago del siniestro

MVP tendrá disponible, la documentación indicada anteriormente, para facilitarla a CNP, cuando sea requerida y en un periodo máximo de 2 días.

13. Gestión de quejas y reclamaciones

13.1) Quejas y reclamaciones presentadas ante el SAC:

A los efectos de la presente cláusula, a continuación, se establece la definición de queja y reclamación de conformidad con el Reglamento de Defensa del Cliente aplicable en CNP. Se entenderá por cliente los asegurados, tomadores, beneficiarios o cualquier tercero con un interés legítimo en cualquiera de los productos contratados con CNP.

Quejas:

Se entienden por quejas las manifestaciones de los clientes, referidas al funcionamiento de los servicios financieros, tales como demoras, desatenciones, y cualesquiera otras manifestaciones, con relación a

intereses y derechos legalmente reconocidos, ya se deriven de los contratos, de la normativa de transparencia y protección de la clientela, del incumplimiento de las buenas prácticas y usos financieros, y en particular del principio de equidad.

Reclamaciones:

Son reclamaciones las que pongan de manifiesto la pretensión del cliente de obtener la restitución de un interés o derecho con relación a intereses y derechos legalmente reconocidos, ya se deriven de los contratos, de la normativa de transparencia y protección de la clientela, del incumplimiento de las buenas prácticas y usos financieros, y en particular del principio de equidad.

MVP será responsable del control, tramitación y respuesta de aquellas quejas y reclamaciones que sean presentadas por actuaciones realizadas por la entidad, cuando éstas se interpongan a través del Área de Protección al Cliente de CNP. La gestión de reclamaciones y quejas se someten a las siguientes reglas de procesamiento:

i. MVP llevará a cabo la gestión y tramitación cumpliendo, en todo momento, con el Reglamento de Protección del Cliente de CNP y con especial atención a los plazos de respuesta establecidos en el mismo y reglas de tratamiento de las reclamaciones. La información mínima requerida para la gestión de la reclamación es la siguiente:

   - Datos personales del Cliente;
   - Datos de contacto;
   - Datos de contrato del Seguro y;
   - En el caso de siniestro, datos del siniestro, así como la documentación recibida.

ii. MVP llevará a cabo la recepción y control de la queja o reclamación y enviará a CNP en el plazo máximo de 3 días el borrador del escrito de acuse de recibo y apertura de expediente que CNP enviará al cliente;

iii. MVP deberá preparar el borrador de carta respuesta al cliente acompañado de toda la documentación que sirva de justificación a dicho expediente y enviarlo al responsable del Área de Protección al Cliente de CNP, en un plazo máximo de 12 días desde la recepción de la reclamación o queja. CNP enviará a MVP una copia de la resolución enviada al cliente, para poder llevar un control sobre este extremo.

iv. Ninguna documentación o correspondencia puede ser eliminada / destruida excepto bajo la instrucción expresa por escrito de CNP.

Sistema de reporte: MVP facilitará un informe mensual a través de un fichero Excel los primeros 7 días del mes con respecto al mes anterior, y una memoria anual, que deberá estar disponible para CNP en un plazo de 15 días desde el 31 de diciembre de cada año, en los que se incluirá como mínimo la siguiente información:

   - Resumen anual de las gestiones de quejas y reclamaciones;
   - Número de quejas y reclamaciones;

- Causas de las quejas y reclamaciones;
- Tipos de resolución de expedientes: aceptados, rechazados;
- Quejas y Reclamaciones pendientes;
- Importe por reclamación estimado y pagado si este importe es conocido por MVP;
- Provincia y código postal del reclamante;
- Cualquier otra información relevante.

MVP no tramitará aquellas reclamaciones que se reciban a través del Defensor de Asegurado u otras entidades públicas, debiendo remitir, en un plazo máximo de 2 días desde su recepción, a CNP dichas reclamaciones junto con toda la documentación necesaria para que sean gestionadas de forma directa por CNP a la siguiente dirección de correo electrónico protecciondelcliente@cnp.es

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Respuesta a cliente por apertura de las reclamaciones	Número de reclamaciones recibidas / número de comunicaciones de apertura de expediente enviadas al cliente en 3 días desde la recepción	Mensual	100%	2
Propuesta de respuesta a Área de Protección del cliente y comunicación de las reclamaciones	Propuestas de respuesta enviadas en 12 días a Área de Protección del cliente / número de reclamaciones recibidas	Mensual	100%	1
Reclamaciones de Defensor del cliente/otros organismos	Número de reclamaciones enviadas a CNP en plazo máximo de dos días desde su recepción	Mensual	100%	2

13.2) Quejas y reclamaciones presentadas ante la DGSFP:

MVP no tramitará aquellas quejas y reclamaciones que se reciban a través de la Dirección General de Seguros y Fondos de Pensiones (DGSFP) u otras entidades públicas que en el futuro pudieran sustituirla. En este sentido, CNP informará a MVP de la entrada de las reclamaciones interpuestas ante la DGSFP que correspondan y MVP enviará, en un plazo máximo de 3 días desde que CNP le haya notificado la reclamación, toda la documentación necesaria que obre en poder de MVP para que la reclamación sea gestionada de forma directa por CNP, a la siguiente dirección de correo electrónico: protecciondelcliente@cnp.es

En caso de que CNP lo requiera, junto con la documentación que MVP envíe, ésta podrá indicar a CNP su criterio para resolver la reclamación.

13.3) Quejas y reclamaciones judiciales (demandas):

El Proveedor se compromete al envío de toda aquella información y documentación de la que el Proveedor disponga y que sea necesaria para que CNP pueda dar trámite al expediente judicial.

Dicho envío de información y/o documentación será realizado por el Proveedor en un plazo máximo de 3 días, desde que CNP se la requirió. No obstante lo anterior, si hubiera documentación que por su naturaleza no pudiera entregarse por MVP en el plazo de 3 días, MVP dispondrá de hasta 5 días para recabar dicha documentación.

En este sentido, si la solicitud de documentación estuviera compuesta de varios documentos y algunos pudieran adelantarse en el plazo de 3 días, MVP enviará aquellos de los que ya dispusiera en dicho plazo y dispondrá de un plazo adicional de 2 días adicionales para recabar aquellos documentos que por cuestiones ajenas a MVP, no pudieran haberse recabado en el citado plazo de 3 días.

La documentación deberá ser enviada a la siguiente dirección de correo electrónico: legal@cnp.es

13.4) Otros:

Si por cualquier motivo se recibiera en el Proveedor alguna queja y/o reclamación correspondiente a la cartera de CNP y dicha reclamación no se encuentre enmarcada en ninguno de los supuestos anteriores, el Proveedor procederá a su envío a CNP a la mayor brevedad posible, y nunca en un plazo superior a 3 días, para que CNP pueda darle el trámite que corresponda.

14. Gestión y registro Ministerio de Justicia (garantía de fallecimiento)

Semanalmente MVP generará el fichero o ficheros necesarios a enviar al Registro del Ministerio de Justicia. El fichero contendrá nuevas altas, modificaciones y bajas de pólizas y los depositará a través del SFTP establecido con CNP.

CNP firmará digitalmente los mismos y los enviará a través de la Web del Ministerio de Justicia.

Una vez enviados y validados por parte de CNP, si hay errores, debe descargar el fichero de errores y enviarlo a MVP para su análisis y modificación. De este modo, MVP realizará una nueva generación de fichero enviándolo en D+5 días para que dichos errores sean procesados correctamente.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío a CNP del fichero con el formato y los registro que son necesarios enviar al Ministerio de Justicia de forma semanal	Número de ficheros enviados en plazo / total de ficheros generados	Mensual	100%	1
Gestión de errores	Número de errores corregidos D+5 / total de errores recibidos	Mensual	100%	1

15. Gestión y reporte ficheros EIAC

MVP extrae de su back-end información en formato XML (estándar EIAC) de pólizas, recibos, comisiones y siniestros, y lo envía a CNP vía SFTP para que proceda a enviar el EIAC, por cada mediador que así lo requiera.

- **Periodicidad:** diaria
- La **validación** (estructura y tipos de datos) de los ficheros EIAC (ficheros XML) se realiza contra el **XSD** definido por el propio estándar EIAC.

Los indicadores para medir el nivel de cumplimiento del presente servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío diario fichero EIAC, en el caso que el distribuidor lo requiera	Envío por parte de MVP de los ficheros EIAC en D+1	Diaria	95%	1

16. Ejercicio de derechos de protección de datos personales

Si MVP recibiera por escrito, alguna solicitud de ejercitar sus derechos de Acceso, Rectificación, Cancelación, Limitación, Portabilidad, Supresión, Oposición o Derecho al Olvido y de no ser objeto de decisiones individualizadas, deberá remitir dicha solicitud en un plazo máximo de 2 Días siguientes a la recepción de la solicitud por correo electrónico a la dirección: gdpr.es.peticion@cnp.es

Cuando el cliente realice esta petición de forma telefónica, MVP deberá infórmale de que para poder tramitar correctamente su solicitud debe dirigirse o bien por escrito a la dirección postal de CNP, o bien a la dirección de correo electrónico: gdpr.es.peticion@cnp.es

MVP enviará a CNP, en un plazo máximo de 5 días, toda la información necesaria de la que el Proveedor disponga para que tramite la petición del interesado. Se entenderá por información necesaria para la tramitación de las solicitudes, tanto la petición del interesado como los datos derivados de la relación contractual, así como cualquier otra necesaria para la tramitación de la solicitud.

Finalmente, si la solicitud de ejercicio de los derechos mencionados anteriormente se recibiera en primer lugar en CNP, MVP dispondrá de un plazo máximo de 5 días para enviar a CNP toda la información y/o documentación que obrara en su poder, desde la recepción de la notificación por parte de CNP.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Tiempo de remisión de las solicitudes de rectificación, cancelación y oposición	Cumplimiento del porcentaje 100% de envío en 2 días	Mensual	100%	1
Número de solicitudes enviadas con la información necesaria	Cumplimiento del porcentaje 100% de las solicitudes recibidas	Mensual	100%	1

17. Prevención blanqueo de capitales y de la financiación del terrorismo (PBC/FT)

Dependerá de la recepción de la información:

17.1) Vía fichero

Para productos de Riesgo de Vida y No Vida, como mínimo de manera mensual, se realizará un proceso para el control de las listas de toda la cartera, para la detección de posibles sancionados. Los ficheros resultantes de estas comprobaciones se enviarán a CNP en la siguiente dirección de correo: upbc@cnp.es en el plazo máximo de un mes, en el formato acordado, por las partes.

Para los productos de Vida Riesgo, se realizará como mínimo de manera semestral (diciembre/Junio año en curso), un proceso para el control de las listas del total de la cartera, para la detección de posibles PEP´s. Los ficheros resultantes de estas comprobaciones se enviarán a CNP en la siguiente dirección de correo: upbc@cnp.es el plazo máximo en un plazo de **seis meses**, en el formato acordado, por ambas Partes.

17.2) Vía Front-End

Para productos de Vida Riesgo, en el supuesto que las altas se realizarán vía front-end, deberá estar implementada los bloqueos contra listas para la detección de posibles PEP/SIP (Sancionados/Terroristas/ e información adversa...)

En el supuesto que el tomador/asegurado fuera positivo contra listas, antes de la grabación del alta, se deberá informar con carácter inmediato a la UPBC de CNP en la siguiente dirección de correo: upbc@cnp.es. La UPBC de CNP una vez revisado, informará a MVP en el plazo máximo de 24 horas, si se procede a la contratación o si es necesario documentación adicional o un análisis más exhaustivo por

parte de CNP. En el caso que se decida la no contratación CNP se pondrá en contacto con el distribuidor, para su información.

Los indicadores para medir el nivel de cumplimiento del presente servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Identificación de siniestros. PEP/SIP(Sancionados/Terroristas/ e información adversa...) para su aprobación previa.	Número de clientes positivos comunicados en 1 día / Número total de clientes Positivos detectados.	Mensual	100%	1
Siniestros: Nº pagos realizados Altas: Nº de contrataciones realizadas.	Número de pagos realizados / número total de comprobaciones contra listas. Número de altas realizadas / número total de comprobaciones contra listas.	Mensual	100%	2
Fichero mensual y semestral. Controles de la cartera contra listas	Envío en el periodo establecido la información de clientes positivos	Mensual/semestral	95%	2

18. Gestión de comisiones

MVP enviará, un mes antes a la fecha del inicio de este Contrato, la documentación con el proceso de comisiones a seguir, con cada una de las entidades.

MVP enviará los ficheros que se relacionan a continuación, en el tercer día de M+1.

- **Productos PPI Y GAV:**
  - 2.14: movimientos de pólizas
- **Producto TAR:**
  - Comisiones

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío de los ficheros necesarios para realizar la gestión de comisiones	Cumplimiento del porcentaje 100% de envío en el tercer día de M+1	Mensual	100%	1

19. Gestión de apuntes contables

MVP enviará los ficheros, que se relacionan a continuación, con la información necesaria para la realización por parte de CNP de los asientos contables, en el tercer día de M+1.

- **Productos PPI Y GAV:**
  - 6.2: provisiones y movimientos económicos de primas acumulados.

- **Producto TAR:**
  - Accounting: movimientos de pólizas.
  - Provisiones: desglosadas por póliza.
  - Provisiones: acumuladas por AM.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío de los ficheros necesarios para realizar la gestión de apuntes contables	Cumplimiento del porcentaje 100%, en el tercer día de M+1.	Mensual	100%	2

20. Gestión modelos fiscales

20.1) Reportar al CONSORCIO y LEA

MVP enviará de manera mensual en D+10 el fichero a CNP, con el formato de registros definidos por el consorcio y para cada una de las sociedades que componen CNP.

20.2) Reportar a la AEAT, en el supuesto que existan retenciones sobre productos de Riesgo.

- MVP enviará de manera mensual en D+10 el fichero con retenciones y bases imponibles a declarar, por cada una de las sociedades que componen CNP.
- MVP enviará de manera anual como máximo el 20 de enero de A+1 el fichero con la información detalla del modelo 188, por cada una de las sociedades que componen CNP.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío de los ficheros necesarios para realizar la gestión por parte de CNP del reporte al Consorcio y LEA	Cumplimiento del porcentaje 100% de envío en D+10	Mensual	100%	2
Envío del fichero con retenciones y bases imponibles a declarar, por cada una de las sociedades que componen CNP	Cumplimiento del porcentaje 100% de envío en D+10	Mensual	100%	1
Envío de fichero con la información detallada del modelo 188, por cada una de las sociedades que componen CNP	Cumplimiento del porcentaje 100% de envío como máximo el 20 de enero de A+1	Anual	100%	1

21. Informes de Actuarial

MVP enviará los siguientes ficheros con la información necesaria para la realización de las tareas por parte de CNP en los plazos que a continuación se detallan:

21.1) Reaseguro

Envío desde MVP a CNP como máximo el quinto día de M+1 de los siguientes ficheros:

- Reaseguro_Promotoras_bajas_altas_suplementos_fich.autom.xls;
- Reaseguro_Santander Renting_Certs.activos_2.15.(uno por cada AM); Reaseguro_Santander Renting_Primas_2.14 (uno por cada AM); Reaseguro_Santander Renting_Siniestros_Operaciones;
- Reaseguro_Renting Finders_Certs.activos_2.15 (uno por cada AM); Reaseguro_Renting Finders_primas_2.14(uno por cada AM); Reaseguro_Renting Finders_Siniestros_Operaciones;
- Reaseguro_GAV_Primas_2.14 (uno por cada AM); Reaseguro_GAV_Siniestros._Operaciones.

21.2) Solvencia II

Envío desde MVP a CNP como máximo el quinto día de M+1 de los siguientes ficheros:

- Fichero Prophet para productos 20 (PPI Vida), 22 (PPI No Vida) y 60 (GAV).
  El producto 61 TAR No Vida no está incluido en este envío ya que no está modelizado por MVP en Prophet.
- Fichero de número de pólizas y asegurados en vigor a una fecha (para productos 20,22,60).
- BEL de siniestros: los ficheros input para que CNP pueda realizar la BEL de siniestros serán los informes de siniestros enviados por Operaciones.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío de los ficheros necesarios para realizar la gestión por parte de CNP del Reaseguro	Cumplimiento del porcentaje 100% de envío en el quinto día de M+1	Mensual	100%	2
Envío de los ficheros necesarios para realizar la gestión por parte de CNP de Solvencia II	Cumplimiento del porcentaje 100% de envío en el quinto día de M+1	Mensual	100%	1

22. Gestión documentación contractual

Toda la documentación contractual, que obra en poder de MVP, tanto en formato físico como electrónico, de la cartera cedida a CNP, será entregada por MVP en el momento de la fecha de cierre de la operación de cesión de cartera. A partir de dicha fecha, MVP cuando sea preciso, podrá reclamar la documentación necesaria, para cumplir con la prestación de Servicios.

23. Servicios adicionales

Con la periodicidad establecida MVP enviará a CNP, los ficheros debidamente cumplimentados para que CNP los remita a los proveedores, en las fechas establecidas.

Los indicadores para medir el nivel de cumplimiento del presente Servicio serán los que se indican a continuación:

Indicador	Cálculo	Periodicidad	Valor Objetivo	Punto penalización por incumplimiento SLA
Envío de los ficheros necesarios para realizar la gestión de los servicios adicionales	Cumplimiento del porcentaje 100%, en el periodo establecido por cada uno de los ficheros	Mensual	100%	1

24. Informes periódicos

MVP enviará de manera mensual el informe de SLA agrupado con los siguientes indicadores de calidad:

- Atención telefónica
- Atención por correo (postal o electrónico)
- Cobros/Impagados
- Modificaciones no económicas
- Modificaciones económicas
- Cancelaciones
- Renovaciones
- Siniestros
- Quejas y Reclamaciones
- Ejercicio de derechos de protección de datos personales

- Blanqueo de Capitales y Financiación del Terrorismo (PBC-FT)
- Ficheros comisiones
- Ficheros para la gestión contable
- Consorcio y LEA
- Informes actuariales

Los informes periódicos serán enviados en un plazo máximo de 6 días del M+1.

Todo el intercambio de información se realizará vía SFTP.

IV. Incumplimiento de SLA's

En caso de incumplimiento de los niveles de servicios se aplicará la penalización correspondiente.

El resultado de la suma de las eventuales penalizaciones individuales de servicio se traduce en el porcentaje de descuento a aplicar a la facturación mensual siguiendo la siguiente tabla:

(a) Si la suma de puntos de penalización es inferior o igual a 5 → No se aplicará penalización alguna.
(b) Si la suma de puntos de penalización está entre 6 y 10 → Se aplicará un 5% de penalización sobre el importe de la facturación mensual.
(c) Si la suma de puntos de penalización está entre 11 y 15 → Se aplicará un 15% de penalización sobre el importe de la facturación mensual.
(d) Si la suma de puntos de penalización es superior a 15 → Se aplicará un 25% de penalización sobre el importe de la facturación mensual.

Si alguno de los indicadores marcados con 2 puntos de penalización se incumpliera durante 3 meses seguidos se deberá presentar en el próximo *Management Meeting,* donde se decidirá si se aplica un 5% de penalización sobre la facturación por cada indicador incumplido.

V. Sistemas de gestión utilizados por MVP

(a) Herramienta de Back-Office MVP: sin acceso por parte de CNP.
(b) Plataforma gestión de Siniestros: MVP CLAIMS. Acceso a sólo consultas por los partes de los usuarios designados por CNP.
(c) Plataforma Reclamaciones: Sharepoint, sin acceso por parte de CNP.
(d) Front-End: Sin acceso por parte de CNP.

Annex 5.1
Fees

From the effective date of this Agreement until the end of the third (3rd) calendar month of this Agreement, the Fees to be paid by the Assignees to the Service Provider shall be € 50,000 per month plus the applicable Value Added Tax.

From the fourth (4th) calendar month of the term of the Agreement, inclusive, and up until the maximum Term, the **amount of the Fees corresponding to a given month ("**month "n"**") to be paid by the Assignees to the Service Provider pursuant to Clause** 5 **shall be the** amount in euros resulting from the following formula:

Fees accrued during month"n" = 15% gross written premiums during month "n" + 15% (Initial PPNC – Final PPNC), where:

"**PPNC**" shall be the unearned premium reserve (Provisión de Primas no Consumidas).

"**Initial PPNC**" shall be the PPNC existing on the first day of month "n".

"**Final PPNC**" shall be the PPNC existing on the last day of month "n".

For the purposes of the formula:

1. The gross written premiums and PPNC to be taken into account for the calculation of the Fees shall be those of PPI policies in respect of which MVP is providing the Services in each given month.

2. To the Fees so calculated shall be added any taxes to be charged thereon (including, in particular, Value Added Tax).

Annex 6.4(c)
Security

The Parties agree to execute the Security Annex in Spanish, with the terms and conditions set forth hereto:

1 INTRODUCCIÓN

MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS, S.A. (en adelante "**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.

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 de CNP ASSURANCES SUCURSAL EN ESPAÑA y CNP CAUTION SUCURSAL EN ESPAÑA (en adelante, "**CNP**"); incluida la Información Confidencial de CNP.
- toda información relativa a CNP.
- cualquier otra información utilizada en la prestación de los Servicios;
- los sistemas informáticos de CNP y de PROVEEDOR (incluidos los Sistemas de PROVEEDOR) que procesen, almacenen o transmitan información; y
- el código informático utilizado para procesar Datos de CNP incluida la Información Confidencial de CNP.

2 FUNCIONES Y RESPONSABILIDADES

2.1 Cumplimiento

Se establecerán reuniones de seguimiento para comprobar el cumplimiento de sus obligaciones establecidas en el presente contrato de forma trimestral. En las reuniones se definirán indicadores de rendimiento que deben ser mantenidos y actualizados por PROVEEDOR en la periodicidad definida por CNP para medir el estado de la seguridad de PROVEEDOR.

Sin perjuicio de las demás acciones y vías de reparación a las que pueda recurrir a CNP, todo incumplimiento comunicado por PROVEEDOR a CNP, dará lugar a una valoración del riesgo por parte de CNP que indicará a PROVEEDOR el plazo de tiempo del que dispondrá para poner en práctica las medidas correctoras que resulten necesarias.

2.2 Personal de PROVEEDOR

PROVEEDOR definirá claramente las funciones y responsabilidades del Personal de 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 de PROVEEDOR.

PROVEEDOR deberá revisar y actualizar la segregación de funciones dentro del procedimiento de gestión de identidades, con la periodicidad que establezca CNP. De esta manera, se garantizará que cualquier tipo de usuario acceda únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

La actividad de todo el Personal de PROVEEDOR que trabaje en los locales de CNP podrá ser supervisada por CNP.

PROVEEDOR se asegurará de que todos los miembros del Personal de PROVEEDOR 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.

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

2.3 Educación, Formación y Sensibilización

El PROVEEDOR llevará a cabo formación periódica en materia de Ciberseguridad, que se basará en los siguientes aspectos:

- Conocimiento de los empleados del PROVEEDOR de la Política de Seguridad del PROVEEDOR.
- Campañas formativas en diferentes formatos (vídeo, texto, etc.)
- Ejercicios de concienciación para los empleados.

Esta formación tendrá como objetivo dotar a los empleados de los conocimientos básicos de Ciberseguridad para evitar un mal uso de las herramientas tecnológicas y prevenir, de ese modo, una afectación negativa en la confidencialidad de la información.

2.4 Responsable de Seguridad

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

El Responsable de Seguridad de PROVEEDOR deberá:

- tener conocimientos sobre asuntos relacionados con la Seguridad de la Información;
- ser capaz de responder a consultas de CNP en materia de Seguridad de la información;
- asegurarse de que 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 de CNP en cuestiones relacionadas con la seguridad.

3 INCIDENTES DE SEGURIDAD

3.1 Notificación de Eventos e Incidentes de Seguridad

Si un Incidente de Seguridad real que afecte a los Sistemas de PROVEEDOR ha provocado, un acceso no autorizado a los Datos de CNP, a la Información Confidencial de CNP a los Sistemas de CNP o a los Sistemas de PROVEEDOR utilizados por PROVEEDOR, por CNP o por sus Agentes, o la revelación de éstos, o pudiera tener un efecto negativo sustancial sobre los mismos, PROVEEDOR realizará todos los esfuerzos razonables para informar inmediatamente CNP de dicho Incidente de Seguridad real, quedando en todo caso obligado a realizar dicha notificación dentro de las **12 horas laborables** siguientes al momento en que PROVEEDOR hubiese tenido conocimiento de dicho Incidente de Seguridad o, en su caso, en plazo legal inferior, y asistirá y cooperará con CNP en lo relativo a cualquier comunicación necesaria a terceros y otras medidas razonables para remediar la situación que solicite CNP o sean exigibles por ley.

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 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 PROVEEDOR para subsanar los efectos del Incidente de Seguridad

A modo meramente ejemplificativo, PROVEEDOR deberá notificar a CNP las incidencias que se produzcan relacionadas con los siguientes eventos:

- Accesos o intentos de acceso a sistemas, equipos, aplicaciones, ficheros, contenedores, dispositivos, etc. por parte de personas o programas sin autorización.
- Revelación o compromiso de credenciales, datos de autenticación o de cifrado.
- Pérdida total o parcial de datos o de información por cualquier causa.
- Distribución incontrolada: envío de información a personas que no deberían recibirla.
- Pérdida o sustracción de equipos o soportes informáticos, de contenedores o de parte de sus contenidos.
- Ataques sufridos por virus/software malicioso que puedan afectar al intercambio de información entre PROVEEDOR y CNP.
- Otros: cualquier irregularidad o deficiencia detectada relativa al cumplimiento de los criterios de seguridad indicados.

En la medida en la que el posible impacto lo haga necesario, CNP y PROVEEDOR deberán acordar las acciones necesarias, tiempos de resolución y mecanismos de seguimiento.

PROVEEDOR se compromete a colaborar en todo lo posible con CNP ante cualquier evento que pueda requerir la notificación a las autoridades pertinentes y la realización de procedimientos forenses relacionados con dichos eventos.

PROVEEDOR implementará los mecanismos necesarios para monitorizar y cuantificar la información estadística de los incidentes de seguridad de la información relacionados con el servicio contratado por CNP, y que tendrán que estar disponibles ante petición de este.

Las notificaciones se deben enviar al buzón de correo: seguridad@cnp.es

3.2 Incidentes de Seguridad

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

PROVEEDOR sólo podrá revelar datos sobre un Incidente de Seguridad al Personal de PROVEEDOR cuando sea necesario para cumplir con sus obligaciones derivadas del presente Contrato, o para

asegurarse de que el Personal de PROVEEDOR pueda desempeñar sus funciones correctamente a efectos de que PROVEEDOR pueda prestar los Servicios.

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

CNP y/o el PROVEEDOR se involucrarán tan pronto como sea razonablemente posible para proporcionar una visión más completa del impacto y la urgencia del incidente.

Todas las resoluciones y tareas propuestas se documentarán en un registro de incidentes.

La actividad de resolución incluirá puntos de control y comunicaciones pertinentes y oportunas a CNP.

PROVEEDOR proporcionará a CNP actualizaciones continuas mientras duren las actividades de reparación, al nivel y con la frecuencia que acuerden las Partes.

PROVEEDOR proporcionará a CNP un informe de actualización del servicio informático tan pronto como sea razonablemente posible, y en cualquier caso no más tarde de 5 (cinco) días laborables desde la resolución del incidente, a menos que las Partes acuerden lo contrario.

3.3 Respuesta de Emergencia

PROVEEDOR establecerá un proceso de respuesta de emergencia respaldado por un equipo dedicado a dar soporte a esa respuesta, que describirá las acciones que pondrá en práctica el Personal de PROVEEDOR en caso de que se produzca un Ataque Significativo

Este equipo estará en comunicación con el buzón: seguridad@cnp.es

3.4 Redundancia

PROVEEDOR implantará controles ambientales con redundancia automática, monitorizados y probados regularmente con el objetivo de asegurar la continuidad y el funcionamiento de sus Centros de Procesamiento de Datos.

PROVEEDOR se asegurará del cumplimiento de las medidas físicas de protección y redundancia para proteger los sistemas de fallos en el suministro eléctrico que puedan afectar al servicio contratado.

3.5 Seguridad Física

Se deberán establecer los mecanismos y procedimientos de control de accesos físicos a las instalaciones de PROVEEDOR para impedir el acceso a los elementos de la infraestructura o a la información de CNP por parte de personal no autorizado.

PROVEEDOR implementará las medidas de seguridad física adecuadas para proteger los datos sensibles de CNP y los sistemas de información que hagan uso de los mismos.

PROVEEDOR implementará las medidas de protección físicas necesarias para hacer frente a cualquier amenaza física (desastre natural, ataque intencionado...) sobre los soportes que contengan información de CNP.

3.6 Copias de Seguridad

PROVEEDOR se compromete a almacenar las copias de seguridad que contengan información de CNP en un lugar distinto y suficientemente alejado de los sistemas de producción y almacenado con las correspondientes medidas de seguridad que aseguren su integridad, disponibilidad y confidencialidad.

3.7 Trazabilidad

PROVEEDOR implementará las medidas técnicas necesarias para controlar la actividad realizada sobre los datos de la entidad en los sistemas involucrados, incluyendo la actividad realizada por usuarios privilegiados y administradores.

3.8 Investigaciones Forenses

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, 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.

4 CONTINUIDAD DE NEGOCIO

PROVEEDOR implementará las medidas técnicas necesarias para el mantenimiento del equipo involucrado en los servicios con el objetivo de asegurar la continuidad y disponibilidad de las operaciones realizadas por el mismo.

PROVEEDOR se compromete a garantizar que ha implementado y mantiene de forma efectiva un Sistema de Gestión de la Continuidad de Negocio y de acuerdo con los requisitos de continuidad de negocio definidos por CNP. En este sentido, los Planes de Continuidad de Negocio de las instalaciones, centros de procesamiento de datos y equipos utilizados para el procesamiento o el uso de los activos de PROVEEDOR, deberán contener como mínimo:

- Una lista de los servicios que participan en el proceso de recuperación de los activos de la compañía.
- Una lista con la priorización de estos activos y servicios.
- Un calendario de las tareas claves que se llevan a cabo en relación con la continuidad de Negocio y la identificación de un responsable para cada tarea.
- Un listado de los empleados del tercero que tengan asignado responsabilidades de Continuidad de Negocio.
- Listado de los procedimientos que deben seguirse en la realización de las tareas y actividades clave en la Continuidad de Negocio y, en caso de emergencia, procedimientos establecidos de recuperación y vuelta a la normalidad.
- Detalle suficiente para que los planes de Continuidad de Negocio puedan ser seguidos por personal que no suele llevarlos a cabo y así ofrecer servicios mínimos de continuidad del Negocio en caso de contingencia.

Los Planes de Continuidad de Negocio, planes de respuesta y recuperación se deberán probar al menos anualmente y se actualizarán sin demora en caso de que se produzca algún cambio en los requisitos de seguridad relacionados con los activos de PROVEEDOR. Los resultados de estas pruebas de respuesta y recuperación de Continuidad del Negocio deberán ser comunicados a CNP.

Los Planes de Continuidad de negocio, planes de respuesta y recuperación estarán disponibles en las oficinas del PROVEEDOR.

El tiempo de recuperación objetivo (RTO) mínimo que se debe cumplir para reestablecer el servicio en caso de incidente crítico debe ser pactado entre CNP y PROVEEDOR pero en ningún caso podrá ser superior a 24 (veinticuatro) horas.

Adicionalmente, CNP se reserva el derecho de obtener evidencia de auditoría acerca de la viabilidad y eficacia de los planes de continuidad de negocio y programa de pruebas asociado de PROVEEDOR.

5 DERECHO DE AUDITORÍA

PROVEEDOR deberá aportar, a requerimiento de CNP, evidencias de evaluaciones o auditorías de seguridad o, incluso, permitir, a petición de CNP, que se lleven a cabo en sus instalaciones auditorías y/o inspecciones independientes con carácter anual de las medidas de seguridad reguladas por el presente anexo.

Dichas auditorías o inspecciones deberán ser acordadas previamente entre CNP y el PROVEEDOR, y podrán ser realizadas por CNP o por una entidad auditora aceptada por CNP. PROVEEDOR se compromete al cumplimiento del posible plan de acción resultante de dichas auditorías.

Al realizar cualquier inspección, CNP deberá causar el menor trastorno posible al funcionamiento de los Servicios.

PROVEEDOR prestará toda la asistencia que CNP pueda solicitarle razonablemente en relación con toda inspección y, sin perjuicio de lo indicado en otras secciones, 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 contrato.

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

6 VALORACIÓN DE LA SEGURIDAD

Como parte de la valoración de la seguridad CNP, se incluirán los sistemas de PROVEEDOR que den servicio a CNP dentro del alcance de los ejercicios de Pentesting y/o Hacking Ético realizadas por el PROVEEDOR acorde a la legislación.

CNP y/o sus Agentes tendrán derecho a realizar una Valoración de la Seguridad en los Sistemas de PROVEEDOR, mediando un preaviso escrito remitido por CNP a 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.

CNP 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 de PROVEEDOR.

PROVEEDOR prestará a CNP 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.

PROVEEDOR, dentro de los DIEZ (1O) 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.

CNP tendrá derecho a aprobar las fechas y las medidas indicadas en el plan de acciones correctoras. Una vez ejecutado el plan, PROVEEDOR confirmará por escrito a CNP 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, CNP tendrá derecho a contratar, o a exigir a PROVEEDOR que contrate, a un Tercero Evaluador de la Seguridad (en ambos casos, a costa de 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.

Si, después de un Incidente de Seguridad, CNP deseara realizar una Valoración de la Seguridad de emergencia 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 CNP.

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 a CNP de forma proactiva en las reuniones trimestrales de seguimiento.

7 GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN

7.1 Gobierno de la Seguridad de la Información

PROVEEDOR deberá definir y documentar su Marco de Gestión de la Seguridad. Esto incluye todos aquellos procedimientos que la organización necesite para asegurar una correcta planificación, operación y control de sus procesos de seguridad de la información. Dichos procedimientos deberán quedar siempre a disposición de CNP, debiendo permanecer actualizados y siendo revisados periódicamente.

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.

7.2 Importancia de la Gestión de la Seguridad de la Información

PROVEEDOR se asegurará de que la función de seguridad de la información, por su importancia para las actividades de PROVEEDOR, esté representada al más alto nivel de dirección dentro de la

organización de PROVEEDOR, y de que el Marco de Gestión de la Seguridad sea aprobado por la alta dirección.

7.3 Función de Seguridad de la Información

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 de PROVEEDOR. Esta función de cara a CNP se materializará en la figura del Responsable de Seguridad, quien se designará en la Fase de Arranque.

8 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

8.1 Política de Seguridad de la Información

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

9 GESTIÓN DE ACTIVOS

9.1 Gestión de los Medios Informáticos

PROVEEDOR se asegurará de que todos los datos de CNP y la Información Confidencial de CNP 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 de CNP e Información Confidencial de CNP 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 a PROVEEDOR o ser gestionadas o contratadas por éste.

9.2 Destrucción de Equipos y Medios Redundantes

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

La destrucción segura de equipos y medios informáticos redundantes a efectos de lo dispuesto en el apartado "Gestión de los Medios Informáticos" incluirá el borrado seguro de la información que ya no sea

necesaria, de una forma que imposibilite su recuperación (lo que incluye cintas magnéticas, discos, material de escritorio y cualquier otro tipo de soporte de información).

10 CONTROL DE ACCESO

10.1 Autenticación

PROVEEDOR se asegurará de que todos los miembros del Personal de PROVEEDOR que tengan acceso al Sistema de 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.

PROVEEDOR se asegurará de que el Sistema de 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 o la fuerza bruta;
- 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.

10.2 Mínimo acceso

PROVEEDOR dispondrá de procedimientos basados en el principio de privilegio mínimo acceso y que tengan en cuenta la necesidad de uso y la confidencialidad de la información cuando autoricen accesos y permisos, de forma que el Personal, sea de PROVEEDOR o de sus subcontratistas, incluyendo usuarios privilegiados y administradores, acceda únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Estos procedimientos permitirán también la gestión de la revocación y modificación de dichos permisos.

10.3 Acceso Privilegiado

PROVEEDOR se asegurará de que:

- Las cuentas de Acceso de Usuarios Privilegiados no puedan utilizarse en operaciones que no requieran esos permisos ;

- 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 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.

10.4 Cuentas Genéricas

PROVEEDOR realizará un inventario de cuentas genéricas y no nominales ubicadas en los sistemas de la entidad, documentando en caso de existir la justificación de su uso, el propietario de esta cuenta y responsabilizará a este de la seguridad, rotado de contraseña y uso de esta cuenta de manera que si un tercero utiliza la cuenta se mantenga un registro de uso.

Una vez finalizada la actividad la contraseña debe cambiarse para garantizar la seguridad. Esto incluye las cuentas no nominales facilitadas por CNP para la realización del servicio.

10.5 Gestión de las contraseñas

PROVEEDOR dispondrá de una política y procedimientos que aseguren la fortaleza de las contraseñas y su actualización periódica.

PROVEEDOR se asegurará de que el Sistema de 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.

- 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.

- Se asegurarán los cambios de las contraseñas en los procesos de instalación de nuevos elementos de hardware o software y, en especial, el cambio de las contraseñas por defecto del fabricante.

- Las credenciales se almacenarán y transmitirán siempre cifradas.

- Relativo a las contraseñas para dar servicio a CNP, estas bajo ningún concepto pueden ser más permisivas que la política de contraseñas de CNP.

10.6 Baja de usuarios

PROVEEDOR definirá un procedimiento de bajas de sus usuarios que incluya, pero no se limite a:

- Asignación, documentación y comunicación de roles y responsabilidades.
- Tiempos para la ejecución de las bajas inferior a 48 (veinticuatro) horas.
- Tiempos para la devolución de los activos.
- Notificación de las bajas a CNP en un plazo inferior a 48 (veinticuatro) horas.

10.7 Entorno Compartido

Si Grupo MEDVIDA presta los Servicios a CNP desde un emplazamiento que comparte con uno o varios Terceros, PROVEEDOR desarrollará y aplicará procesos, sujetos a la aprobación previa de CNP 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 de PROVEEDOR que intervengan en la prestación de los Servicios.

11 CONFIGURACIÓN DEL SISTEMA

11.1 Diseño del Sistema

PROVEEDOR identificara 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.

11.2 Administración

El acceso a los puertos de diagnóstico y configuración de sistemas que traten información de CNP estará restringido únicamente a las personas y aplicaciones autorizadas por el PROVEEDOR.

11.3 Configuración de Sistemas Anfitriones y Redes

PROVEEDOR se asegurará de que los sistemas anfitriones y las redes que formen parte de los Sistemas de 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.

11.4 Parches

PROVEEDOR llevará a cabo una correcta actualización e instalación de parches de seguridad, versiones, actualizaciones, y licencias pertinentes en el software de los sistemas que traten los datos de CNP.

12 MONITORIZACIÓN

12.1 Registro de Sucesos

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 a CNP 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 de PROVEEDOR.

PROVEEDOR conservará este registro al menos durante los DOCE (12) meses siguientes a su creación, o durante el período distinto que CNP 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). PROVEEDOR transmitirá el registro a CNP, previa solicitud de éste.

PROVEEDOR revisará los registros relativos a todos los sucesos clave que se encuentren en los Sistemas de 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.

12.2 Sustracción de Datos

PROVEEDOR se compromete expresa y formalmente a no realizar ejecuciones automáticas y/o sustraer datos de los sistemas mediante el uso de soportes físicos.

12.3 Ubicación

PROVEEDOR deberá comunicar siempre a CNP lo relativo a la, reubicación de hardware y software que trate información de CNP a otra ubicación. Asimismo, no se podrán mover los datos fuera de la UE.

12.4 Software no autorizado

PROVEEDOR implementará las medidas técnicas necesarias para prevenir la ejecución de software no autorizado y código móvil no autorizado (software transferido entre sistemas a través de redes confiables o no confiables y ejecutado en un sistema local sin instalación o ejecución explícita por parte del receptor) en cualquier dispositivo, infraestructura de red o componente del sistema que trate datos de la CNP.

13 SEGURIDAD DE LA RED

13.1 Diseño de la Red

La red de 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.

PROVEEDOR debe establecer los mecanismos y procedimientos de control de accesos lógicos para impedir el acceso a la Información Protegida por parte de personal no autorizado durante el tiempo en el que PROVEEDOR disponga de Información de CNP.

13.2 Conexiones Externas

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

13.2.1 Conexiones con terceros

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

Las aplicaciones o servicios que transmitan información con datos sensibles o confidenciales utilizarán protocolos seguros (HTTPS, SFTP, SSH, TLS...)

13.3 Cortafuegos

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

Cierre de todos los puertos no necesarios para la ejecución del servicio y justificación de aquellos que queden abiertos

Todas las reglas deben estar comentadas enlazando al ticket de la petición o requerimiento.

Implementación de controles que limiten el acceso de usuarios desde el exterior.

Las reglas se revisarán cada 6 meses y se mostrará el resultado en la revisión periódica del servicio junto a CNP.

13.4 Acceso inalámbrico

PROVEEDOR se asegurará de que el acceso inalámbrico a los Sistemas de 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 PROVEEDOR.

13.5 Comunicaciones Electrónicas

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

Mensajería Instantánea: 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 de PROVEEDOR.

Proxy: Implantación de proxys para limitar el acceso a redes públicas por partes de los empleados de PROVEEDOR y filtrado de contenido proveniente de Internet.

14 PROTECCIÓN CONTRA CÓDIGO MALICIOSO

PROVEEDOR establecerá y mantendrá medios actualizados de protección contra Código Malicioso, (EDR y antivirus) en toda su organización y en los sistemas que den servicio a CNP.

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

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

15 GESTIÓN DE LOS CAMBIOS, PARCHES Y VULNERABILIDADES

15.1 Gestión de los Cambios

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

15.2 Soluciones de Emergencia

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 de 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 de PROVEEDOR.

15.3 Gestión de los Parches y Obsolesencia

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 de 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.

15.4 Gestión de Vulnerabilidades

PROVEEDOR dispondrá de una gestión correcta de las vulnerabilidades de seguridad que presente el software entregado a CNP, implementará las medidas técnicas requeridas para la detección periódica de vulnerabilidades y facilitará a CNP 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.

16 CONFIDENCIALIDAD

PROVEEDOR será responsable de cualquier incumplimiento de las obligaciones de confidencialidad por parte de cualquiera de sus accionistas, administradores, personal, cesionarios, subcontratistas o asesores profesionales, que hayan tenido acceso a la Información Confidencial, reservándose CNP el derecho a interponer las acciones legales pertinentes en defensa de sus intereses con relación al quebranto de confidencialidad.

17 TERCEROS Y SUBCONTRATISTAS

17.1 Contrato de servicios

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 PROVEEDOR está obligado a aplicar en virtud del presente contrato. Dichos servicios se prestarán en virtud de los correspondientes contratos.

17.2 Aseguramiento de Cumplimiento

PROVEEDOR se asegurará de que todos los contratos firmados con subcontratistas y otros terceros que cuenten con la confianza de PROVEEDOR para la prestación de los Servicios establezcan el derecho de PROVEEDOR y de CNP (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 PROVEEDOR en virtud del presente Contrato.

Alternativamente, y únicamente a instancias de CNP, CNP podrá aceptar un compromiso del Subcontratista por el que se obligue a acordar con 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 CNP.

Annex 14.1
Data Processing Agreement

The Parties agree to execute the Data Processing Agreement in Spanish, with the terms and conditions set forth hereto:

Por medio del presente Anexo 14.1 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: MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS, S.A. (SOCIEDAD UNIPERSONAL) (en adelante, el "**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:

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

☐ Comunicación

X Otros: Otros tratamientos que deriven del acuerdo de prestación de servicios ("**TSA**") al que se anexa este contrato de encargo del tratamiento.

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:

Categorías de interesados: tomadores, asegurados, terceros beneficiarios y cualesquier otra categoría que resulte necesaria para la ejecución del TSA.

Categorías de datos personales: nombre, apellidos, nacionalidad, DNI, NIE, fecha de nacimiento, domicilio y dirección fiscal, email, Datos bancarios, datos de salud, género, parentesco y siniestros, en su caso, datos de actividad profesional o de carácter socioeconómico, cuando sea necesario para el cumplimiento de medidas de diligencia en materia de prevención del blanqueo de capitales, y cualesquier otra categoría que resulte necesaria para la ejecución del TSA.

3. Duración

La duración del Encargo de tratamiento se vincula a la duración del TSA al que se anexa este contrato de encargo del tratamiento suscrito entre el CLIENTE y el PROVEEDOR.

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

4. Obligaciones del Encargado del tratamiento

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

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

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

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

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

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

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

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

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

   i) La seudoanimización y el cifrado de datos personales.

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

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

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

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

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

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

e. Subcontratación

   Para subcontratar con otras empresas, el Encargado debe comunicarlo por escrito al Responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

En particular, el encargado facilitará al responsable la siguiente información sobre el tercer proveedor: (i) identificación de la entidad subcontratada, incluyendo nombre comercial y denominación social, NIF, domicilio social y señas de contacto; (ii) identificación del objeto del subencargo que realizará, incluyendo la duración, naturaleza y finalidad del tratamiento, el tipo de datos personales y categorías de interesados y el tipo de tratamiento de datos que llevará a cabo; (iii) las medidas técnicas y organizativas con las que cuenta el subencargado para realizar el tratamiento; (iv) en su caso, información sobre las transferencias internacionales que pudiera realizar y detalle sobre las garantías del RGPD que está aplicando en todo caso; (v) cualquier otra información que se considere relevante para garantizar el adecuado tratamiento de los datos personales del responsable (por ejemplo, certificado de cumplimiento normativo, adhesión a códigos de conducta, etc.).La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de quince (15) días naturales.

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

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

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

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

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

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

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

Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el Encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección gdpr.es.peticion@cnp.es.

La comunicación remitirse en la forma y plazos indicados en el apartado 16 del Anexo 2.2 del contrato de prestación de servicios suscrito entre el Responsable del Tratamiento y el Encargado del Tratamiento.

k. Derecho de información

El Encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar, incluyendo toda la información necesaria bajo los arts. 12 a 14 del RGPD. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio 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 12 horas, y a través de correo electrónico enviado a seguridad@cnp.es 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.

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 (en la sola opinión razonable del responsable del tratamiento).

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

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 se Seguridad de acuerdo con la evaluación de riesgos realizada por el responsable de tratamiento con fecha de firma del presente Anexo.

En todo caso, asistirá al Responsable del tratamiento en el cumplimiento de sus obligaciones en materia de medidas de seguridad y 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.

En caso de contradicción entre la presente cláusula (contrato de encargo del tratamiento) y el Apéndice de Seguridad, prevalecerá lo dispuesto en el presente contrato de encargo.

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.

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, cuando corresponda en la sola opinión razonable del responsable del tratamiento.

c) Realizar las consultas previas que corresponda, en la sola opinión razonable del responsable del tratamiento.

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 que considere oportunas.

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 en los términos previstos en la cláusula de responsabilidad del *TSA*. 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) (u otra autoridad competente en materia de protección de datos) se personaran en las instalaciones del PROVEEDOR al

objeto de ejercer su potestad inspectora, EL PROVEEDOR se compromete a comunicar esta circunstancia al CLIENTE en el menor tiempo posible (y en todo caso en un (1) día natural).

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 EL CLIENTE deberá cumplir lo establecido en la presente cláusula, cuya obligación subsistirá incluso hasta después de finalizar las relaciones contractuales entre las Partes.

Signature page

MEDVIDA PARTNERS DE SEGUROS Y REASEGUROS, S.A. (SOCIEDAD UNIPERSONAL)
By

DocuSigned by:
5C99210BC9B6499...

Mr. Jaime Kirkpatrick de la Vega

CNP ASSURANCES SUCURSAL EN ESPAÑA
By

DocuSigned by:
David Lattes
6AD39B55E982422...

Mr. David Lattes

CNP CAUTION SUCURSAL EN ESPAÑA
By

DocuSigned by:
David Lattes
6AD39B55E982422...

Mr. David Lattes