AJ233

Hoja de Control: Documentación a Firmar

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

Fecha:	22/08/2022						
Sociedad:	CNP ASSURANCES						
Tipo de documento:	Contrato /Anexos ☐	Presupuesto/ Proyecto ☐	Doc. Consejo ☐	Doc. Hacienda ☐	Doc. DGSFP ☐	Doc. Planes/EPSV ☐	Otro:
Solicitado por: *(Director del CODIR)*	THIERRY VASQUEZ						
Contenido / Objetivo: Principal Acuerdo, entregables y descripción del servicio	Soporte BASIS Convista						

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

Denominación del Documento:	Convista soporte BASIS	
Apoderado/s de CNP: *(según importe económico del contrato)* (1)	DAVID LATTES	
Contraparte: *(proveedor, o interviniente)*	CONVISTA	
Fecha de inicio del contrato:	MAI 2022	
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	
Código CECO:		
Código PEP:		
Activable:	☐ SI ☐ NO	
Periodicidad del pago:	Mensual ☐	*Trimestral* ☐ *Anual* ☐ *Pago único* ☐

- OBLIGATORIO-

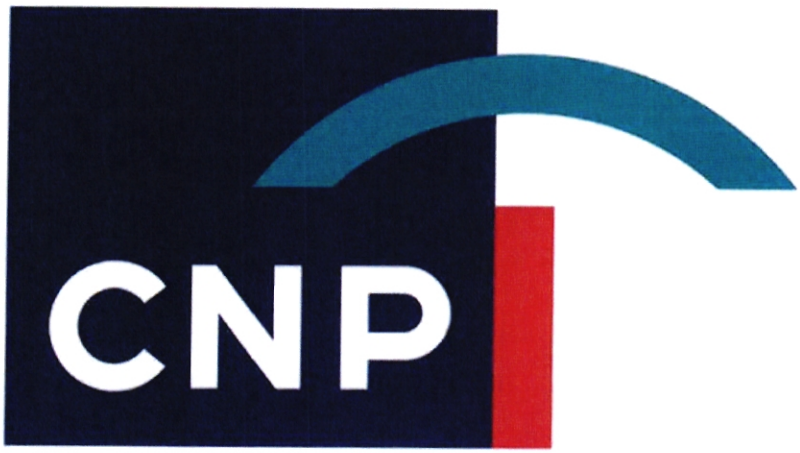
Responsable del Departamento y Director del CODIR correspondiente: Oscar Rodriguez PA	Fecha: 23.08	Firma:	Firma:
Verificación de Control Financiero: *En el caso de que el gasto sea activable.*	Fecha:	Firma:	
Verificación de Control de Gestión: *En el caso de que el gasto esté presupuestado y el pedido o la factura no superen el presupuesto, no será necesaria la firma del Control de Gestión.*	Fecha:	Firma:	
Revisión Asesoría Jurídica: *(persona del equipo legal que ha revisado el contrato y verificado que cumple con todos los requerimientos solicitados) N ereida CANO*	Fecha:	Firma:	
Comentarios Asesoría Jurídica:			
Verificación de Compras: T VASQUEZ	Fecha: 23-08-22	Firma:	
Directora Operativa o Directora Financiera:	Fecha:	Firma:	
Representante Legal de la sucursal – D LATTES	Fecha: 30.08.22	Firma:	

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

CONVISTA

Contrato de Servicios

Soporte Basis – CNP Assurances, S.A., Sucursal en España y CNP Caution, Sucursal en España



Created by: ConVista Consulting & Advisors, SLU

Version	Date	Author	Change
1.0	23.05.2022	Norbert Nielsen	

Índice de contenidos

1 INTRODUCCIÓN 4
1.1 Marco previo 4
1.2 Motivación y objetivos 4
2 Descripción del servicio 5
2.1 Ámbito de cobertura 5
2.2 Establecimiento del Servicio 6
2.3 Monitorización y continuidad de los entornos SAP 6
2.3.1 Monitorización del estado actual del sistema 6
2.3.2 Continuidad de los entornos 7
2.4 Respaldo técnico experto para el soporte a entornos SAP 7
2.4.1 Ejecución de acciones correctivas y/o preventivas 8
2.4.2 Gestión y resolución de solicitudes de servicio e incidencias 8
2.5 Tareas cubiertas por el servicio 8
2.5.1 Administración y mantenimiento del sistema SAP 9
2.5.2 Escalado de incidencias a SAP 9
2.5.3 Administración y mantenimiento de la base de datos 9
3 Horario del servicio 10
4 Limitaciones del servicio 10
4.1 Servicios adicionales no incluidos 10
4.2 Servicios excluidos 10
5 Organización del servicio 11
5.1 Modalidad de prestación del servicio 11
5.2 Canales de comunicación con el Centro de Operaciones 11
6 Duración del servicio 12
6.1 Periodo de contratación del servicio 12
6.2 Cancelación anticipada del Contrato 12
7 Propuesta económica 13
7.1 Coste del servicio 13
7.2 Jornadas a demanda 13
7.3 Tarifas para la ejecución de tareas adicionales 13
7.4 Facturación 14
7.5 Gastos de desplazamiento 14

8 Requerimientos y condiciones del servicio **14**
9 Aplicación de sanciones financieras **15**
10 Obligaciones laborales de CONVISTA **15**
11 Notificaciones **16**
12 Cláusula de prevención frente al fraude, soborno y corrupción **17**
13 Independencia de las Partes **17**
14 Cesión y subcontratación **18**
15 Términos y condiciones **18**
15.1 Confidencialidad 18
15.2 Protección de datos 18
15.3 Datos personales de los firmantes 19
15.4 Obligaciones del Cliente 20
15.5 Obligaciones de CONVISTA 20
15.6 Información propiedad de CONVISTA 20
15.7 Propiedad del sistema y de la solución 21
15.8 Causas de terminación anormal 21
16 Nulidad o anulabilidad **21**
17 Legislación aplicable **22**
18 Jurisdicción aplicable **22**
19 Contrato completo **22**
20 Firma del contrato **23**

1 INTRODUCCIÓN

1.1 Marco previo

CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA Y CNP CAUTION, SUCURSAL EN ESPAÑA desean formalizar la petición de servicios realizada a CONVISTA para cubrir los servicios deseados de "*Soporte Basis para CNP Assurances, S.A., Sucursal en España y CNP Caution, Sucursal en España*"

CONVISTA es una empresa especializada en la prestación de servicios cuya actividad cubre las necesidades de CNP ASSURANCES S.A., SUCURSAL EN ESPAÑA Y CNP CAUTION, SUCURSAL EN ESPAÑA. .

REUNIDOS

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

Ambas denominadas conjuntamente en adelante como el "**CLIENTE**".

Y, DE OTRA PARTE, **D. NORBERT NIELSEN**, mayor de edad, con domicilio a estos efectos en Calle Santa Leonor, n.º 65, Edificio E, Planta 3, 28037, Madrid, y con N.I.E. número X-3584601-M, en nombre y representación de la mercantil "**CONVISTA CONSULTING & ADVISORS S.L.U.**", con domicilio a estos efectos en Calle Santa Leonor, n.º 65, Edificio E, Planta 3, 28037, Madrid y con C.I.F. n.º B-62421805 (en adelante, el "**PROVEEDOR" o "CONVISTA**").

El CLIENTE y el PROVEEDOR, podrán ser denominadas individual e indistintamente como "**la Parte**" y conjuntamente como "**las Partes**", reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente contrato (en adelante, el "**Contrato**").

1.2 Motivación y objetivos

El Cliente solicita a CONVISTA sus servicios de Soporte Remoto SAP Basis, con el propósito de asegurar el correcto funcionamiento de sus respectivos sistemas.

Así pues, el servicio ofertado por CONVISTA responde a las necesidades planteadas por el Cliente.

- Monitorización de los sistemas SAP y envío de alertas ante caídas;
- Respaldo técnico experto, ágil y flexible, para gestión de solicitudes e incidencias;

- Asesoramiento experto en la evolución y mejora continuada de los sistemas SAP.

La presente propuesta, de carácter anual, es decir, doces(12) meses, responde a la necesidad planteada por el Cliente de asegurar un soporte para el correcto funcionamiento de sus sistemas productivos SAP, así como un asesoramiento experto en la evolución y mejora continuada de los mismos.

2 Descripción del servicio

2.1 Ámbito de cobertura

El ámbito de cobertura de este Contrato son los entornos actuales de SAP en:

- SAP S4/HANA (Dev + QA + Prod)
- SAP Solution Manager

CONVISTA dará soporte remoto a las necesidades que el Cliente pueda tener en el ámbito de gestión de sistemas SAP Basis. El servicio ofertado abarca el soporte a tareas relacionadas con la gestión y explotación del sistema según tres niveles o tipologías:

- **Correctivos:** Incidencias que afecten al buen funcionamiento del sistema.
- **Preventivos:** Iniciativas que ayuden a prevenir incidencias futuras.
- **Evolutivos:** Nuevas funcionalidades o cambios en la infraestructura existente serán valorados aparte y no están incluidos en la presente propuesta.

Con este propósito, el servicio se estructura en tres niveles:
- Monitorización y continuidad de los entornos SAP productivos.
- Asesoramiento experto en la evolución de los sistemas SAP.
- Respaldo técnico experto para el soporte a los entornos SAP.

Queda dentro del alcance del Contrato:
- Proyecto de Establecimiento del servicio.
- Mantenimiento correctivo.
  - Monitorización y reacción proactiva de alertas continua.
  - Supervisión diaria de los principales procesos e indicadores de rendimiento del sistema.
  - Tratamiento de incidencias de segundo nivel.
  - Apertura y tratamiento de notas a SAP.
- Mantenimiento preventivo.
  - Gestión y monitorización del servicio, incluyendo reuniones de seguimiento con el equipo designado por el Cliente.
  - Análisis, planificación y ejecución de las recomendaciones del EarlyWatch Alert previa consolidación con el cliente.

A continuación, se indican los grandes bloques que definen el servicio ofertado:

Establecimiento del servicio	Servicio Correctivo	Servicio Preventivo	Gestión
•Procedimiento previo a la puesta en marcha del servicio.	•Gestión de requerimientos que se deban corregir o modificar, según prioridad.	•Serie de acciones orientadas a ser proactivo y prevenir futuros problemas.	•Informes de seguimiento e informes ejecutivos.

Es necesario tener una conexión permanente mediante una red privada virtual (Túnel VPN) para la monitorización automática de los sistemas. En caso de no ser posible la línea VPN punto a punto no será posible establecer la monitorización automática.

2.2 Establecimiento del Servicio

CONVISTA tiene definido un procedimiento de "Establecimiento del Servicio" previo al comienzo del servicio, que asegura el éxito del traspaso de competencias y que incluye las siguientes tareas:

Tareas de establecimiento del servicio
Toma de datos de los sistemas SAP cubiertos
Definición de los usuarios y privilegios (roles) a utilizar por el equipo CONVISTA
Identificación de los Key User (usuarios clave, adelante "KU") del cliente
Definición de los usuarios y privilegios a utilizar por los KU en la herramienta de ticketing de CONVISTA
Configuración de la línea de comunicación con el Centro de Servicios Gestionados de CONVISTA
Presentación y comunicación del servicio y su funcionamineto a Usuarios Clave

2.3 Monitorización y continuidad de los entornos SAP

El propósito de este bloque es monitorizar periódicamente el estado de los entornos SAP del Cliente contratados, con objeto de controlar su estado y disponer de información para prevenir posibles incidencias y prescribir acciones correctivas.

2.3.1 Monitorización del estado actual del sistema

El equipo de CONVISTA realizará una serie de verificaciones de los principales parámetros del sistema para asegurar el buen funcionamiento del mismo. Fruto de esta revisión, CONVISTA enviará un Informe de estado de los elementos relevantes de los sistemas monitorizados, junto con una valoración del estado de los mismos, así como elementos a revisar para asegurar su

buen funcionamiento. La periodicidad del envío de los informes al Cliente será mensual, con un máximo de diez (10) días laborales desde que finaliza el mes.

Este proceso de revisión del sistema incluirá, entre otros, los siguientes conceptos:

- **Revisión y análisis de los sistemas SAP contratados.**
  Estado de las instancias y de los procesos de trabajo, Usuarios conectados, Rendimiento del sistema, Órdenes de actualización, Log del sistema, Jobs de reorganización y Jobs cancelados, RFC transaccional, Buffers de servidor de aplicaciones SAP, "Short dumps" de ABAP, Entradas de bloqueo y todas las medidas de seguridad incluidas en el anexo 2, apéndice 1. **Revisión y análisis de la base de datos subyacente a los sistemas SAP contratados.**

  "Tablespaces" e índices, histórico de la base de datos, tareas de base de datos, lanzamiento de backup integrado y revisión de "logs" y rendimiento de base de datos.

- **Sistema operativo de los sistemas SAP contratados.**
  Análisis del sistema de archivos y monitor de Sistema Operativo a nivel básico.

2.3.2 Continuidad de los entornos

CONVISTA deberá detectar cualquier desvío no controlado de los principales parámetros definidos para asegurar la continuidad de los sistemas monitorizados. En tal caso, se procederá a una intervención manual, en principio, de manera remota, aunque podría ser presencial, si fuera necesario, para subsanar el problema, siempre dentro del horario de cobertura contratado. Para ello, por un lado, el Cliente y, por otro lado, CONVISTA definirán conjuntamente el procedimiento de reacción ante estas situaciones, regulándose en el correspondiente anexo al presente Contrato.

Las alertas a monitorizar incluidas en la presente propuesta son las siguientes:

- Paradas no programadas de los entornos monitorizados.
- Errores en los servicios del servidor de aplicación SAP.
- Todas aquellas alertas recogidas en el anexo 2, apéndice 1 del presente Contrato.

2.4 Respaldo técnico experto para el soporte a entornos SAP

Dada la transcendencia de los sistemas SAP del Cliente sobre el negocio, además de asegurar su buen funcionamiento, es primordial planificar con antelación tanto su evolución como las acciones preventivas necesarias para asegurar su correcto funcionamiento a medio y largo plazo en función de los cambiantes requerimientos del negocio. CONVISTA asignará un especialista que llevará a cabo las siguientes tareas:

- Soporte experto en la resolución de dudas y/o consultas relacionadas con los entornos SAP.
- Revisión y análisis del informe mensual de monitorización de los sistemas SAP.

- Generación de un informe de recomendaciones, enviadas al Cliente de forma bimestral, a ejecutar en tres ámbitos:
  - Correctivos: Riesgos a corto plazo;
  - Preventivos: Potenciales riesgos a medio o largo plazo;
  - Evolutivos: Optimización y evolución de la infraestructura SAP.

Por defecto, este bloque del servicio se prestará en horario laboral y en remoto sobre los sistemas contratados, pudiendo extenderse si fuese necesario y previa aprobación del Cliente, según la cobertura horaria.

Las acciones correctivas y preventivas quedan incluidas en el marco del presente Contrato. Las tareas evolutivas ejecutadas en este servicio se facturarán según tarifas vigentes para cada perfil y previa aceptación del CLIENTE.

2.4.1 Ejecución de acciones correctivas y/o preventivas

Se consideran acciones correctivas y/o preventivas todas aquellas detectadas por el equipo CONVISTA en la monitorización diaria del sistema y cuya ejecución ha sido propuesta por los mecanismos establecidos. Una vez ejecutada la acción, CONVISTA pondrá a disposición del Clienteun resumen detallado de la misma que enviará al Cliente todos los meses.

2.4.2 Gestión y resolución de solicitudes de servicio e incidencias

Se consideran solicitudes de servicio o incidencias aquellas reportadas por el personal del Cliente a través de los canales estipulados (ticketing) al centro de operaciones de CONVISTA, cuyo ámbito se corresponda con los servicios ofertados en la presente propuesta.

El proceso de gestión y resolución de las solicitudes e incidencias consta de al menos los siguientes pasos:

- Notificación y registro de la solicitud o incidencia en el Centro de Operaciones.
- Análisis de la solicitud o incidencia y sus repercusiones sobre el entorno.
- Clasificación de la prioridad definida entre el Cliente y CONVISTA.
- Asignación de recursos y planificación de la acción según prioridad.
- En caso de ser necesario, propuesta de solución alternativa temporal.
- Resolución de la solicitud o incidencia.
- Informe de gestión y/o ejecución mensual de las mismas que tendrá que ser reportado al Cliente con un máximo de diez (10) días laborales desde que finaliza el mes..

2.5 Tareas cubiertas por el servicio

A continuación, se detallan el conjunto de tareas cuyo ámbito de ejecución se encuentra recogido bajo la presente propuesta:

2.5.1 Administración y mantenimiento del sistema SAP

- Recuperación del sistema ante caídas.
- Cambios de versión de la base de datos.
- Mantenimiento de los perfiles de instancia del entorno.
- Mantenimiento de los modos de operación del entorno.
- Mantenimiento del acceso a la infraestructura vía VPN.
- Informar al proveedor de la infraestructura de las acciones de mantenimiento de hardware.
- Gestión de la capa de transporte entre sistemas.
- Mantenimiento de los ficheros de órdenes de transporte.
- Gestión de los destinos SAP RFC y conexiones del sistema.
- Gestión del subsistema de Jobs y ejecución de procesos de fondo.
- Administración de los servicios de impresión.
- Ajuste de la memoria compartida y buffers de los sistemas SAP.
- Descarga y aplicación de parches y actualizaciones por componente. Se incluye la aplicación de parches recomendados por notas de SAP, pero no la migración de base de datos.
- Copias de mandante (bajo petición).
- Copias homogéneas / refrescos de sistemas (bajo petición, el contrato incluye 1 refresco por sistema y año).
- Todas aquellas alertas recogidas en el anexo 2, apéndice 1 del presente Contrato.

2.5.2 Escalado de incidencias a SAP

- Búsqueda de notas y mensajes SAP OSS, así como su aplicación.
- Gestión de la conexión OSS (On-line Service System).
- Creación y seguimiento de mensajes OSS.
- Coordinación de sesiones remotas con SAP Support.

2.5.3 Administración y mantenimiento de la base de datos

- Definición y supervisión de las políticas de backup y restore de la Base de Datos con carácter semanal.
- Supervisión de los estados de las diferentes BBDD de entornos SAP.
- Gestión y ajuste de espacio según crecimiento de la BBDD.
- Reorganización de tablas.
- Gestión del espacio en disco y de "tablespaces".
- Configuración de parámetros de ejecución: índices, "datafiles", tablas, cursores…
- Descarga y aplicación de parches y actualizaciones de base de datos.
- Informe de gestión y/o ejecución mensual de las mismas que tendrá que ser reportado al Cliente con un máximo de diez (10) días laborales desde que finaliza el mes.

3 Horario del servicio

El horario de servicio se establece para cada sistema del perímetro técnico la franja horaria de disponibilidad del servicio, dentro del cual tienen vigencia las responsabilidades y tareas incluidas en dicho nivel de servicio.

El horario de servicio de CONVISTA es de 09:00 horas a 18:00 horas, de lunes a viernes, ambos inclusive, de acuerdo con el calendario laboral de la Comunidad de Madrid y los festivos de Madrid capital.

4 Limitaciones del servicio

4.1 Servicios adicionales no incluidos

En caso de ser requeridos serán contemplados y facturados a parte:

- Cambios a Unicode.
- Instalación de nuevos sistemas.
- Subida de Enhanced Packages de SAP.
- Instalación o actualización de Sistema Operativo y SW de alta disponibilidad.
- Instalación y configuración de escenarios de SAP Solution Manager.
- Otros: Proyectos de archivado de datos, Formación.

4.2 Servicios excluidos

- Soporte funcional y soporte a entornos no incluidos en la presente propuesta.
- Definición y gestión de roles, perfiles u otros objetos de autorización de usuario.
- Servicios Basis motivados por evolutivos funcionales o por cambios de versión.
- Mantenimiento de hardware (servidores, almacenamiento, redes).
- Instalación de SW en las estaciones "Cliente" de los usuarios.
- Servicios de operación y copias de seguridad (cambio de cintas de back-up, etc.).
- No se incluyen licencias software ni hardware de aplicativos o dispositivos a utilizar.
- Operación del sistema operativo, aunque sí se trabajara de modo conjunto con el equipo del cliente en el caso de que sea necesario aplicar recomendaciones de SAP a este nivel.
- Incidencias de primer nivel (reportadas directamente por el usuario final).
- Ejecución de transportes.
- Manos remotas.
- Revisión / supervisión de las instalaciones propias del CPD del cliente (comunicaciones, almacenamiento, ...).

5 Organización del servicio

5.1 Modalidad de prestación del servicio

En función del bloque de cobertura del servicio, la modalidad de prestación será la siguiente:

- Monitorización de los entornos, generación remota y remisión electrónica mensual del informe de estado.
- Continuidad de los entornos productivos, control remoto constante de estado y envío de avisos electrónicos en caso de alerta.
- Después del envío del aviso electrónico, CONVISTA realizará un segundo aviso a través de ticketing al Cliente.
- Asesoramiento técnico en la evolución de los entornos, reunión con fecha a consensuar, pero con una periodicidad trimestral, con el Cliente.
- Respaldo técnico experto, el Cliente designará y comunicará a CONVISTA la persona o personas autorizadas para solicitar intervenciones. Una vez recibida la solicitud en el Centro de Operaciones de CONVISTA, a través de los canales habilitados (ticketing) al efecto, CONVISTA seguirá el siguiente procedimiento:
  - Análisis de la solicitud a través de la información suministrada.
  - Clasificación de prioridad de solicitud en base a la urgencia en la resolución, así como al impacto en el negocio, tal y como se describe en el punto siguiente.
  - Asignación del experto o expertos más adecuados para la resolución de la incidencia y planificación de la ejecución de los trabajos pertinentes.
  - Ejecución de las acciones requeridas para solventar la incidencia.

5.2 Canales de comunicación con el Centro de Operaciones

- **Herramienta de Ticketing de CONVISTA (JIRA):** Se facilitarán accesos y procedimientos al inicio del proyecto.
- **Teléfono:** Se facilita al inicio del servicio.
- **Correo electrónico:** Se facilita al inicio del servicio.

Para poder cumplir con las condiciones del servicio ofertadas en el Contrato es requisito indispensable que el Cliente utilice alguno de estos canales siempre que deseen realizar alguna solicitud de servicio, pues de otra manera CONVISTA no puede asegurar el cumplimiento de los tiempos de respuesta acordados.

6 Duración del servicio

6.1 Periodo de contratación del servicio

El presente Contrato entre CONVISTA y CNP ASSURANCES y CNP CAUTION tiene una duración de un (1) año, prorrogándose con carácter automático por igual periodo de plazo de un (1) año salvo que las Partes notifiquen con seis (6) meses de antelación su voluntad de no proceder a la prórroga del Contrato, bajo las condiciones estipuladas en el presente Contrato .

La fecha de inicio del presente Contrato se establece el 01 de octubre de 2022 o, en su defecto, cuando el Proyecto de Implantación de SAP que en la actualidad está realizando CONVISTA haya concluido.

6.2 Cancelación anticipada del Contrato

En el caso en que el Cliente decidiera cancelar el Contrato unilateralmente, deberá notificarlo por escrito a CONVISTA con una antelación suficiente, teniendo en cuenta las siguientes consideraciones:

- A partir de que el contrato despliegue sus efectos, el Cliente deberá notificar a CONVISTA su voluntad de terminar la presente relación con seis (6) meses de antelación.
- En cualquier caso, el Cliente abonará el 100% de los servicios que hasta el momento de la resolución efectiva se hubieran devengado a favor de CONVISTA por los servicios que efectivamente hubiera prestado .

En el caso en que CONVISTA decidiera cancelar el Contrato unilateralmente, deberá notificarlo por escrito al Cliente con una antelación de seis (6) meses y teniendo en cuenta las siguientes consideraciones:

- CONVISTA se hará cargo de todos los costes asociados a dicha cancelación.
- CONVISTA terminará los servicios que en el momento de la cancelación ya hubieran sido aprobados por las Partes.
- COVISTA entregará todos los materiales, sistemas, BBDD y/o cualquier soporte que pertenezca a El Cliente y que haya sido proporcionado a CONVISTA para la ejecución del presente Contrato teniendo en cuenta las instrucciones establecidas en el anexo 2 del mismo.
- CONVISTA facilitará al Cliente una extracción en formato CSV de las peticiones realizadas a través de ticketing que se hayan realizado durante la ejecución del presente Contrato.

7 Propuesta económica

7.1 Coste del servicio

Con relación al pago de los servicios contratados y regulados en el presente Contrato, el NOVENTA POR CIENTO (90%) del Precio será abonado por CNP CAUTION, mientras que CNP ASSURANCES abonará el DIEZ POR CIENTO (10%) del Precio restante. Ambas cantidades serán abonadas a CONVISTA en el plazo previsto y del modo establecido en el presente Contrato.

En el supuesto de que las condiciones económicas del Contrato, recogidas a continuación, sufrieran cambios, las Partes pactarán por escrito los mismos y se anexarán al presente Contrato como documento inseparable.

Concepto	Importe
Establecimiento del servicio[1]	0,00 €
Servicio Preventivo y Correctivo	2.500,00 €/mes

7.2 Jornadas a demanda

- En el caso de que el Cliente solicite a CONVISTA un servicio fuera del horario establecido en el presente Contrato, el Cliente deberá aprobarlo previamente y acordarlo conjuntamente con COVISTA a través de ticketing. Dicho servicio será abonado en en base al marco tarifario acordado en el apartado siguiente.

7.3 Tarifas para la ejecución de tareas adicionales

Con la contratación del soporte Basis, se define una tarifa especial para el Cliente en el desarrollo de correctivos y evolutivos, fuera del servicio remoto definido.

[1] Se establecen 4 jornadas de establecimiento y traspaso de servicio.

Acuerdo marco para horas adicionales a la bolsa contratada:

Tipo de Intervención	Remoto[2]	Presencial
Intervención en horario de cobertura	65 €/hora	90 €/hora
Intervención fuera de horario de cobertura	105 €/hora	135 €/hora

- Para la prestación de tareas en modo presencial la prestación mínima será de ocho (8) horas.

7.4 Facturación

- Los precios de la presente propuesta no incluyen I.V.A.
- CONVISTA facturará mensualmente los servicios prestados.
- El pago de las facturas se realizará en un plazo de treinta (30) días, contados desde la fecha de recepción de las facturas por parte de CNP ASSURANCES y CNP CAUTION.
- La forma de pago será mediante transferencia bancaria al número de cuenta de CONVISTA que figure en las facturas remitidas a CNP ASSURANCES y CNP CAUTION.
- CONVISTA enviará una factura a cada empresa, según lo establecido en la cláusula 7.1, y ambas facturas serán remitirás al siguiente correo electrónico: facturas@cnp.es

7.5 Gastos de desplazamiento

No habrá gastos de desplazamiento.

8 Requerimientos y condiciones del servicio

- CONVISTA realizará su trabajo atendiendo en todo momento a lo establecido en el presente Contrato.
- El Cliente proporcionará todo el soporte técnico y funcional posible y que sea realmente necesario al equipo de CONVISTA con su conocimiento de los procesos de negocio y del entorno técnico y funcional que se necesite para llevar a cabo los servicios establecidos en el presente Contrato.
- Los retrasos que pudiesen producirse por circunstancias no atribuibles a CONVISTA no serán asumidos por CONVISTA.

[2] Para jornadas presenciales, la facturación mínima será el equivalente a una jornada de ocho horas.

- Los retrasos que pudiesen producirse por culpa de las acciones u omisiones de CONVISTA o de cualquier de sus subcontratistas serán asumidos en todo caso por CONVISTA, siendo plenamente responsable de los daños y/o perjuicios que se pudieran irrogar al Cliente o a terceros.
- Para las tareas ejecutadas de manera remota, el Cliente habilitará el acceso a sus sistemas mediante las herramientas y procedimientos necesarios a CONVISTA. El acceso a los sistemas del Cliente se realizará cumpliendo con todas las obligaciones e instrucciones del anexo 2 y el apéndice 1 del presente Contrato.
- La prestación del servicio no incluye posibles licencias software ni hardware necesario de ninguno de los aplicativos o dispositivos a utilizar,
- CONVISTA no se responsabilizará de cualquier acción o mejora que el Cliente precise realizar en sus sistemas corporativos y que no haya sido contemplado en el Contrato (aplicaciones de parches, mejoras funcionales...). No obstante a lo anterior, CONVISTA podrá realizar la acción o mejora en cuestión previa solicitud expresa y por escrito del Cliente. En el supuesto de que CONVISTA actuara sin la debida aprobación del Cliente, CONVISTA será plenamente responsable de dicha acción o mejora y asumirá su coste.

9 Aplicación de sanciones financieras

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

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

10 Obligaciones laborales de CONVISTA

La naturaleza de este Contrato es la propia de un arrendamiento de servicios de carácter exclusivamente mercantil. Por lo expuesto, no se deriva relación o vínculo laboral alguno entre las Partes, ni entre el Cliente y el personal o colaboradores de CONVISTA que, eventualmente, pudieran estar prestando alguno de los servicios que constituyen el objeto del Contrato.

En ningún caso los empleados de CONVISTA se consideran personal del Cliente, no dependiendo ni funcional ni orgánicamente y no asumiendo el Cliente responsabilidad alguna en materia laboral respecto de los mismos.

En caso de baja de alguno de los empleados de CONVISTA, este se compromete a reemplazarlo en el plazo máximo de dos (2) días laborables.

CONVISTA se obliga a cumplir y hacer cumplir con todo rigor a su personal las obligaciones impuestas por la legislación laboral, especialmente en materia de Seguridad Social y Prevención de riesgos laborales, lo que justificará en cualquier momento a petición del Cliente y deberá disponer de una persona encargada de la vigilancia y cumplimiento de tales obligaciones.

CONVISTA deberá entregar al Cliente, si así se le solicita, y mantener actualizada la siguiente documentación:

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

El incumplimiento de cualquiera de las obligaciones especificadas facultará al Cliente para resolver el Contrato siempre que, habiéndose concedido un plazo razonable de un (1) mes para la aportación de la documentación citada, CONVISTA no la hubiera presentado.

Asimismo, para el supuesto de que por resolución judicial CNP ASSURANCES o CNP CAUTION fuera condenada a hacerse cargo de personal que hubiera pertenecido a la plantilla de CONVISTA, CONVISTA deberá pagar al Cliente una cantidad igual a la que el Cliente debiera pagar a ese personal en concepto de indemnización por despido improcedente.

11 Notificaciones

Las Partes señalan como domicilios para notificaciones relacionadas con el presente contrato, los siguientes:

1. **CNP ASSURANCES y CNP CAUTION** mediante notificación:

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

   Carrera de San Jerónimo, n.º 21

   28014 – Madrid

   peticiones@cnp.es

2. **CONVISTA** mediante notificación a:

   CONVISTA CONSULTING & ADVISORS S.L.U.

   Calle Santa Leonor, n.º 65, Edificio E, Planta 3

28037 - Madrid

Las notificaciones serán válidas cuando se realicen mediante alguno de los procedimientos siguientes:

- Comunicación escrita privada remitida por cualquier medio que permita dejar constancia de su recepción por la otra Parte.

Comunicación escrita privada presentada en el domicilio de la otra Parte y en la que conste sello y/o firma del destinatario como prueba de su recepción

12 Cláusula de prevención frente al fraude, soborno y corrupción

CNP ASSURANCES y CNP CAUTION tienen tolerancia cero en lo que se refiere a prácticas de soborno y corrupción, así como mantienen un estricto control para prevenir el fraude por lo que cuentan con políticas cuyo objetivo es prevenir estas prácticas en el seno de ambas entidades y en cualquier relación con terceros. Se adjunta como **Anexo 1** carta sobre los Principios Éticos que aplican a CNP ASSURANCES y CNP CAUTION y de los que CONVISTA debe ser conocedor y respetar en sus relaciones con CNP ASSURANCES y CNP CAUTION.

Con base a lo anterior, CONVISTA declara contar con políticas y procedimientos internos adecuados aplicables a sus empleados, así como a cualquier tercero que colaboren con ella, para prevenir y evitar la participación en actividades relacionadas con el fraude, la corrupción y el soborno y que serán de aplicación en el desarrollo del presente Contrato. Adicionalmente las Partes declaran que el Contrato se celebra única y exclusivamente para desarrollar objetivos de negocio, y que en ningún caso atiende a intereses particulares de cualesquiera de las Partes o al propósito de obtener una ventaja indebida para una de las Partes, uno de sus empleados o directivos.

En concreto, CONVISTA garantiza, en relación con el presente Contrato, que no existirán ventajas financieras o de cualquier otro tipo que hayan sido acordadas o que lo puedan ser en el futuro con cualquier persona perteneciente a CNP ASSURANCES y CNP CAUTION.

El incumplimiento de cualquiera de las previsiones anteriores será considerado como un incumplimiento grave del Contrato y dará derecho a CNP ASSURANCES y a CNP CAUTION a su terminación inmediata sin perjuicio de cualesquiera otras acciones legales que les puedan corresponder.

13 Independencia de las Partes

Este Contrato no convierte a ninguna de las Partes en representante legal de la otra, y no crea ningún tipo de asociación o empresa en común. Las Partes actúan como contratistas independientes y asumen plenamente y en nombre propio sus respectivas obligaciones, derivadas de este Contrato.

14 Cesión y subcontratación

Las Partes no podrán ceder el presente Contrato sin el previo consentimiento por escrito de la otra.

CONVISTA no podrá subcontratar a una tercera parte para la prestación de los servicios establecidos en el Contrato salvo que medie previo consentimiento y por escrito del Cliente.

En el caso de que CONVISTA recurra a subcontratistas para llevar a cabo los servicios descritos en el presente Contrato deberá obtener autorización previa y por escrito del Cliente. A tal efecto, CONVISTA informará por escrito al Cliente con carácter previo de las subcontrataciones previstas, facilitando los datos de los terceros a los que pretenda subcontratar. Si el Cliente no manifestara por escrito su oposición a dicha subcontratación en el plazo de cinco (5) hábiles desde la recepción de la notificación correspondiente, se entenderá que no se oponen a la misma. Los mismos términos y obligaciones resultarán aplicables en el supuesto de que CONVISTA tuviera intención de sustituir a alguno o algunos de sus subcontratistas.

15 Términos y condiciones

15.1 Confidencialidad

El uso que CONVISTA realice de los datos de CNP ASSURANCES y CNP CAUTION tendrá, en cualquier caso, carácter confidencial y se adecuará a los fines estipulados en el Contrato.

Todo el personal de CONVISTA que pueda tener acceso a información confidencial propiedad de CNP ASSURANCES y CNP CAUTION está sujeto al más estricto secreto profesional. A estos efectos se entenderá por personal (filiales, directivos, empleados, subcontratados o persona interpuesta).

CONVISTA y su personal estará obligada a guardar absoluta confidencialidad por si misma o a través de terceros sobre cualquier información del Cliente que sea considerada como secreto comercial o empresarial y a la que CONVISTA tenga acceso como consecuencia del cumplimiento de sus obligaciones bajo el contrato. La revelación y cesión de dicha información confidencial a terceros no relacionados con el cumplimiento del Contrato sólo podrá llevarse a cabo con el previo consentimiento por escrito de CNP ASSURANCES y de CNP CAUTION. La información confidencial tampoco podrá entregarse a las autoridades salvo que medie un mandato solicitando la información.

El Cliente estará obligados a guardar absoluta confidencialidad sobre cualquier know-how comercial, técnico o científico de CONVISTA que les sea revelado durante el periodo de vigencia del contrato correspondiente y a no revelar dicha información confidencial a ningún tercero, salvo previa autorización por escrito de CONVISTA o cuando haya solicitado formalmente por una autoridad administrativa.

15.2 Protección de datos

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la normativa nacional sobre protección de datos

aplicable (incluyendo las disposiciones específicas sobre protección de datos incluida en la normativa del sector seguros de aplicación en cada momento) y/o cualquier otra legislación que las modifique o sustituya en un futuro, será de obligado cumplimiento para cada una de las partes.

CONVISTA no tendrá acceso a ningún dato de CNP ASSURANCES y de CNP CAUTION.

15.3 Datos personales de los firmantes

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

¿Quién es el Responsable del Tratamiento de sus Datos Personales?	Por parte de CONVISTA: **ConVista Consulting** Dirección postal: C/Josep Pla 2, Edificio B3 – Planta 4, E-08019 Barcelona Delegado de Protección de Datos: Oscar.Barrios@convista.com Por parte de **CNP ASSURANCES y CNP CAUTION**: CNP ASSURANCES SUCURSAL EN ESPAÑA Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpspain.eu CNP CAUTION SUCURSAL EN ESPAÑA: Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpspain.eu
¿Con qué finalidad se tratan sus Datos personales?	La finalidad del Tratamiento de los firmantes y las personas de contacto es gestionar de forma adecuada la relación contractual objeto de este Contrato. Las Partes tratarán estos datos para satisfacer el interés legítimo que tienen ambas compañías de mantener el contacto entre ellas durante la prestación de los servicios. Los Datos Personales serán conservados mientras sean necesarios para cumplir con las obligaciones contractuales y legales asumidas.
¿Cuál es la legitimación para el Tratamiento de sus Datos Personales?	La base de legitimación deriva del interés legítimo de cada una de las Partes de mantener relaciones de cualquier índole con la otra para cumplir con las condiciones del Contrato.
¿Cuáles son sus derechos cuando facilita sus Datos Personales?	Los sujetos interesados tienen derecho a obtener confirmación sobre si las Partes están tratando Datos Personales que les conciernan, o no. En particular, tienen derecho a: Acceder a sus Datos Personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. En determinadas circunstancias, pueden solicitar la limitación del Tratamiento de sus Datos Personales, en cuyo caso

	únicamente serán conservados para el ejercicio o la defensa de reclamaciones. Asimismo, también tiene derecho a oponerse al Tratamiento de sus Datos Personales. En tal caso, el Responsable del Tratamiento dejará de tratar los Datos Personales, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. Los representantes de las Partes pueden ejercer los referidos derechos dirigiendo un correo electrónico a cada una de las direcciones electrónicas designadas en la primera fila de esta tabla. Puede obtener información adicional acerca de sus derechos ante la Agencia Española de Protección de Datos en www.agpd.es Cuando el representante no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Agencia Española de Protección de Datos en www.agpd.es .

15.4 Obligaciones del Cliente

En el marco de sus actividades empresariales, el Cliente estará obligado a prestar la asistencia y el soporte razonables que precise CONVISTA para el efectivo cumplimiento de las obligaciones pactadas en el presente Contrato, así como crear las condiciones necesarias para el adecuado cumplimiento de las obligaciones contractuales de CONVISTA y a facilitar puntualmente a CONVISTA toda la documentación y demás información que le sea requerida y que sea absolutamente necesaria en cada momento y que el Cliente disponga en dicho momento. En el supuesto de que no dispusiera de la información solicitada, el Cliente dispondrá de un plazo razonable de tiempo para la entrega de la misma.

15.5 Obligaciones de CONVISTA

Además de las obligaciones establecidas con relación a CONVISTA en el presente Contrato, CONVISTA deberá solicitar la información necesaria al Cliente para la prestación de los servicios contratados, así como a solicitar el soporte técnico y funcional necesario para el desarrollo de los servicios contratados. Si CONVISTA, siendo necesario, no lo solicitara, los daños y perjuicios que se ocasionaren serían de su exclusiva responsabilidad.

15.6 Información propiedad de CONVISTA

Se entiende por información propiedad de CONVISTA todos aquellos elementos desarrollados por CONVISTA con carácter previo a este Proyecto. A modo de ejemplo, todo código propiedad de CONVISTA (librerías, frameworks...) desarrollado previamente a modo de componente reutilizable, que sea utilizado en el ámbito de este Proyecto para acelerar su ejecución, seguirá siendo propiedad de CONVISTA, permitiéndose sin coste alguno su utilización indefinida única y exclusivamente dentro del ámbito del proyecto ofertado en esta propuesta, no pudiendo ser reutilizado por el Cliente o terceros ni cedido a terceros por parte del Cliente sin autorización expresa y por escrito de CONVISTA. En caso de utilizar estos elementos, CONVISTA informará

por escrito al Cliente sobre la existencia de este tipo de información de su propiedad durante la ejecución del Proyecto.

15.7 Propiedad del sistema y de la solución

El Cliente será titular en exclusiva de todos los derechos de explotación derivados de la Propiedad Intelectual del programa de ordenador o parte del programa que resulte de desarrollos específicos que puedan ser objeto de la prestación de los servicios contratados, a cuyo efecto CONVISTA cede a favor del Cliente su uso, no pudiendo reutilizarse por parte de CONVISTA en otros clientes salvo consentimiento previo, expreso y por escrito del Cliente.

CONVISTA garantiza que los trabajos y servicios prestados al Cliente en la ejecución de este Contrato no infringen derechos de Propiedad Intelectual o Industrial o cualesquiera otros derechos de terceros, haciéndose CONVISTA, en todo caso, plena e individualmente responsable de toda clase de reclamaciones y/o indemnizaciones por razón de este concepto frente a todo tipo de terceros.

15.8 Causas de terminación anormal

El presente contrato podrá ser extinguido de forma unilateral por CONVISTA, con independencia de cualquier otra causa de resolución indicada en este Contrato y/o en la Ley, en los supuestos siguientes:

1. Si el Cliente no hubiera abonado facturas emitidas y vencidas, una vez apercibidos de impago por escrito con acuse de recibo o de cualquier otro modo que dejara constancia del recibimiento del apercibimiento y no habiendo subsanado esta contingencia en el plazo improrrogable de treinta (30) días naturales, CONVISTA queda liberado de seguir prestando cualquier tipo de servicios pudiendo, a partir de ese momento, cancelar la prestación de los servicios con el Cliente, incluso cesar la prestación del control remoto, como el mantenimiento en uso de los servidores contratados con CONVISTA, quedando a su vez liberado el Cliente de cualquier obligación, salvo el abono de las cantidades debidas a CONVISTA por servicios ya prestados.
2. La no realización o la realización defectuosa de los servicios estipulados en el presente Contrato por parte de CONVISTA dará derecho al Cliente a resolver el Contrato, pudiendo en su caso solicitar a CONVISTA la pertinente indemnización por los daños y/o perjuicios ocasionados al Cliente por razón de su acción u omisión.
3. Si cualquiera de las Partes fuera declarada en concurso a instancia de acreedor legítimo, o si presentara solicitud de concurso voluntaria o suspensión de pagos, o si se hubieran instado en su contra juicios ejecutivos o decretados embargos preventivos u otras medidas cautelares que pongan de manifiesto la disminución de la solvencia económica o dificultades financieras para atender al normal cumplimiento de sus obligaciones.
4. Cualquier incumplimiento relativo a la Información Confidencial.

16 Nulidad o anulabilidad

Cualquier modificación de los presentes Términos y Condiciones Generales o de los Anexos, sólo será válida si se efectúa mediante instrumento escrito firmado por ambas Partes.

Si cualquiera de las estipulaciones del presente Contrato resultase nula o inválida, la nulidad o invalidez de las mismas no afectará a las demás estipulaciones, las cuales se mantendrán en vigor y seguirán surtiendo plenos efectos.

La renuncia por cualquier de las Partes a exigir en un momento determinado el cumplimiento de uno cualquiera de las estipulaciones aquí estipuladas no implicará una renuncia con carácter general ni creará un derecho adquirido por la otra Parte.

17 Legislación aplicable

El presente Contrato se halla sujeto a las disposiciones de la Ley española.

18 Jurisdicción aplicable

En caso de que surgiera entre las Partes cualquier discrepancia o conflicto derivado de la interpretación o cumplimiento del presente Contrato las Partes, con renuncia a su propio fuero o aquel que pudiera corresponderles, se someten expresamente al fuero de los Juzgados y Tribunales de Madrid capital.

19 Contrato completo

El presente Contrato constituye la totalidad del convenio regulador de la relación contractual que se establece entre las Partes en las materias objeto del presente Contrato con efectos a la fecha de la firma y, en consecuencia, quedan anulados y sustituidos cuantos acuerdos, convenios y contratos pudieran haberse concluido entre las mismas partes sobre el mismo objeto con anterioridad a este acto.

20 Firma del contrato

Y, a tal efecto, las partes firman el presente contrato por duplicado en Madrid, a 13 de junio de 2022.

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España	**POR CONVISTA CONSULTING & ADVISORS S.L.U.**
Fdo.: David Lattes	**Fdo.:** Norbert Nielsen

ANEXO 1

AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

(Principios Éticos Grupo CNP)

ENTRE

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

Y

CONVISTA CONSULTING & ADVISORS S.L.U.

ANEXO 1 AL
CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

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

ÉTICA DE NEGOCIOS.
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

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

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

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

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

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

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

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

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

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

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

Y en prueba de recepción el suscribiente en el carácter con el que interviene, firma el presente anexo en Madrid a 13 de junio de 2022.

Por duplicado a un solo efecto.

POR CONVISTA CONSULTING & ADVISORS S.L.U.

Fdo.: Norbert Nielsen

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SOPORTE BASIS

ENTRE

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

E

CONVISTA CONSULTING & ADVISORS S.L.U.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

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

Introducción

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

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

   - los Datos del CLIENTE; incluida la Información Confidencial del CLIENTE.
   - toda información relativa a EL CLIENTE.
   - cualquier otra información utilizada en la prestación de los Servicios;
   - los sistemas informáticos del CLIENTE y del PROVEEDOR (incluidos los Sistemas del PROVEEDOR) que procesen, almacenen o transmitan información; y
   - el código informático utilizado para procesar Datos del CLIENTE incluida la Información Confidencial del CLIENTE.

Funciones y Responsabilidades

Cumplimiento

- Se establecerán reuniones de seguimiento para comprobar el cumplimiento de sus obligaciones establecidas en el presente contrato de forma mensual.
- Sin perjuicio de las demás acciones y vías de reparación a las que pueda recurrir al CLIENTE, todo incumplimiento comunicado por EL PROVEEDOR al CLIENTE de acuerdo con lo dispuesto en el apartado Cumplimiento, dará lugar a una valoración del riesgo por parte del CLIENTE que indicará al PROVEEDOR en el plazo de tiempo del que dispondrá para poner en práctica las medidas correctoras que resulten necesarias.
- EL PROVEEDOR se compromete a colaborar en las auditorías realizadas por el CLIENTE, y entregará al CLIENTE las evidencias, informes y certificados necesarios para asegurar que cumple con los términos del presente Contrato en un periodo razonable.

Valoración del riesgo

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

Personal del PROVEEDOR

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

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

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

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

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

Educación, Formación y Sensibilización

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

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

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

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

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

- otras cuestiones relacionadas con la Seguridad Informática;

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

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

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

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

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

Responsable de Seguridad del PROVEEDOR

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

El Responsable de Seguridad del PROVEEDOR deberá:

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

Incidentes de Seguridad

Notificación de los Incidentes de Seguridad

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

notificación dentro de las veinticuatro (24) horas naturales siguientes al momento en que EL PROVEEDOR hubiese tenido conocimiento de dicho Incidente de Seguridad.

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

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

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

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

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

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

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

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

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

Si, en opinión del CLIENTE, un subcontratista o cualquier Tercero Proveedor fuese considerado no apto tras la correspondiente revisión de la seguridad, EL CLIENTE podrá exigir al PROVEEDOR (en el plazo de tiempo que EL CLIENTE considere apropiado) que deje de recurrir a dicho Subcontratista o a ese Tercero, y que encuentre un sustituto que EL CLIENTE considere aceptable. Alternativamente, y únicamente a instancias del CLIENTE, EL CLIENTE podrá aceptar un compromiso del Subcontratista por el que se obligue a acordar con EL PROVEEDOR un plan correctivo legalmente vinculante, en el que deberán indicarse las acciones y los plazos necesarios para subsanar las deficiencias puestas de manifiesto a través de la revisión, y cuya finalización exitosa deberá ser aprobada por EL CLIENTE.

Derecho de inspección del CLIENTE

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

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

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

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

Valoración de la Seguridad

EL CLIENTE podría contratar, a su costa, a un Tercero Evaluador de la Seguridad que realizará al menos una Valoración de la Seguridad con el fin de evaluar el nivel de cumplimiento del presente contrato bajo demanda durante el período de vigencia de este.

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

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

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

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

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

Gobierno de la seguridad de la información

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

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

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

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

Política de Seguridad de la Información

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

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

Gestión de Activos

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

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

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

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

Control de Acceso

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

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

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

Acceso Privilegiado
EL PROVEEDOR se asegurará de que:

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

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

- los mecanismos de autenticación deben garantizar que no puedan ser eludidos para obtener un acceso no autorizado a los sistemas;
- los datos de autenticación, incluidas las contraseñas, no deben almacenarse de una forma que permita que los mismos puedan ser recuperados en un formato legible o descifrable; y
- las contraseñas deben ser complejas e incluir una combinación de distintos tipos de caracteres y tener una longitud suficiente para evitar ataques exhaustivos o de diccionario.
- Relativo a las contraseñas para dar servicio al CLIENTE, se podrá pactar la política de contraseñas junto con EL CLIENTE.

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

Configuración del Sistema

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

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

Monitorización de los sistemas

Registro de Sucesos
EL PROVEEDOR mantendrá registros de todos los sucesos clave, y en especial de los que sean susceptibles de afectar a la confidencialidad, la integridad y la disponibilidad de los Servicios

prestados al CLIENTE que servirán para facilitar la identificación y la investigación de los Incidentes y/o incumplimientos significativos de los derechos de acceso que se produzcan en relación con los Sistemas del PROVEEDOR.

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

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

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

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

Seguridad de la Red

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

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

Los sistemas de CLIENTE gestionados por el PROVEEDOR estarán respaldados por diagramas precisos y actualizados que incluirán todos los componentes del sistema y las interfaces con otros sistemas. Estos diagramas se pondrán a disposición del CLIENTE bajo petición en un tiempo razonable tras la solicitud.

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

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

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

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

Las reglas se revisarán cada SEIS (6) meses y se mostrará el resultado en la revisión periódica del servicio junto al CLIENTE.

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

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

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

Criptografía

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

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

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

Protección Contra Código Malicioso

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

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

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

Gestión de los cambios y parches

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

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

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

Los parches de seguridad y demás actualizaciones relativas a la vulnerabilidad de la seguridad sólo se aplicarán si están disponibles y han sido previamente aprobados, a menos que su utilización suponga un riesgo mayor para el negocio. Se instalarán medidas de seguridad adicional en los Sistemas del PROVEEDOR que, por cualquier motivo, no puedan actualizarse, para que el sistema vulnerable quede totalmente protegido. Todos los cambios deben realizarse de acuerdo con el proceso de gestión de cambios aprobado.

EL PROVEEDOR dispondrá de un proceso documentado para identificar y subsanar mensualmente las vulnerabilidades de seguridad que presente el *software SAP* entregado a EL CLIENTE y facilitará al CLIENTE las actualizaciones correspondientes en cuanto estén disponibles. Así como, las soluciones temporales que sirvan para mitigar el riesgo en caso de no existir un parche oficial disponible.

Los parches de seguridad de sistema operativo que se aplicarán de manera semestral. Aquellos parches cuyo impacto sea muy alto se documentarán y se podrían no instalar en mutuo acuerdo entre EL CLIENTE y EL PROVEEDOR.

Gestión de Terceros

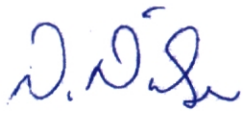
Acuerdos con Terceros
EL PROVEEDOR se asegurará de que las conexiones de Terceros se sometan a una valoración del riesgo, y de que sean aprobadas y acordadas por ambas partes a través de un acuerdo documentado, como puede ser un contrato.

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

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

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

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España	**POR CONVISTA CONSULTING & ADVISORS S.L.U.**
Fdo.: David Lattes	**Fdo.:** Norbert Nielsen



ANEXO 3

AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

ENTRE

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

Y

CONVISTA CONSULTING & ADVISORS S.L.U.

ANEXO 3 AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

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

1. Acuerdos de Nivel de Servicio

Los criterios de priorización que se seguirán, así como los diferentes Acuerdos de Nivel de servicio por servicio y prioridad atendiendo a los siguientes indicadores:

Indicador	Descripción	Medida
Tiempo de entrega de Mantenimiento Preventivo	Las soluciones, según su clasificación simple o compleja, deben entregarse en la fecha planificada.	Días de desviación respecto a la fecha prevista.
Tiempo promedio para el inicio de atención de incidencias	Tiempo promedio que se tarda en iniciar la resolución de una solicitud de servicio.	Tiempo desde la recepción de la petición hasta el inicio de su resolución)/(Nº total de solicitudes recibidas)
Porcentaje de Resolución incidencias	Cantidad total de incidencias resueltas en un tiempo menor al valor objetivo establecido.	(Nº incidencias resultas en -X horas)/(Nº incidencias resueltas en el periodo contractual)
Elaboración y Entrega de los Informes sobre el estado de los elementos relevantes, así como el informe de monitorización de los sistemas SAP.	Mide que los informes críticos se manden en los plazos establecidos	(Nº informes rechazados en el periodo)/(Nº informes entregados en el periodo)

2. Incumplimiento de los Acuerdos de Nivel de Servicio

En caso de incumplimiento de los niveles de servicios se aplicará la penalización correspondiente, computando cada SLA incumplido con 1 punto.

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:

- Si la suma de puntos de penalización igual a 1 → No se aplicará penalización alguna
- Si la suma de puntos de penalización está entre 2 y 3 → Se aplicará un 5% de penalización sobre el importe de la facturación mensual.
- Si la suma de puntos de penalización es superior a 4 → Se aplicará un 10% de penalización sobre el importe de la facturación mensual.

ANEXO 3 AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

Si alguno de los indicadores marcados con 2 puntos de penalización se incumpliera durante dos (2) meses seguidos se deberá presentar en el siguiente Comité de Streering Commite donde el Cliente decidirá si se aplica un 5% de penalización sobre la facturación por cada indicador incumplido.

Y en prueba de recepción el suscribiente en el carácter con el que interviene, firma el presente anexo en Madrid a 13 de junio de 2022.

Por duplicado a un solo efecto.

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

Fdo.: David Lattes

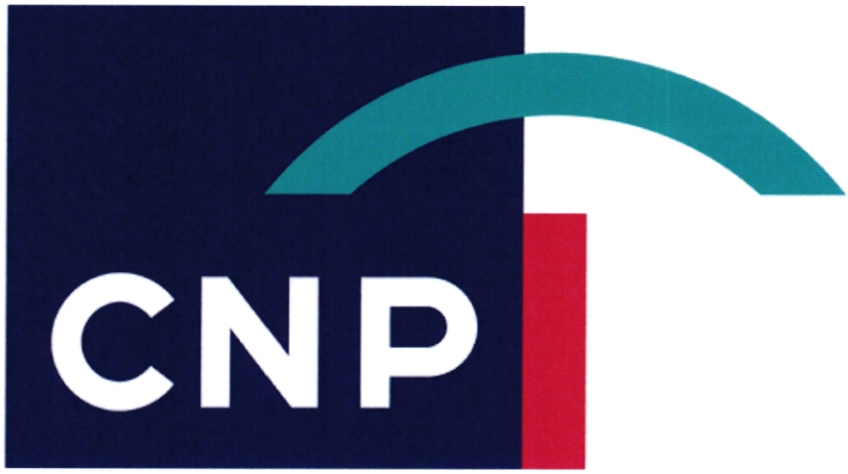
POR CONVISTA CONSULTING & ADVISORS S.L.U.

Fdo.: Norbert Nielsen

CONVISTA
moving ahead

Contrato de Servicios

Soporte Basis – CNP Assurances, S.A., Sucursal en España y CNP Caution, Sucursal en España



Created by: ConVista Consulting & Advisors, SLU

Version	Date	Author	Change
1.0	23.05.2022	Norbert Nielsen	

Índice de contenidos

1 INTRODUCCIÓN 4
1.1 Marco previo 4
1.2 Motivación y objetivos 4
2 Descripción del servicio 5
2.1 Ámbito de cobertura 5
2.2 Establecimiento del Servicio 6
2.3 Monitorización y continuidad de los entornos SAP 6
2.3.1 Monitorización del estado actual del sistema 6
2.3.2 Continuidad de los entornos 7
2.4 Respaldo técnico experto para el soporte a entornos SAP 7
2.4.1 Ejecución de acciones correctivas y/o preventivas 8
2.4.2 Gestión y resolución de solicitudes de servicio e incidencias 8
2.5 Tareas cubiertas por el servicio 8
2.5.1 Administración y mantenimiento del sistema SAP 9
2.5.2 Escalado de incidencias a SAP 9
2.5.3 Administración y mantenimiento de la base de datos 9
3 Horario del servicio 10
4 Limitaciones del servicio 10
4.1 Servicios adicionales no incluidos 10
4.2 Servicios excluidos 10
5 Organización del servicio 11
5.1 Modalidad de prestación del servicio 11
5.2 Canales de comunicación con el Centro de Operaciones 11
6 Duración del servicio 12
6.1 Periodo de contratación del servicio 12
6.2 Cancelación anticipada del Contrato 12
7 Propuesta económica 13
7.1 Coste del servicio 13
7.2 Jornadas a demanda 13
7.3 Tarifas para la ejecución de tareas adicionales 13
7.4 Facturación 14
7.5 Gastos de desplazamiento 14

8 Requerimientos y condiciones del servicio 14

9 Aplicación de sanciones financieras 15

10 Obligaciones laborales de CONVISTA 15

11 Notificaciones 16

12 Cláusula de prevención frente al fraude, soborno y corrupción 17

13 Independencia de las Partes 17

14 Cesión y subcontratación 18

15 Términos y condiciones 18

15.1 Confidencialidad 18

15.2 Protección de datos 18

15.3 Datos personales de los firmantes 19

15.4 Obligaciones del Cliente 20

15.5 Obligaciones de CONVISTA 20

15.6 Información propiedad de CONVISTA 20

15.7 Propiedad del sistema y de la solución 21

15.8 Causas de terminación anormal 21

16 Nulidad o anulabilidad 21

17 Legislación aplicable 22

18 Jurisdicción aplicable 22

19 Contrato completo 22

20 Firma del contrato 23

1 INTRODUCCIÓN

1.1 Marco previo

CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA Y CNP CAUTION, SUCURSAL EN ESPAÑA desean formalizar la petición de servicios realizada a CONVISTA para cubrir los servicios deseados de "*Soporte Basis para CNP Assurances, S.A., Sucursal en España y CNP Caution, Sucursal en España*"

CONVISTA es una empresa especializada en la prestación de servicios cuya actividad cubre las necesidades de CNP ASSURANCES S.A., SUCURSAL EN ESPAÑA Y CNP CAUTION, SUCURSAL EN ESPAÑA. .

REUNIDOS

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

Ambas denominadas conjuntamente en adelante como el "**CLIENTE**".

Y, DE OTRA PARTE, **D. NORBERT NIELSEN**, mayor de edad, con domicilio a estos efectos en Calle Santa Leonor, n.º 65, Edificio E, Planta 3, 28037, Madrid, y con N.I.E. número X-3584601-M, en nombre y representación de la mercantil "**CONVISTA CONSULTING & ADVISORS S.L.U.**", con domicilio a estos efectos en Calle Santa Leonor, n.º 65, Edificio E, Planta 3, 28037, Madrid y con C.I.F. n.º B-62421805 (en adelante, el "**PROVEEDOR" o "CONVISTA**").

El CLIENTE y el PROVEEDOR, podrán ser denominadas individual e indistintamente como "**la Parte**" y conjuntamente como "**las Partes**", reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente contrato (en adelante, el "**Contrato**").

1.2 Motivación y objetivos

El Cliente solicita a CONVISTA sus servicios de Soporte Remoto SAP Basis, con el propósito de asegurar el correcto funcionamiento de sus respectivos sistemas.

Así pues, el servicio ofertado por CONVISTA responde a las necesidades planteadas por el Cliente.

- Monitorización de los sistemas SAP y envío de alertas ante caídas;
- Respaldo técnico experto, ágil y flexible, para gestión de solicitudes e incidencias;

- Asesoramiento experto en la evolución y mejora continuada de los sistemas SAP.

La presente propuesta, de carácter anual, es decir, doces(12) meses, responde a la necesidad planteada por el Cliente de asegurar un soporte para el correcto funcionamiento de sus sistemas productivos SAP, así como un asesoramiento experto en la evolución y mejora continuada de los mismos.

2 Descripción del servicio

2.1 Ámbito de cobertura

El ámbito de cobertura de este Contrato son los entornos actuales de SAP en:

- SAP S4/HANA (Dev + QA + Prod)
- SAP Solution Manager

CONVISTA dará soporte remoto a las necesidades que el Cliente pueda tener en el ámbito de gestión de sistemas SAP Basis. El servicio ofertado abarca el soporte a tareas relacionadas con la gestión y explotación del sistema según tres niveles o tipologías:

- **Correctivos:** Incidencias que afecten al buen funcionamiento del sistema.
- **Preventivos:** Iniciativas que ayuden a prevenir incidencias futuras.
- **Evolutivos:** Nuevas funcionalidades o cambios en la infraestructura existente serán valorados aparte y no están incluidos en la presente propuesta.

Con este propósito, el servicio se estructura en tres niveles:
- Monitorización y continuidad de los entornos SAP productivos.
- Asesoramiento experto en la evolución de los sistemas SAP.
- Respaldo técnico experto para el soporte a los entornos SAP.

Queda dentro del alcance del Contrato:
- Proyecto de Establecimiento del servicio.
- Mantenimiento correctivo.
  - Monitorización y reacción proactiva de alertas continua.
  - Supervisión diaria de los principales procesos e indicadores de rendimiento del sistema.
  - Tratamiento de incidencias de segundo nivel.
  - Apertura y tratamiento de notas a SAP.
- Mantenimiento preventivo.
  - Gestión y monitorización del servicio, incluyendo reuniones de seguimiento con el equipo designado por el Cliente.
  - Análisis, planificación y ejecución de las recomendaciones del EarlyWatch Alert previa consolidación con el cliente.

A continuación, se indican los grandes bloques que definen el servicio ofertado:

Establecimiento del servicio	Servicio Correctivo	Servicio Preventivo	Gestión
•Procedimiento previo a la puesta en marcha del servicio.	•Gestión de requerimientos que se deban corregir o modificar, según prioridad.	•Serie de acciones orientadas a ser proactivo y prevenir futuros problemas.	•Informes de seguimiento e informes ejecutivos.

Es necesario tener una conexión permanente mediante una red privada virtual (Túnel VPN) para la monitorización automática de los sistemas. En caso de no ser posible la línea VPN punto a punto no será posible establecer la monitorización automática.

2.2 Establecimiento del Servicio

CONVISTA tiene definido un procedimiento de "Establecimiento del Servicio" previo al comienzo del servicio, que asegura el éxito del traspaso de competencias y que incluye las siguientes tareas:

Tareas de establecimiento del servicio
Toma de datos de los sistemas SAP cubiertos
Definición de los usuarios y privilegios (roles) a utilizar por el equipo CONVISTA
Identificación de los Key User (usuarios clave, adelante "KU") del cliente
Definición de los usuarios y privilegios a utilizar por los KU en la herramienta de ticketing de CONVISTA
Configuración de la línea de comunicación con el Centro de Servicios Gestionados de CONVISTA
Presentación y comunicación del servicio y su funcionamineto a Usuarios Clave

2.3 Monitorización y continuidad de los entornos SAP

El propósito de este bloque es monitorizar periódicamente el estado de los entornos SAP del Cliente contratados, con objeto de controlar su estado y disponer de información para prevenir posibles incidencias y prescribir acciones correctivas.

2.3.1 Monitorización del estado actual del sistema

El equipo de CONVISTA realizará una serie de verificaciones de los principales parámetros del sistema para asegurar el buen funcionamiento del mismo. Fruto de esta revisión, CONVISTA enviará un Informe de estado de los elementos relevantes de los sistemas monitorizados, junto con una valoración del estado de los mismos, así como elementos a revisar para asegurar su

buen funcionamiento. La periodicidad del envío de los informes al Cliente será mensual, con un máximo de diez (10) días laborales desde que finaliza el mes.

Este proceso de revisión del sistema incluirá, entre otros, los siguientes conceptos:

- **Revisión y análisis de los sistemas SAP contratados.**
  Estado de las instancias y de los procesos de trabajo, Usuarios conectados, Rendimiento del sistema, Órdenes de actualización, Log del sistema, Jobs de reorganización y Jobs cancelados, RFC transaccional, Buffers de servidor de aplicaciones SAP, "Short dumps" de ABAP, Entradas de bloqueo y todas las medidas de seguridad incluidas en el anexo 2, apéndice 1. **Revisión y análisis de la base de datos subyacente a los sistemas SAP contratados.**

  "Tablespaces" e índices, histórico de la base de datos, tareas de base de datos, lanzamiento de backup integrado y revisión de "logs" y rendimiento de base de datos.

- **Sistema operativo de los sistemas SAP contratados.**
  Análisis del sistema de archivos y monitor de Sistema Operativo a nivel básico.

2.3.2 Continuidad de los entornos

CONVISTA deberá detectar cualquier desvío no controlado de los principales parámetros definidos para asegurar la continuidad de los sistemas monitorizados. En tal caso, se procederá a una intervención manual, en principio, de manera remota, aunque podría ser presencial, si fuera necesario, para subsanar el problema, siempre dentro del horario de cobertura contratado. Para ello, por un lado, el Cliente y, por otro lado, CONVISTA definirán conjuntamente el procedimiento de reacción ante estas situaciones, regulándose en el correspondiente anexo al presente Contrato.

Las alertas a monitorizar incluidas en la presente propuesta son las siguientes:

- Paradas no programadas de los entornos monitorizados.
- Errores en los servicios del servidor de aplicación SAP.
- Todas aquellas alertas recogidas en el anexo 2, apéndice 1 del presente Contrato.

2.4 Respaldo técnico experto para el soporte a entornos SAP

Dada la transcendencia de los sistemas SAP del Cliente sobre el negocio, además de asegurar su buen funcionamiento, es primordial planificar con antelación tanto su evolución como las acciones preventivas necesarias para asegurar su correcto funcionamiento a medio y largo plazo en función de los cambiantes requerimientos del negocio. CONVISTA asignará un especialista que llevará a cabo las siguientes tareas:

- Soporte experto en la resolución de dudas y/o consultas relacionadas con los entornos SAP.
- Revisión y análisis del informe mensual de monitorización de los sistemas SAP.

- Generación de un informe de recomendaciones, enviadas al Cliente de forma bimestral, a ejecutar en tres ámbitos:
  - Correctivos: Riesgos a corto plazo;
  - Preventivos: Potenciales riesgos a medio o largo plazo;
  - Evolutivos: Optimización y evolución de la infraestructura SAP.

Por defecto, este bloque del servicio se prestará en horario laboral y en remoto sobre los sistemas contratados, pudiendo extenderse si fuese necesario y previa aprobación del Cliente, según la cobertura horaria.

Las acciones correctivas y preventivas quedan incluidas en el marco del presente Contrato. Las tareas evolutivas ejecutadas en este servicio se facturarán según tarifas vigentes para cada perfil y previa aceptación del CLIENTE.

2.4.1 Ejecución de acciones correctivas y/o preventivas

Se consideran acciones correctivas y/o preventivas todas aquellas detectadas por el equipo CONVISTA en la monitorización diaria del sistema y cuya ejecución ha sido propuesta por los mecanismos establecidos. Una vez ejecutada la acción, CONVISTA pondrá a disposición del Clienteun resumen detallado de la misma que enviará al Cliente todos los meses.

2.4.2 Gestión y resolución de solicitudes de servicio e incidencias

Se consideran solicitudes de servicio o incidencias aquellas reportadas por el personal del Cliente a través de los canales estipulados (ticketing) al centro de operaciones de CONVISTA, cuyo ámbito se corresponda con los servicios ofertados en la presente propuesta.

El proceso de gestión y resolución de las solicitudes e incidencias consta de al menos los siguientes pasos:

- Notificación y registro de la solicitud o incidencia en el Centro de Operaciones.
- Análisis de la solicitud o incidencia y sus repercusiones sobre el entorno.
- Clasificación de la prioridad definida entre el Cliente y CONVISTA.
- Asignación de recursos y planificación de la acción según prioridad.
- En caso de ser necesario, propuesta de solución alternativa temporal.
- Resolución de la solicitud o incidencia.
- Informe de gestión y/o ejecución mensual de las mismas que tendrá que ser reportado al Cliente con un máximo de diez (10) días laborales desde que finaliza el mes..

2.5 Tareas cubiertas por el servicio

A continuación, se detallan el conjunto de tareas cuyo ámbito de ejecución se encuentra recogido bajo la presente propuesta:

2.5.1 Administración y mantenimiento del sistema SAP

- Recuperación del sistema ante caídas.
- Cambios de versión de la base de datos.
- Mantenimiento de los perfiles de instancia del entorno.
- Mantenimiento de los modos de operación del entorno.
- Mantenimiento del acceso a la infraestructura vía VPN.
- Informar al proveedor de la infraestructura de las acciones de mantenimiento de hardware.
- Gestión de la capa de transporte entre sistemas.
- Mantenimiento de los ficheros de órdenes de transporte.
- Gestión de los destinos SAP RFC y conexiones del sistema.
- Gestión del subsistema de Jobs y ejecución de procesos de fondo.
- Administración de los servicios de impresión.
- Ajuste de la memoria compartida y buffers de los sistemas SAP.
- Descarga y aplicación de parches y actualizaciones por componente. Se incluye la aplicación de parches recomendados por notas de SAP, pero no la migración de base de datos.
- Copias de mandante (bajo petición).
- Copias homogéneas / refrescos de sistemas (bajo petición, el contrato incluye 1 refresco por sistema y año).
- Todas aquellas alertas recogidas en el anexo 2, apéndice 1 del presente Contrato.

2.5.2 Escalado de incidencias a SAP

- Búsqueda de notas y mensajes SAP OSS, así como su aplicación.
- Gestión de la conexión OSS (On-line Service System).
- Creación y seguimiento de mensajes OSS.
- Coordinación de sesiones remotas con SAP Support.

2.5.3 Administración y mantenimiento de la base de datos

- Definición y supervisión de las políticas de backup y restore de la Base de Datos con carácter semanal.
- Supervisión de los estados de las diferentes BBDD de entornos SAP.
- Gestión y ajuste de espacio según crecimiento de la BBDD.
- Reorganización de tablas.
- Gestión del espacio en disco y de "tablespaces".
- Configuración de parámetros de ejecución: índices, "datafiles", tablas, cursores…
- Descarga y aplicación de parches y actualizaciones de base de datos.
- Informe de gestión y/o ejecución mensual de las mismas que tendrá que ser reportado al Cliente con un máximo de diez (10) días laborales desde que finaliza el mes.

3 Horario del servicio

El horario de servicio se establece para cada sistema del perímetro técnico la franja horaria de disponibilidad del servicio, dentro del cual tienen vigencia las responsabilidades y tareas incluidas en dicho nivel de servicio.

El horario de servicio de CONVISTA es de 09:00 horas a 18:00 horas, de lunes a viernes, ambos inclusive, de acuerdo con el calendario laboral de la Comunidad de Madrid y los festivos de Madrid capital.

4 Limitaciones del servicio

4.1 Servicios adicionales no incluidos

En caso de ser requeridos serán contemplados y facturados a parte:

- Cambios a Unicode.
- Instalación de nuevos sistemas.
- Subida de Enhanced Packages de SAP.
- Instalación o actualización de Sistema Operativo y SW de alta disponibilidad.
- Instalación y configuración de escenarios de SAP Solution Manager.
- Otros: Proyectos de archivado de datos, Formación.

4.2 Servicios excluidos

- Soporte funcional y soporte a entornos no incluidos en la presente propuesta.
- Definición y gestión de roles, perfiles u otros objetos de autorización de usuario.
- Servicios Basis motivados por evolutivos funcionales o por cambios de versión.
- Mantenimiento de hardware (servidores, almacenamiento, redes).
- Instalación de SW en las estaciones "Cliente" de los usuarios.
- Servicios de operación y copias de seguridad (cambio de cintas de back-up, etc.).
- No se incluyen licencias software ni hardware de aplicativos o dispositivos a utilizar.
- Operación del sistema operativo, aunque sí se trabajara de modo conjunto con el equipo del cliente en el caso de que sea necesario aplicar recomendaciones de SAP a este nivel.
- Incidencias de primer nivel (reportadas directamente por el usuario final).
- Ejecución de transportes.
- Manos remotas.
- Revisión / supervisión de las instalaciones propias del CPD del cliente (comunicaciones, almacenamiento, ...).

5 Organización del servicio

5.1 Modalidad de prestación del servicio

En función del bloque de cobertura del servicio, la modalidad de prestación será la siguiente:

- Monitorización de los entornos, generación remota y remisión electrónica mensual del informe de estado.
- Continuidad de los entornos productivos, control remoto constante de estado y envío de avisos electrónicos en caso de alerta.
- Después del envío del aviso electrónico, CONVISTA realizará un segundo aviso a través de ticketing al Cliente.
- Asesoramiento técnico en la evolución de los entornos, reunión con fecha a consensuar, pero con una periodicidad trimestral, con el Cliente.
- Respaldo técnico experto, el Cliente designará y comunicará a CONVISTA la persona o personas autorizadas para solicitar intervenciones. Una vez recibida la solicitud en el Centro de Operaciones de CONVISTA, a través de los canales habilitados (ticketing) al efecto, CONVISTA seguirá el siguiente procedimiento:
  - Análisis de la solicitud a través de la información suministrada.
  - Clasificación de prioridad de solicitud en base a la urgencia en la resolución, así como al impacto en el negocio, tal y como se describe en el punto siguiente.
  - Asignación del experto o expertos más adecuados para la resolución de la incidencia y planificación de la ejecución de los trabajos pertinentes.
  - Ejecución de las acciones requeridas para solventar la incidencia.

5.2 Canales de comunicación con el Centro de Operaciones

- **Herramienta de Ticketing de CONVISTA (JIRA):** Se facilitarán accesos y procedimientos al inicio del proyecto.
- **Teléfono:** Se facilita al inicio del servicio.
- **Correo electrónico:** Se facilita al inicio del servicio.

Para poder cumplir con las condiciones del servicio ofertadas en el Contrato es requisito indispensable que el Cliente utilice alguno de estos canales siempre que deseen realizar alguna solicitud de servicio, pues de otra manera CONVISTA no puede asegurar el cumplimiento de los tiempos de respuesta acordados.

6 Duración del servicio

6.1 Periodo de contratación del servicio

El presente Contrato entre CONVISTA y CNP ASSURANCES y CNP CAUTION tiene una duración de un (1) año, prorrogándose con carácter automático por igual periodo de plazo de un (1) año salvo que las Partes notifiquen con seis (6) meses de antelación su voluntad de no proceder a la prórroga del Contrato, bajo las condiciones estipuladas en el presente Contrato .

La fecha de inicio del presente Contrato se establece el 01 de octubre de 2022 o, en su defecto, cuando el Proyecto de Implantación de SAP que en la actualidad está realizando CONVISTA haya concluido.

6.2 Cancelación anticipada del Contrato

En el caso en que el Cliente decidiera cancelar el Contrato unilateralmente, deberá notificarlo por escrito a CONVISTA con una antelación suficiente, teniendo en cuenta las siguientes consideraciones:

- A partir de que el contrato despliegue sus efectos, el Cliente deberá notificar a CONVISTA su voluntad de terminar la presente relación con seis (6) meses de antelación.
- En cualquier caso, el Cliente abonará el 100% de los servicios que hasta el momento de la resolución efectiva se hubieran devengado a favor de CONVISTA por los servicios que efectivamente hubiera prestado .

En el caso en que CONVISTA decidiera cancelar el Contrato unilateralmente, deberá notificarlo por escrito al Cliente con una antelación de seis (6) meses y teniendo en cuenta las siguientes consideraciones:

- CONVISTA se hará cargo de todos los costes asociados a dicha cancelación.
- CONVISTA terminará los servicios que en el momento de la cancelación ya hubieran sido aprobados por las Partes.
- COVISTA entregará todos los materiales, sistemas, BBDD y/o cualquier soporte que pertenezca a El Cliente y que haya sido proporcionado a CONVISTA para la ejecución del presente Contrato teniendo en cuenta las instrucciones establecidas en el anexo 2 del mismo.
- CONVISTA facilitará al Cliente una extracción en formato CSV de las peticiones realizadas a través de ticketing que se hayan realizado durante la ejecución del presente Contrato.

7 Propuesta económica

7.1 Coste del servicio

Con relación al pago de los servicios contratados y regulados en el presente Contrato, el NOVENTA POR CIENTO (90%) del Precio será abonado por CNP CAUTION, mientras que CNP ASSURANCES abonará el DIEZ POR CIENTO (10%) del Precio restante. Ambas cantidades serán abonadas a CONVISTA en el plazo previsto y del modo establecido en el presente Contrato.

En el supuesto de que las condiciones económicas del Contrato, recogidas a continuación, sufrieran cambios, las Partes pactarán por escrito los mismos y se anexarán al presente Contrato como documento inseparable.

Concepto	Importe
Establecimiento del servicio[1]	0,00 €
Servicio Preventivo y Correctivo	2.500,00 €/mes

7.2 Jornadas a demanda

- En el caso de que el Cliente solicite a CONVISTA un servicio fuera del horario establecido en el presente Contrato, el Cliente deberá aprobarlo previamente y acordarlo conjuntamente con COVISTA a través de ticketing. Dicho servicio será abonado en en base al marco tarifario acordado en el apartado siguiente.

7.3 Tarifas para la ejecución de tareas adicionales

Con la contratación del soporte Basis, se define una tarifa especial para el Cliente en el desarrollo de correctivos y evolutivos, fuera del servicio remoto definido.

[1] Se establecen 4 jornadas de establecimiento y traspaso de servicio.

Acuerdo marco para horas adicionales a la bolsa contratada:

Tipo de Intervención	Remoto[2]	Presencial
Intervención en horario de cobertura	65 €/hora	90 €/hora
Intervención fuera de horario de cobertura	105 €/hora	135 €/hora

- Para la prestación de tareas en modo presencial la prestación mínima será de ocho (8) horas.

7.4 Facturación

- Los precios de la presente propuesta no incluyen I.V.A.
- CONVISTA facturará mensualmente los servicios prestados.
- El pago de las facturas se realizará en un plazo de treinta (30) días, contados desde la fecha de recepción de las facturas por parte de CNP ASSURANCES y CNP CAUTION.
- La forma de pago será mediante transferencia bancaria al número de cuenta de CONVISTA que figure en las facturas remitidas a CNP ASSURANCES y CNP CAUTION.
- CONVISTA enviará una factura a cada empresa, según lo establecido en la cláusula 7.1, y ambas facturas serán remitirás al siguiente correo electrónico: facturas@cnp.es

7.5 Gastos de desplazamiento

No habrá gastos de desplazamiento.

8 Requerimientos y condiciones del servicio

- CONVISTA realizará su trabajo atendiendo en todo momento a lo establecido en el presente Contrato.
- El Cliente proporcionará todo el soporte técnico y funcional posible y que sea realmente necesario al equipo de CONVISTA con su conocimiento de los procesos de negocio y del entorno técnico y funcional que se necesite para llevar a cabo los servicios establecidos en el presente Contrato.
- Los retrasos que pudiesen producirse por circunstancias no atribuibles a CONVISTA no serán asumidos por CONVISTA.

[2] Para jornadas presenciales, la facturación mínima será el equivalente a una jornada de ocho horas.

- Los retrasos que pudiesen producirse por culpa de las acciones u omisiones de CONVISTA o de cualquier de sus subcontratistas serán asumidos en todo caso por CONVISTA, siendo plenamente responsable de los daños y/o perjuicios que se pudieran irrogar al Cliente o a terceros.
- Para las tareas ejecutadas de manera remota, el Cliente habilitará el acceso a sus sistemas mediante las herramientas y procedimientos necesarios a CONVISTA. El acceso a los sistemas del Cliente se realizará cumpliendo con todas las obligaciones e instrucciones del anexo 2 y el apéndice 1 del presente Contrato.
- La prestación del servicio no incluye posibles licencias software ni hardware necesario de ninguno de los aplicativos o dispositivos a utilizar,
- CONVISTA no se responsabilizará de cualquier acción o mejora que el Cliente precise realizar en sus sistemas corporativos y que no haya sido contemplado en el Contrato (aplicaciones de parches, mejoras funcionales...). No obstante a lo anterior, CONVISTA podrá realizar la acción o mejora en cuestión previa solicitud expresa y por escrito del Cliente. En el supuesto de que CONVISTA actuara sin la debida aprobación del Cliente, CONVISTA será plenamente responsable de dicha acción o mejora y asumirá su coste.

9 Aplicación de sanciones financieras

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

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

10 Obligaciones laborales de CONVISTA

La naturaleza de este Contrato es la propia de un arrendamiento de servicios de carácter exclusivamente mercantil. Por lo expuesto, no se deriva relación o vínculo laboral alguno entre las Partes, ni entre el Cliente y el personal o colaboradores de CONVISTA que, eventualmente, pudieran estar prestando alguno de los servicios que constituyen el objeto del Contrato.

En ningún caso los empleados de CONVISTA se consideran personal del Cliente, no dependiendo ni funcional ni orgánicamente y no asumiendo el Cliente responsabilidad alguna en materia laboral respecto de los mismos.

En caso de baja de alguno de los empleados de CONVISTA, este se compromete a reemplazarlo en el plazo máximo de dos (2) días laborables.

CONVISTA se obliga a cumplir y hacer cumplir con todo rigor a su personal las obligaciones impuestas por la legislación laboral, especialmente en materia de Seguridad Social y Prevención de riesgos laborales, lo que justificará en cualquier momento a petición del Cliente y deberá disponer de una persona encargada de la vigilancia y cumplimiento de tales obligaciones.

CONVISTA deberá entregar al Cliente, si así se le solicita, y mantener actualizada la siguiente documentación:

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

El incumplimiento de cualquiera de las obligaciones especificadas facultará al Cliente para resolver el Contrato siempre que, habiéndose concedido un plazo razonable de un (1) mes para la aportación de la documentación citada, CONVISTA no la hubiera presentado.

Asimismo, para el supuesto de que por resolución judicial CNP ASSURANCES o CNP CAUTION fuera condenada a hacerse cargo de personal que hubiera pertenecido a la plantilla de CONVISTA, CONVISTA deberá pagar al Cliente una cantidad igual a la que el Cliente debiera pagar a ese personal en concepto de indemnización por despido improcedente.

11 Notificaciones

Las Partes señalan como domicilios para notificaciones relacionadas con el presente contrato, los siguientes:

1. **CNP ASSURANCES y CNP CAUTION** mediante notificación:

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

   Carrera de San Jerónimo, n.º 21

   28014 – Madrid

   peticiones@cnp.es

2. **CONVISTA** mediante notificación a:

   CONVISTA CONSULTING & ADVISORS S.L.U.

   Calle Santa Leonor, n.º 65, Edificio E, Planta 3

28037 - Madrid

Las notificaciones serán válidas cuando se realicen mediante alguno de los procedimientos siguientes:

- Comunicación escrita privada remitida por cualquier medio que permita dejar constancia de su recepción por la otra Parte.

Comunicación escrita privada presentada en el domicilio de la otra Parte y en la que conste sello y/o firma del destinatario como prueba de su recepción

12 Cláusula de prevención frente al fraude, soborno y corrupción

CNP ASSURANCES y CNP CAUTION tienen tolerancia cero en lo que se refiere a prácticas de soborno y corrupción, así como mantienen un estricto control para prevenir el fraude por lo que cuentan con políticas cuyo objetivo es prevenir estas prácticas en el seno de ambas entidades y en cualquier relación con terceros. Se adjunta como **Anexo 1** carta sobre los Principios Éticos que aplican a CNP ASSURANCES y CNP CAUTION y de los que CONVISTA debe ser conocedor y respetar en sus relaciones con CNP ASSURANCES y CNP CAUTION.

Con base a lo anterior, CONVISTA declara contar con políticas y procedimientos internos adecuados aplicables a sus empleados, así como a cualquier tercero que colaboren con ella, para prevenir y evitar la participación en actividades relacionadas con el fraude, la corrupción y el soborno y que serán de aplicación en el desarrollo del presente Contrato. Adicionalmente las Partes declaran que el Contrato se celebra única y exclusivamente para desarrollar objetivos de negocio, y que en ningún caso atiende a intereses particulares de cualesquiera de las Partes o al propósito de obtener una ventaja indebida para una de las Partes, uno de sus empleados o directivos.

En concreto, CONVISTA garantiza, en relación con el presente Contrato, que no existirán ventajas financieras o de cualquier otro tipo que hayan sido acordadas o que lo puedan ser en el futuro con cualquier persona perteneciente a CNP ASSURANCES y CNP CAUTION.

El incumplimiento de cualquiera de las previsiones anteriores será considerado como un incumplimiento grave del Contrato y dará derecho a CNP ASSURANCES y a CNP CAUTION a su terminación inmediata sin perjuicio de cualesquiera otras acciones legales que les puedan corresponder.

13 Independencia de las Partes

Este Contrato no convierte a ninguna de las Partes en representante legal de la otra, y no crea ningún tipo de asociación o empresa en común. Las Partes actúan como contratistas independientes y asumen plenamente y en nombre propio sus respectivas obligaciones, derivadas de este Contrato.

14 Cesión y subcontratación

Las Partes no podrán ceder el presente Contrato sin el previo consentimiento por escrito de la otra.

CONVISTA no podrá subcontratar a una tercera parte para la prestación de los servicios establecidos en el Contrato salvo que medie previo consentimiento y por escrito del Cliente.

En el caso de que CONVISTA recurra a subcontratistas para llevar a cabo los servicios descritos en el presente Contrato deberá obtener autorización previa y por escrito del Cliente. A tal efecto, CONVISTA informará por escrito al Cliente con carácter previo de las subcontrataciones previstas, facilitando los datos de los terceros a los que pretenda subcontratar. Si el Cliente no manifestara por escrito su oposición a dicha subcontratación en el plazo de cinco (5) hábiles desde la recepción de la notificación correspondiente, se entenderá que no se oponen a la misma. Los mismos términos y obligaciones resultarán aplicables en el supuesto de que CONVISTA tuviera intención de sustituir a alguno o algunos de sus subcontratistas.

15 Términos y condiciones

15.1 Confidencialidad

El uso que CONVISTA realice de los datos de CNP ASSURANCES y CNP CAUTION tendrá, en cualquier caso, carácter confidencial y se adecuará a los fines estipulados en el Contrato.

Todo el personal de CONVISTA que pueda tener acceso a información confidencial propiedad de CNP ASSURANCES y CNP CAUTION está sujeto al más estricto secreto profesional. A estos efectos se entenderá por personal (filiales, directivos, empleados, subcontratados o persona interpuesta).

CONVISTA y su personal estará obligada a guardar absoluta confidencialidad por si misma o a través de terceros sobre cualquier información del Cliente que sea considerada como secreto comercial o empresarial y a la que CONVISTA tenga acceso como consecuencia del cumplimiento de sus obligaciones bajo el contrato. La revelación y cesión de dicha información confidencial a terceros no relacionados con el cumplimiento del Contrato sólo podrá llevarse a cabo con el previo consentimiento por escrito de CNP ASSURANCES y de CNP CAUTION. La información confidencial tampoco podrá entregarse a las autoridades salvo que medie un mandato solicitando la información.

El Cliente estará obligados a guardar absoluta confidencialidad sobre cualquier know-how comercial, técnico o científico de CONVISTA que les sea revelado durante el periodo de vigencia del contrato correspondiente y a no revelar dicha información confidencial a ningún tercero, salvo previa autorización por escrito de CONVISTA o cuando haya solicitado formalmente por una autoridad administrativa.

15.2 Protección de datos

El REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la normativa nacional sobre protección de datos

aplicable (incluyendo las disposiciones específicas sobre protección de datos incluida en la normativa del sector seguros de aplicación en cada momento) y/o cualquier otra legislación que las modifique o sustituya en un futuro, será de obligado cumplimiento para cada una de las partes.

CONVISTA no tendrá acceso a ningún dato de CNP ASSURANCES y de CNP CAUTION.

15.3 Datos personales de los firmantes

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

¿Quién es el Responsable del Tratamiento de sus Datos Personales?	Por parte de CONVISTA: **ConVista Consulting** Dirección postal: C/Josep Pla 2, Edificio B3 – Planta 4, E-08019 Barcelona Delegado de Protección de Datos: Oscar.Barrios@convista.com Por parte de **CNP ASSURANCES y CNP CAUTION**: CNP ASSURANCES SUCURSAL EN ESPAÑA Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpspain.eu CNP CAUTION SUCURSAL EN ESPAÑA: Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpspain.eu
¿Con qué finalidad se tratan sus Datos personales?	La finalidad del Tratamiento de los firmantes y las personas de contacto es gestionar de forma adecuada la relación contractual objeto de este Contrato. Las Partes tratarán estos datos para satisfacer el interés legítimo que tienen ambas compañías de mantener el contacto entre ellas durante la prestación de los servicios. Los Datos Personales serán conservados mientras sean necesarios para cumplir con las obligaciones contractuales y legales asumidas.
¿Cuál es la legitimación para el Tratamiento de sus Datos Personales?	La base de legitimación deriva del interés legítimo de cada una de las Partes de mantener relaciones de cualquier índole con la otra para cumplir con las condiciones del Contrato.
¿Cuáles son sus derechos cuando facilita sus Datos Personales?	Los sujetos interesados tienen derecho a obtener confirmación sobre si las Partes están tratando Datos Personales que les conciernan, o no. En particular, tienen derecho a: Acceder a sus Datos Personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. En determinadas circunstancias, pueden solicitar la limitación del Tratamiento de sus Datos Personales, en cuyo caso

	únicamente serán conservados para el ejercicio o la defensa de reclamaciones. Asimismo, también tiene derecho a oponerse al Tratamiento de sus Datos Personales. En tal caso, el Responsable del Tratamiento dejará de tratar los Datos Personales, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones. Los representantes de las Partes pueden ejercer los referidos derechos dirigiendo un correo electrónico a cada una de las direcciones electrónicas designadas en la primera fila de esta tabla. Puede obtener información adicional acerca de sus derechos ante la Agencia Española de Protección de Datos en www.agpd.es Cuando el representante no haya obtenido satisfacción en el ejercicio de sus derechos, puede presentar una reclamación ante la Agencia Española de Protección de Datos en www.agpd.es .

15.4 Obligaciones del Cliente

En el marco de sus actividades empresariales, el Cliente estará obligado a prestar la asistencia y el soporte razonables que precise CONVISTA para el efectivo cumplimiento de las obligaciones pactadas en el presente Contrato, así como crear las condiciones necesarias para el adecuado cumplimiento de las obligaciones contractuales de CONVISTA y a facilitar puntualmente a CONVISTA toda la documentación y demás información que le sea requerida y que sea absolutamente necesaria en cada momento y que el Cliente disponga en dicho momento. En el supuesto de que no dispusiera de la información solicitada, el Cliente dispondrá de un plazo razonable de tiempo para la entrega de la misma.

15.5 Obligaciones de CONVISTA

Además de las obligaciones establecidas con relación a CONVISTA en el presente Contrato, CONVISTA deberá solicitar la información necesaria al Cliente para la prestación de los servicios contratados, así como a solicitar el soporte técnico y funcional necesario para el desarrollo de los servicios contratados. Si CONVISTA, siendo necesario, no lo solicitara, los daños y perjuicios que se ocasionaren serían de su exclusiva responsabilidad.

15.6 Información propiedad de CONVISTA

Se entiende por información propiedad de CONVISTA todos aquellos elementos desarrollados por CONVISTA con carácter previo a este Proyecto. A modo de ejemplo, todo código propiedad de CONVISTA (librerías, frameworks...) desarrollado previamente a modo de componente reutilizable, que sea utilizado en el ámbito de este Proyecto para acelerar su ejecución, seguirá siendo propiedad de CONVISTA, permitiéndose sin coste alguno su utilización indefinida única y exclusivamente dentro del ámbito del proyecto ofertado en esta propuesta, no pudiendo ser reutilizado por el Cliente o terceros ni cedido a terceros por parte del Cliente sin autorización expresa y por escrito de CONVISTA. En caso de utilizar estos elementos, CONVISTA informará

por escrito al Cliente sobre la existencia de este tipo de información de su propiedad durante la ejecución del Proyecto.

15.7 Propiedad del sistema y de la solución

El Cliente será titular en exclusiva de todos los derechos de explotación derivados de la Propiedad Intelectual del programa de ordenador o parte del programa que resulte de desarrollos específicos que puedan ser objeto de la prestación de los servicios contratados, a cuyo efecto CONVISTA cede a favor del Cliente su uso, no pudiendo reutilizarse por parte de CONVISTA en otros clientes salvo consentimiento previo, expreso y por escrito del Cliente.

CONVISTA garantiza que los trabajos y servicios prestados al Cliente en la ejecución de este Contrato no infringen derechos de Propiedad Intelectual o Industrial o cualesquiera otros derechos de terceros, haciéndose CONVISTA, en todo caso, plena e individualmente responsable de toda clase de reclamaciones y/o indemnizaciones por razón de este concepto frente a todo tipo de terceros.

15.8 Causas de terminación anormal

El presente contrato podrá ser extinguido de forma unilateral por CONVISTA, con independencia de cualquier otra causa de resolución indicada en este Contrato y/o en la Ley, en los supuestos siguientes:

1. Si el Cliente no hubiera abonado facturas emitidas y vencidas, una vez apercibidos de impago por escrito con acuse de recibo o de cualquier otro modo que dejara constancia del recibimiento del apercibimiento y no habiendo subsanado esta contingencia en el plazo improrrogable de treinta (30) días naturales, CONVISTA queda liberado de seguir prestando cualquier tipo de servicios pudiendo, a partir de ese momento, cancelar la prestación de los servicios con el Cliente, incluso cesar la prestación del control remoto, como el mantenimiento en uso de los servidores contratados con CONVISTA, quedando a su vez liberado el Cliente de cualquier obligación, salvo el abono de las cantidades debidas a CONVISTA por servicios ya prestados.
2. La no realización o la realización defectuosa de los servicios estipulados en el presente Contrato por parte de CONVISTA dará derecho al Cliente a resolver el Contrato, pudiendo en su caso solicitar a CONVISTA la pertinente indemnización por los daños y/o perjuicios ocasionados al Cliente por razón de su acción u omisión.
3. Si cualquiera de las Partes fuera declarada en concurso a instancia de acreedor legítimo, o si presentara solicitud de concurso voluntaria o suspensión de pagos, o si se hubieran instado en su contra juicios ejecutivos o decretados embargos preventivos u otras medidas cautelares que pongan de manifiesto la disminución de la solvencia económica o dificultades financieras para atender al normal cumplimiento de sus obligaciones.
4. Cualquier incumplimiento relativo a la Información Confidencial.

16 Nulidad o anulabilidad

Cualquier modificación de los presentes Términos y Condiciones Generales o de los Anexos, sólo será válida si se efectúa mediante instrumento escrito firmado por ambas Partes.

Si cualquiera de las estipulaciones del presente Contrato resultase nula o inválida, la nulidad o invalidez de las mismas no afectará a las demás estipulaciones, las cuales se mantendrán en vigor y seguirán surtiendo plenos efectos.

La renuncia por cualquier de las Partes a exigir en un momento determinado el cumplimiento de uno cualquiera de las estipulaciones aquí estipuladas no implicará una renuncia con carácter general ni creará un derecho adquirido por la otra Parte.

17 Legislación aplicable

El presente Contrato se halla sujeto a las disposiciones de la Ley española.

18 Jurisdicción aplicable

En caso de que surgiera entre las Partes cualquier discrepancia o conflicto derivado de la interpretación o cumplimiento del presente Contrato las Partes, con renuncia a su propio fuero o aquel que pudiera corresponderles, se someten expresamente al fuero de los Juzgados y Tribunales de Madrid capital.

19 Contrato completo

El presente Contrato constituye la totalidad del convenio regulador de la relación contractual que se establece entre las Partes en las materias objeto del presente Contrato con efectos a la fecha de la firma y, en consecuencia, quedan anulados y sustituidos cuantos acuerdos, convenios y contratos pudieran haberse concluido entre las mismas partes sobre el mismo objeto con anterioridad a este acto.

20 Firma del contrato

Y, a tal efecto, las partes firman el presente contrato por duplicado en Madrid, a 13 de junio de 2022.

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España	**POR CONVISTA CONSULTING & ADVISORS S.L.U.**
Fdo.: David Lattes	**Fdo.:** Norbert Nielsen

ANEXO 1

AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

(Principios Éticos Grupo CNP)

ENTRE

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

Y

CONVISTA CONSULTING & ADVISORS S.L.U.

ANEXO 1 AL
CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

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

Insuring
a more
open world

ÉTICA DE NEGOCIOS.
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

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

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

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

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

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

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

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

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

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

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

Y en prueba de recepción el suscribiente en el carácter con el que interviene, firma el presente anexo en Madrid a 13 de junio de 2022.

Por duplicado a un solo efecto.

POR CONVISTA CONSULTING & ADVISORS S.L.U.

Fdo.: Norbert Nielsen

31

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SOPORTE BASIS

ENTRE

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

E

CONVISTA CONSULTING & ADVISORS S.L.U.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS SORPORTE BASIS

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

Introducción

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

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

    - los Datos del CLIENTE; incluida la Información Confidencial del CLIENTE.
    - toda información relativa a EL CLIENTE.
    - cualquier otra información utilizada en la prestación de los Servicios;
    - los sistemas informáticos del CLIENTE y del PROVEEDOR (incluidos los Sistemas del PROVEEDOR) que procesen, almacenen o transmitan información; y
    - el código informático utilizado para procesar Datos del CLIENTE incluida la Información Confidencial del CLIENTE.

Funciones y Responsabilidades

Cumplimiento

- Se establecerán reuniones de seguimiento para comprobar el cumplimiento de sus obligaciones establecidas en el presente contrato de forma mensual.
- Sin perjuicio de las demás acciones y vías de reparación a las que pueda recurrir al CLIENTE, todo incumplimiento comunicado por EL PROVEEDOR al CLIENTE de acuerdo con lo dispuesto en el apartado Cumplimiento, dará lugar a una valoración del riesgo por parte del CLIENTE que indicará al PROVEEDOR en el plazo de tiempo del que dispondrá para poner en práctica las medidas correctoras que resulten necesarias.
- EL PROVEEDOR se compromete a colaborar en las auditorías realizadas por el CLIENTE, y entregará al CLIENTE las evidencias, informes y certificados necesarios para asegurar que cumple con los términos del presente Contrato en un periodo razonable.

Valoración del riesgo

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

Personal del PROVEEDOR

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

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

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

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

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

Educación, Formación y Sensibilización

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

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

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

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

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

- otras cuestiones relacionadas con la Seguridad Informática;

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

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

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

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

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

Responsable de Seguridad del PROVEEDOR

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

El Responsable de Seguridad del PROVEEDOR deberá:

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

Incidentes de Seguridad

Notificación de los Incidentes de Seguridad

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

notificación dentro de las veinticuatro (24) horas naturales siguientes al momento en que EL PROVEEDOR hubiese tenido conocimiento de dicho Incidente de Seguridad.

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

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

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

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

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

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

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

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

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

Si, en opinión del CLIENTE, un subcontratista o cualquier Tercero Proveedor fuese considerado no apto tras la correspondiente revisión de la seguridad, EL CLIENTE podrá exigir al PROVEEDOR (en el plazo de tiempo que EL CLIENTE considere apropiado) que deje de recurrir a dicho Subcontratista o a ese Tercero, y que encuentre un sustituto que EL CLIENTE considere aceptable. Alternativamente, y únicamente a instancias del CLIENTE, EL CLIENTE podrá aceptar un compromiso del Subcontratista por el que se obligue a acordar con EL PROVEEDOR un plan correctivo legalmente vinculante, en el que deberán indicarse las acciones y los plazos necesarios para subsanar las deficiencias puestas de manifiesto a través de la revisión, y cuya finalización exitosa deberá ser aprobada por EL CLIENTE.

Derecho de inspección del CLIENTE

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

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

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

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

Valoración de la Seguridad

EL CLIENTE podría contratar, a su costa, a un Tercero Evaluador de la Seguridad que realizará al menos una Valoración de la Seguridad con el fin de evaluar el nivel de cumplimiento del presente contrato bajo demanda durante el período de vigencia de este.

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

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

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

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

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

Gobierno de la seguridad de la información

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

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

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

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

Política de Seguridad de la Información

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

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

Gestión de Activos

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

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

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

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

Control de Acceso

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

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

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

Acceso Privilegiado
EL PROVEEDOR se asegurará de que:

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

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

- los mecanismos de autenticación deben garantizar que no puedan ser eludidos para obtener un acceso no autorizado a los sistemas;
- los datos de autenticación, incluidas las contraseñas, no deben almacenarse de una forma que permita que los mismos puedan ser recuperados en un formato legible o descifrable; y
- las contraseñas deben ser complejas e incluir una combinación de distintos tipos de caracteres y tener una longitud suficiente para evitar ataques exhaustivos o de diccionario.
- Relativo a las contraseñas para dar servicio al CLIENTE, se podrá pactar la política de contraseñas junto con EL CLIENTE.

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

Configuración del Sistema

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

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

Monitorización de los sistemas

Registro de Sucesos
EL PROVEEDOR mantendrá registros de todos los sucesos clave, y en especial de los que sean susceptibles de afectar a la confidencialidad, la integridad y la disponibilidad de los Servicios

prestados al CLIENTE que servirán para facilitar la identificación y la investigación de los Incidentes y/o incumplimientos significativos de los derechos de acceso que se produzcan en relación con los Sistemas del PROVEEDOR.

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

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

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

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

Seguridad de la Red

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

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

Los sistemas de CLIENTE gestionados por el PROVEEDOR estarán respaldados por diagramas precisos y actualizados que incluirán todos los componentes del sistema y las interfaces con otros sistemas. Estos diagramas se pondrán a disposición del CLIENTE bajo petición en un tiempo razonable tras la solicitud.

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

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

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

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

Las reglas se revisarán cada SEIS (6) meses y se mostrará el resultado en la revisión periódica del servicio junto al CLIENTE.

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

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

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

Criptografía

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

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

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

Protección Contra Código Malicioso

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

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

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

Gestión de los cambios y parches

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

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

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

Los parches de seguridad y demás actualizaciones relativas a la vulnerabilidad de la seguridad sólo se aplicarán si están disponibles y han sido previamente aprobados, a menos que su utilización suponga un riesgo mayor para el negocio. Se instalarán medidas de seguridad adicional en los Sistemas del PROVEEDOR que, por cualquier motivo, no puedan actualizarse, para que el sistema vulnerable quede totalmente protegido. Todos los cambios deben realizarse de acuerdo con el proceso de gestión de cambios aprobado.

EL PROVEEDOR dispondrá de un proceso documentado para identificar y subsanar mensualmente las vulnerabilidades de seguridad que presente el *software SAP* entregado a EL CLIENTE y facilitará al CLIENTE las actualizaciones correspondientes en cuanto estén disponibles. Así como, las soluciones temporales que sirvan para mitigar el riesgo en caso de no existir un parche oficial disponible.

Los parches de seguridad de sistema operativo que se aplicarán de manera semestral. Aquellos parches cuyo impacto sea muy alto se documentarán y se podrían no instalar en mutuo acuerdo entre EL CLIENTE y EL PROVEEDOR.

Gestión de Terceros

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

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

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

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

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

Fdo.: David Lattes

POR CONVISTA CONSULTING & ADVISORS S.L.U.

Fdo.: Norbert Nielsen

ANEXO 3

AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

ENTRE

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

Y

CONVISTA CONSULTING & ADVISORS S.L.U.

ANEXO 3 AL CONTRATO DE PRESTACIÓN DE SERVICIOS BASIS

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

1. Acuerdos de Nivel de Servicio

Los criterios de priorización que se seguirán, así como los diferentes Acuerdos de Nivel de servicio por servicio y prioridad atendiendo a los siguientes indicadores:

Indicador	Descripción	Medida
Tiempo de entrega de Mantenimiento Preventivo	Las soluciones, según su clasificación simple o compleja, deben entregarse en la fecha planificada.	Días de desviación respecto a la fecha prevista.
Tiempo promedio para el inicio de atención de incidencias	Tiempo promedio que se tarda en iniciar la resolución de una solicitud de servicio.	Tiempo desde la recepción de la petición hasta el inicio de su resolución)/(Nº total de solicitudes recibidas)
Porcentaje de Resolución incidencias	Cantidad total de incidencias resueltas en un tiempo menor al valor objetivo establecido.	(Nº incidencias resultas en -X horas)/(Nº incidencias resueltas en el periodo contractual)
Elaboración y Entrega de los Informes sobre el estado de los elementos relevantes, así como el informe de monitorización de los sistemas SAP.	Mide que los informes críticos se manden en los plazos establecidos	(Nº informes rechazados en el periodo)/(Nº informes entregados en el periodo)

2. Incumplimiento de los Acuerdos de Nivel de Servicio

En caso de incumplimiento de los niveles de servicios se aplicará la penalización correspondiente, computando cada SLA incumplido con 1 punto.

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:

- Si la suma de puntos de penalización igual a 1 → No se aplicará penalización alguna
- Si la suma de puntos de penalización está entre 2 y 3 → Se aplicará un 5% de penalización sobre el importe de la facturación mensual.
- Si la suma de puntos de penalización es superior a 4 → Se aplicará un 10% de penalización sobre el importe de la facturación mensual.

Si alguno de los indicadores marcados con 2 puntos de penalización se incumpliera durante dos (2) meses seguidos se deberá presentar en el siguiente Comité de Streering Commite donde el Cliente decidirá si se aplica un 5% de penalización sobre la facturación por cada indicador incumplido.

Y en prueba de recepción el suscribiente en el carácter con el que interviene, firma el presente anexo en Madrid a 13 de junio de 2022.

Por duplicado a un solo efecto.

POR CNP ASSURANCES, S.A., Sucursal en España Y CNP CAUTION, Sucursal en España	**POR CONVISTA CONSULTING & ADVISORS S.L.U.**
Fdo.: David Lattes	**Fdo.:** Norbert Nielsen