

AJ250 / CNP caution / Convista / 01.01



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 <input type="checkbox"/>	Presupuesto/ Proyecto <input type="checkbox"/>	Doc. Consejo <input type="checkbox"/>	Doc. Hacienda <input type="checkbox"/>	Doc. DGSFP <input type="checkbox"/>	Doc. Planes/EPSP <input type="checkbox"/>	Otro:
Solicitado por: (Director del CODIR)	THIERRY VASQUEZ						
Contenido / Objetivo: Principal Acuerdo, entregables y descripción del servicio	Contrato de servicio proyecto Convista						

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

Denominación del Documento:	Contrato de servicio proyecto Convista		
Apoderado/s de CNP: <i>(según importe económico del contrato)⁽¹⁾</i>	DAVID LATTES		
Contraparte: <i>(proveedor, o interviniente)</i>	CONVISTA		
Fecha de inicio del contrato:	MAI 2022		
Fecha de vencimiento del contrato:			
Renovación Tácita:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	
Preaviso Cancelación:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	Especificar preaviso:
Penalización por cancelación:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	Importe:
Actualización precio por IPC, etc.:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	
Delegación actividades críticas:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	Especificar:
KPI / SLA:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	
Presupuestado:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	
Código CECO:			
Código PEP:			
Activable:	<input type="checkbox"/> SI	<input type="checkbox"/> NO	
Periodicidad del pago:	Mensual <input type="checkbox"/>	Trimestral <input type="checkbox"/>	Anual <input type="checkbox"/> Pago único <input type="checkbox"/>

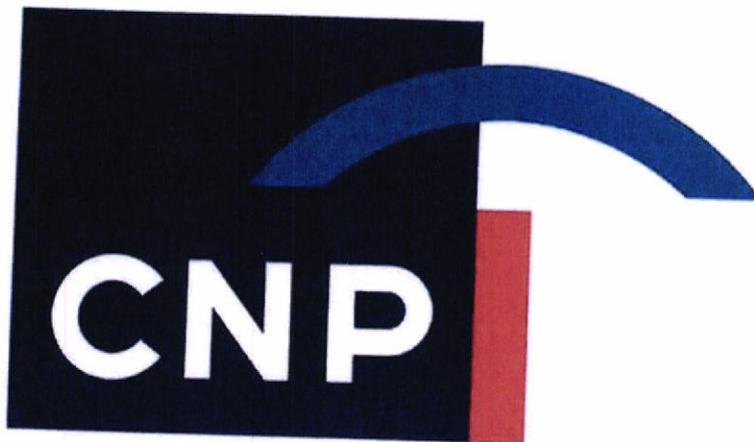
- OBLIGATORIO -

Responsable del Departamento y Director del CODIR correspondiente: Oscar Rodriguez <i>Fabrica ASW</i>	Fecha: 22.08	Firma:	Firma:
Verificación de Control Financiero: <i>En el caso de que el gasto sea activable.</i>	Fecha:	Firma:	
Verificación de Control de Gestión: <i>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.</i>	Fecha:	Firma:	
Revisión Asesoría Jurídica: <i>(persona del equipo legal que ha revisado el contrato y verificado que cumple con todos los requerimientos solicitados) N ereida CANO</i>	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.

Contrato de Servicios

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
3 Horario del servicio	5
4 Delimitación del alcance	6
5 Organización del servicio	6
5.1 Planificación	6
5.2 Entregables	7
6 Duración del servicio	7
6.1 Período de contratación del servicio.....	7
6.2 Renovación del servicio.....	7
6.3 Cancelación anticipada del contrato	7
7 Propuesta económica	8
7.1 Coste del servicio	8
7.2 Facturación	8
7.3 Gastos de desplazamiento	9
8 Garantía.....	9
9 Requerimientos y condiciones del servicio.....	9
10 Aplicación de sanciones financieras	10
11 Obligaciones laborales de CONVISTA	10
12 Notificaciones	11
13 Cláusula de prevención frente al fraude, soborno y corrupción.....	12
14 Independencia de las Partes.....	12
15 Cesión y subcontratación	13
16 Términos y condiciones.....	13
16.1 Confidencialidad	13
16.2 Protección de datos.....	14
16.3 Datos personales de los firmantes.....	14
16.4 Obligaciones del Cliente	15
16.5 Obligaciones de CONVISTA.....	15
16.6 Información propiedad de CONVISTA.....	16

DC

16.7 Propiedad del sistema y de la solución.....	16
16.8 Causas de terminación anormal.....	16
17 Nulidad o anulabilidad.....	17
18 Legislación aplicable.....	17
19 Jurisdicción aplicable.....	17
20 Contrato completo.....	17
21 Firma del Contrato.....	18

1 INTRODUCCIÓN

1.1 Marco previo

CNP CAUTION, SUCURSAL EN ESPAÑA y CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA desean formalizar la petición de servicios realizada a CONVISTA para cubrir los servicios que se describen a continuación necesarios para el desarrollo del proyecto denominado "Proyecto de Implantación sucursales francesas en SAP" (en adelante, el "Proyecto") que están llevando a cabo.

CONVISTA es una empresa especializada, entre otros, en la prestación de servicios de consultoría de management y software en general y consultoría informática cuya actividad cubre las necesidades de CNP CAUTION, SUCURSAL EN ESPAÑA y CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA para la realización del Proyecto.

REUNIDOS

DE UNA PARTE, D. DAVID LATTES, mayor de edad, de nacionalidad francesa, con domicilio a estos efectos en Carrera de San Jerónimo, nº 21, 28014, Madrid y con NIE Y-6119145-D, en su condición de representante legal de **CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA**, en virtud de Escritura de poderes otorgada el 12 de julio de 2018 ante el Notario de Madrid D. Juan Aznar de la Haza con el n.º 2563 de orden de su protocolo e inscrita en el Registro Mercantil de Madrid al Tomo 30.634, Folio 137 Hoja M-73979 (en adelante, "**CNP ASSURANCES**") (W0013620J) y de **CNP CAUTION, SUCURSAL EN ESPAÑA**, en virtud de Escritura de poderes otorgada el 19 de febrero de 2021 ante el Notario de Madrid D. Juan Aznar de la Haza con el n.º 728 de orden de su protocolo e inscrita en el Registro Mercantil de Madrid al Tomo 33803, Folio 166, Hoja M-608403 (en adelante, "**CNP CAUTION**") (W0010754J).

Ambas denominadas conjuntamente 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

CNP ASSURANCES y CNP CAUTION solicitan a CONVISTA la prestación de sus servicios de consultoría SAP en el ámbito financiero y tecnológico.

El objetivo del Proyecto es la puesta en marcha de un nuevo sistema tecnológico SAP S/4HANA, con entornos de Desarrollo, Implantación y Producción y la puesta en marcha de un entorno SAP Router y un entorno SAP Solution Manager.

2 Descripción del servicio

El servicio que CONVISTA se compromete a prestar contiene las siguientes tareas:

- Instalación de entornos de Desarrollo, Integración y Producción.
- Instalación del SAP Router.
- Instalación del SAP Solution Manager.
- Inicialización del sistema SAP S/4HANA.
- Inicialización del entorno Fiori.
- Implantación de los módulos de SAP FI, SAP AF, SAP CO para las sociedades 802 y 803 y planes de cuentas P801 – CNP IAM S.A. Sucursal, P802 – CNP ASSURANCES S.A. Sucursal, PSUC – Plan Sucursales Francia.
- Implantación de CONVISTA ELECTRONIC BANK STATEMENT.
- Norma 34 Transferencias bancarias ISO20022 – SEPA CT.
- Norma 43 Para la recepción y carga del extracto bancario.
- Informe de sumas y saldos.
- Transacciones y programas a medida a implantar (como copia de lo actualmente implantado en la máquina actual de SAP ECC).
- ZCNP_DISTRIBUIR_GAST – Reclasificación Gastos Destino.
- ZCNP_ADD_PORC_RECLAS – Tratar Fichero Gastos Destino.
- ZCARTERA – Mantenimiento de ZCARTERA.
- ZFI_EXCEL_FB01 – Carga asientos FI.
- Programa: ZCNP_FI_CARGA_EXCEL_MULTI.
- CONVISTA implementará la configuración de los roles y autorizaciones de usuario necesarios según la definición realizada.
- Se realizará la puesta en marcha de un entorno Fiori, pero no se realizarán la implantación de Fiori apps que no vengán con el estándar de inicio.

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 Delimitación del alcance

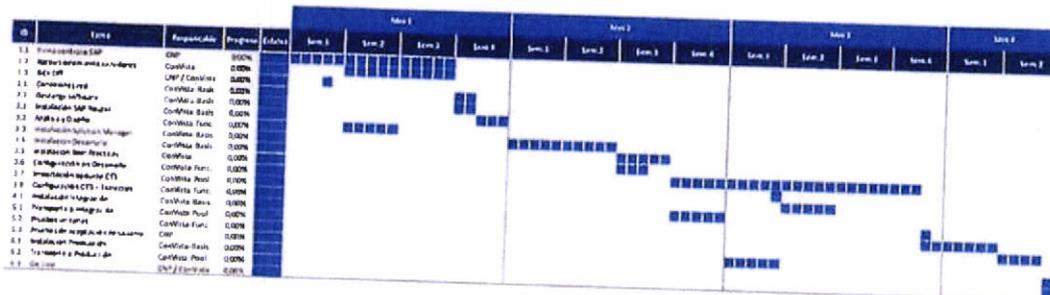
El servicio prestado por CONVISTA no incluirá los siguientes servicios:

- Mantenimiento de hardware (servidores, almacenamiento, redes).
- 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.
- Revisión / supervisión de las instalaciones propias del CPD del cliente (comunicaciones, almacenamiento, ...).
- Dentro de esta propuesta no se encuentran valorado el desarrollo de informes propios del negocio de CNP ASSURANCES y CNP CAUTION que no hayan quedado descritos en la misma. Cualquier otro informe propio del negocio de CNP ASSURANCES y CNP CAUTION que sea adicionalmente necesario deberá ser primero analizado para ver su posible encaje en el estándar de SAP. Todos aquellos informes que no se adapten al estándar de SAP y se soliciten serán valorados por adicionalmente para su implantación.
- No se realizarán adaptaciones al estándar. Cualquier necesidad adicional será estimada adicionalmente.
- No se realizará migración de saldos de cuentas. La inicialización de los saldos de cuentas se realizará mediante un apunte de apertura de cuenta contra una cuenta no relevante.
- No se contemplan actividades relacionadas con los módulos de SAP FAM, SAP BCM, SAP CM ni ningún otro no descrito en la presente oferta.
- No se llevarán a cabo ningún tipo de integración con otros sistemas SAP y no SAP.
- CONVISTA no realizará tareas dentro de los entornos de SAP ECC o cualquier otro que no haya sido descrito en la presente oferta. Si fuera de necesidad que CONVISTA los realizase de estimará adicionalmente.
- CONVISTA realizará la inicialización financiera necesaria en el nuevo sistema SAP S/4HANA para la puesta en marcha de las sociedades descritas en la presente oferta, no realizando ningún tipo de integración contable técnica y o funcional.

5 Organización del servicio

5.1 Planificación

El plan de Proyecto será el siguiente:



5.2 Entregables

A continuación, se presenta el listado de los entregables previstos durante la ejecución del Proyecto, los cuales serán realizados en castellano.

Entregable	Detalle
Documentación de gestión del Proyecto (informes de seguimiento)	Estos informes tienen como objetivo que los Comités de Gobierno del Proyecto puedan tener conocimiento del estado real del Proyecto y permiten la toma de decisiones que pueda afectar a los objetivos del mismo.
Guías de parametrización	Guías de Parametrización de toda la configuración realizada.
Mapa de sistemas y de integraciones objetivo	Documento con el detalle del mapa de soluciones y sistemas
Plan de pruebas	Plan de pruebas detallado

6 Duración del servicio

6.1 Período de contratación del servicio

El presente Contrato entre CNP ASSURANCES y CNP CAUTION y CONVISTA entrará en vigor el día 13 de junio de 2022 (fecha de inicio del Proyecto) y será válido hasta poner en marcha las dos sociedades en el sistema productivo (previsto para el día 30 de septiembre de 2022).

No obstante lo anterior, si por causas no imputables al Cliente, el proyecto no pudiera finalizarse a la fecha prevista (30 de septiembre de 2022) CONVISTA tendrá el plazo de un (1) mes de gracia para finalizar dicho proyecto. Consecuentemente, si a fecha 30 de octubre de 2022, CONVISTA no entregase el proyecto al Cliente, se establece como penalización un importe equivalente al 50% del importe que a dicha fecha quedase pendiente de facturar al Cliente.

6.2 Renovación del servicio

No está prevista una renovación del Contrato, al tratarse de un Proyecto.

6.3 Cancelación anticipada del contrato

En el caso en que el Cliente decidiera cancelar el Contrato de forma unilateral, deberán notificarlo por escrito a CONVISTA con un plazo de antelación suficiente, entendiéndose como tal, al menos, UN (1) mes.

En el supuesto de que CONVISTA incumpliera cualquiera de las obligaciones asumidas en el presente Contrato, el CLIENTE podrá denunciar el Contrato en cualquier momento sin necesidad de preaviso, pudiendo poner fin al mismo de manera inmediata sin que CONVISTA tenga derecho a reclamar indemnización alguna y reservándose su derecho a reclamar aquellos conceptos o daños y perjuicios a los que el Cliente tenga derecho.

En cualquier caso, CNP ASSURANCES SA. SUC abonará el 100% del importe de los servicios que hasta el momento de la resolución efectiva hubieran sido efectivamente realizados.

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 a continuación:

Por grupos de funcionalidades propuestas por CONVISTA	
Gestión del Proyecto	8.400,00 €
Tareas Funcionales / Técnicas	27.000,00 €
Tareas Basis	20.500,00 €
Migración del histórico	5.500,00 €
Tareas de Seguridad	5.000,00 €
Total servicios para la implantación en SAP S/4HANA	66.400,00 €
Descuento de un 5 % sobre los servicios de CONVISTA	-3.162,00 €
Licencia CONVISTA ELECTRONIC BANK STATEMENT	10.000,00 €
Descuento de un 50 % sobre la licencia CTS	-5.000,00 €
TOTAL DE LA PRESENTE OFERTA	68.238,00 €

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.

7.2 Facturación

- Los precios de la presente propuesta no incluyen el Impuesto sobre el Valor Añadido.
- El pago de las facturas se realizará a 30 días desde la fecha de recepción de las facturas en el email indicado a continuación.

- La forma de pago a través de la cual CNP ASSURANCES y CNP CAUTION abonarán el Precio será mediante transferencia bancaria al número de cuenta que conste en las facturas emitidas por CONVISTA para cada una de las entidades..
- Todas las facturas deberán abonarse en el plazo acordado.

El proveedor percibirá los honorarios conforme a los siguientes pagos parciales:

1. 25% del Precio en el momento de la firma del presente Contrato.
2. 25% del Precio en el momento de terminar la instalación de la máquina de SAP Desarrollo
3. 25% del Precio restante en el momento de PRUEBA DE (5.3) terminación del proyecto y su validación por parte del Cliente.
4. 25% restante en el momento de validación de la puesta en producción (Go Live).

El PROVEEDOR girará las pertinentes facturas, una para cada empresa, y las remitirá al email: facturas@cnp.es

7.3 Gastos de desplazamiento

No habrá gastos de desplazamiento.

8 Garantía

El período de garantía del Proyecto comenzará a partir de su aceptación y se extenderá por un periodo de 6 meses a contar desde la terminación del mismo (Go live) sobre errores detectados imputables a los servicios de CONVISTA (no incluyéndose en los mismos cambios o ampliaciones de alcance) o hasta el momento en que se hayan subsanado los mencionados errores, el sistema se encuentre funcionando en perfectas condiciones y haya sido validado por el CLIENTE.

Asimismo, esta garantía solo tendrá valor mientras no se produzcan modificaciones en la solución de gestión de tesorería no controladas por CONVISTA.

9 Requerimientos y condiciones del servicio

- CONVISTA se ceñirá a los requerimientos realizados por el CLIENTE, donde se establece rigurosamente lo cubierto por el estándar y los servicios a desarrollar.
- 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 el Proyecto.
- El cliente designará una persona interna que realice tareas de interlocución con los diferentes departamentos que pudieran verse involucrados en el Proyecto y para la documentación de las solicitudes de adaptación o modificación solicitadas.
- Los retrasos que pudiesen producirse por circunstancias no atribuibles a CONVISTA o a sus proveedores no serán asumidos por CONVISTA.

- Los retrasos que pudieran producirse por culpa de las acciones u omisiones de CONVISTA o de cualquiera de sus proveedores serán asumidos en todo caso por CONVISTA, siendo plenamente responsable de los daños y/o perjuicios que se pudieran irrogar de las mismas que afectaran a CNP ASSURANCES y/o CNP CAUTION o a terceros.
- En los casos en los que fuera necesario para la ejecución de los servicios CNP ASSURANCES SA. SUC habilitará a CONVISTA el acceso a sus sistemas mediante las herramientas y procedimientos.
- Para la prestación de los servicios contratados no es necesario conceder licencias software ni hardware sobre ninguno de los aplicativos o dispositivos a utilizar.
- CONVISTA no se responsabilizará de ninguna acción o mejora que CNP ASSURANCES y CNP CAUTION precisen realizar en sus sistemas corporativos y que no haya sido contemplada expresamente en el presente 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 actuará sin la debida aprobación del Cliente, CONVISTA será plenamente responsable de dicha acción o mejora y asumirá su coste.

10 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.

11 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 de CNP ASSURANCES o de CNP CAUTION, no dependiendo ni funcional ni orgánicamente y no asumiendo CNP ASSURANCES y CNP CAUTION responsabilidad alguna en materia laboral respecto de los mismos. Para el supuesto de que, por resolución judicial firme el CLIENTE fuera condenada a hacerse cargo de personal que hubiera pertenecido a la plantilla del PROVEEDOR el mismo

deberá pagar a CNP ASSURANCES una cantidad igual a la que CNP ASSURANCES debiera pagar a ese personal en concepto de indemnización por despido improcedente.

En caso de baja de alguno de los empleados de CONVISTA, éste se compromete a reemplazarlo en el plazo máximo de DOS (2) días hábiles.

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 de CNP ASSURANCES y de CNP CAUTION y deberá disponer de una persona encargada de la vigilancia y cumplimiento de tales obligaciones.

CONVISTA deberá entregar a CNP ASSURANCES y CNP CAUTION, 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 soliciten CNP ASSURANCES y CNP CAUTION, 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 a CNP ASSURANCES y a CNP CAUTION 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.

12 Notificaciones

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

1. **CNP ASSURANCES y CNP CAUTION** mediante notificación a:
CNP CAUTION, Sucursal en España/CNP ASSURANCES, S.A. 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.

13 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 4 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.

14 Independencia de las Partes

Este Contrato no convierte a ninguna de las Partes en agente o 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.

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

16 Términos y condiciones

16.1 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 sí misma o a través de sobre cualquier información de CNP ASSURANCES y CNP CAUTION 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.

CNP ASSURANCES y CNP CAUTION estarán 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.

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

16.3 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:

<p>¿Quién es el Responsable del Tratamiento de sus Datos Personales?</p>	<p>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</p> <p>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</p> <p>CNP CAUTION SUCURSAL EN ESPAÑA: Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpSpain.eu</p>
<p>¿Con qué finalidad se tratan sus Datos personales?</p>	<p>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.</p> <p>Los Datos Personales serán conservados mientras sean necesarios para cumplir con las obligaciones contractuales y legales asumidas.</p>
<p>¿Cuál es la legitimación para el Tratamiento de sus Datos Personales?</p>	<p>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.</p>

<p>¿Cuáles son sus derechos cuando facilita sus Datos Personales?</p>	<p>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:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p> <p>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.</p>
---	--

16.4 Obligaciones del Cliente

En el marco de sus actividades empresariales, CNP ASSURANCES y CNP CAUTION estarán obligados 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 de la cual CNP ASSURANCES y CNP CAUTION dispongan en dicho momento. En el supuesto de que no dispusieran de la información solicitada, CNP ASSURANCES y CNP CAUTION dispondrán de un plazo razonable de tiempo para la entrega de la misma, sin dilación indebida.

16.5 Obligaciones de CONVISTA

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

16.6 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 CNP ASSURANCES y CNP CAUTION o terceros ni cedido a terceros por parte de CNP ASSURANCES y CNP CAUTION sin autorización expresa y por escrito de CONVISTA. En caso de utilizar estos elementos, CONVISTA informará por escrito a CNP ASSURANCES y CNP CAUTION sobre la existencia de este tipo de información de su propiedad durante la ejecución del Proyecto.

16.7 Propiedad del sistema y de la solución

CNP ASSURANCES y CNP CAUTION serán titulares 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 de CNP ASSURANCES y CNP CAUTION su uso, no pudiendo reutilizarse por parte de CONVISTA en otros clientes salvo que medio consentimiento previo, expreso y por escrito de CNP ASSURANCES y CNP CAUTION.

CONVISTA garantiza que los trabajos y servicios prestados a CNP ASSURANCES y CNP CAUTION 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.

16.8 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 CNP ASSURANCES y CNP CAUTION no hubieran 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 CNP ASSURANCES y CNP CAUTION, incluso cesar la prestación del control remoto, como el mantenimiento en uso de los servidores contratados con CONVISTA, quedando a su vez liberados CNP ASSURANCES y CNP CAUTION 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 decretado 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.

17 Nulidad o anulabilidad

Cualquier modificación de los presentes Términos y Condiciones Generales o los anexos, si los hubiera, 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 siendo vinculantes para las Partes

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.

18 Legislación aplicable

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

19 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.

20 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.

21 Firma del Contrato

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

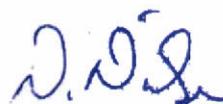
**POR CNP ASSURANCES, S.A., Sucursal
en España Y CNP CAUTION, Sucursal en
España**

**POR CONVISTA CONSULTING &
ADVISORS S.L.U.**

Fdo.: David Lattes



Fdo.: Norbert Nielsen



ANEXO 1

**AL CONTRATO DE
PRESTACIÓN DE
SERVICIOS**

“Proyecto de Implantación
sucursales francesas en SAP”

(Principios Éticos Grupo CNP)

ENTRE

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

Y

**CONVISTA CONSULTING
& ADVISORS S.L.U.**

ANEXO 1 AL CONTRATO DE PRESTACIÓN DE SERVICIOS Proyecto de Implantación sucursales francesas en SAP

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 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 barras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero. La implementación de medidas energéticas 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, mantendremos 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 TURTOSA
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.

**CONVISTA CONSULTING & ADVISORS
S.L.U.**

Fdo.: Norbert Nielsen



**ANEXO 2 AL CONTRATO
DE PRESTACIÓN DE
SERVICIOS**

“Proyecto de Implantación
sucursales francesas en SAP”

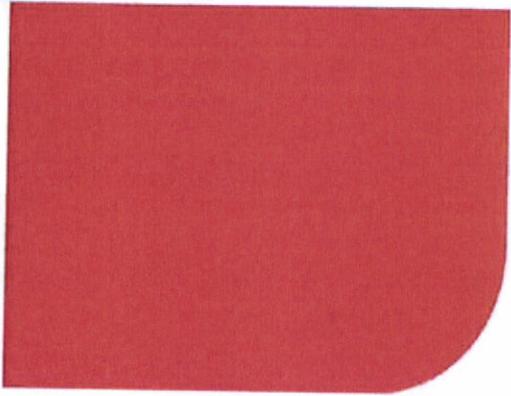
*(Protección de datos
personales)*

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

“Proyecto de Implantación sucursales francesas en SAP”

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

A los efectos de esta cláusula:

‘Responsable de tratamiento’ significa: **CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA y CNP CAUTION, SUCURSAL EN ESPAÑA** (en adelante, el **CLIENTE**).

‘Encargado de tratamiento’ significa: **CONVISTA CONSULTING & ADVISORS S.L.U.** (en adelante, **PROVEEDOR**).

1. Objeto del encargo del tratamiento

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

- | | |
|--|---|
| <input type="checkbox"/> Recogida | <input checked="" type="checkbox"/> Registro |
| <input type="checkbox"/> Estructuración | <input type="checkbox"/> Modificación |
| <input type="checkbox"/> Conservación | <input type="checkbox"/> Extracción |
| <input checked="" type="checkbox"/> Consulta | <input type="checkbox"/> Comunicación por transmisión |
| <input type="checkbox"/> Difusión | <input type="checkbox"/> Interconexión |
| <input type="checkbox"/> Cotejo | <input type="checkbox"/> Limitación |
| <input type="checkbox"/> Supresión | <input type="checkbox"/> Destrucción |
| <input type="checkbox"/> Conservación | <input type="checkbox"/> Comunicación |
| <input type="checkbox"/> Otros: | |

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

"Proyecto de Implantación sucursales francesas en SAP"

2. Identificación de la información afectada

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

- IBAN
- NIF

3. Duración

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

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

4. Obligaciones del encargado del tratamiento

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

- Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

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

- Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
 - El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos (éste último, en el caso de que sea obligatoria su designación de acuerdo a lo dispuesto en la normativa).
 - Las categorías de tratamientos efectuados por cuenta de cada responsable.
 - En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49.1 párrafo segundo del RGPD, la documentación de garantías adecuadas. En todo caso, queda prohibido realizar una transferencia internacional de los datos propiedad del CLIENTE, a un tercer país que no cuente con unas garantías adecuadas.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

- i) La seudoanonimización y el cifrado de datos personales.
- ii) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- iii) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- iv) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

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

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

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

e. Subcontratación

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

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

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

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

- g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:
 - 1. Acceso, rectificación, supresión y oposición
 - 2. Limitación del tratamiento
 - 3. Portabilidad de datos
 - 4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

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

- k. Derecho de información

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

- l. Notificación de violaciones de la seguridad de los datos

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

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

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

- a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

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

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

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

- m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.
- o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- p. Implementar las medidas de seguridad siguientes:

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

En todo caso, deberá implementar mecanismos para:

- (i) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- (ii) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- (iii) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento.
- (iv) Seudonimizar y cifrar los datos personales, en su caso.

51

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

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

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

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

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

- a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
- b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
- c) Realizar las consultas previas que corresponda.
- d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
- e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
- f) Facilitar al encargado la descripción de las medidas de seguridad que debe implementar.

6. Responsabilidad

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

"Proyecto de Implantación sucursales francesas en SAP"

7. Inspección de la Agencia Española de Protección de Datos

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

8. Obligación de cumplimiento

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

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

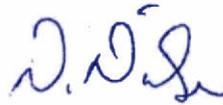
POR CNP ASSURANCES, S.A., Sucursal en
España Y CNP CAUTION, Sucursal en España

POR CONVISTA CONSULTING & ADVISORS
S.L.U.

Fdo.: David Lattes



Fdo.: Norbert Nielsen



ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

"Proyecto de Implantación sucursales francesas en SAP"

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

“Proyecto de Implantación sucursales francesas en SAP”

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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 instaure 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.

41

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 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 de hacking ético y/o penetration test del CLIENTE gestionados por EL PROVEEDOR, mediando un preaviso escrito remitido por EL CLIENTE al

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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.

Dstrucción 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:

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

- 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 entorno compartido dedicado a los Servicios los empleados, subcontratistas o agentes del PROVEEDOR que intervengan en la prestación de los Servicios.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 el acceso y/o 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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

Documentación de la Red

Los sistemas DEL CLIENTE gestionados por EL PROVEEDOR estarán respaldados por diagramas precisos y actualizados y por obligaciones y procedimientos de control documentados.

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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.

→

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 podrán 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

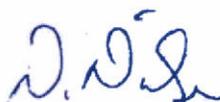
POR CNP ASSURANCES, S.A., Sucursal en
España Y CNP CAUTION, Sucursal en España

POR CONVISTA CONSULTING & ADVISORS
S.L.U.

Fdo.: David Lattes

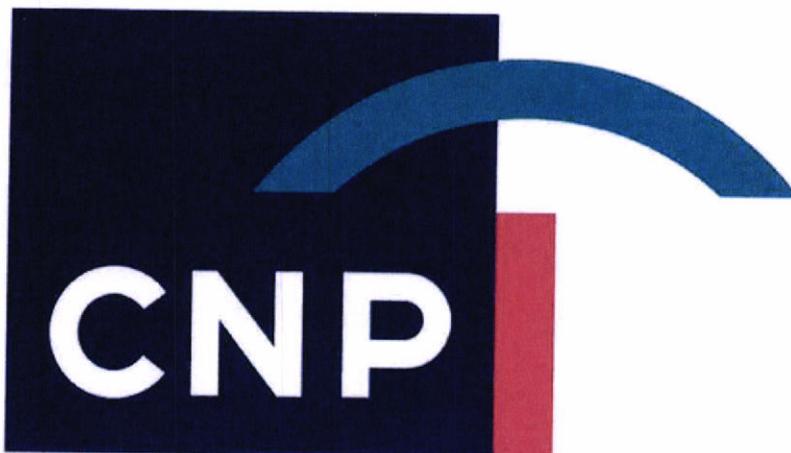


Fdo.: Norbert Nielsen



Contrato de Servicios

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
3 Horario del servicio	5
4 Delimitación del alcance	6
5 Organización del servicio	6
5.1 Planificación	6
5.2 Entregables	7
6 Duración del servicio	7
6.1 Período de contratación del servicio.....	7
6.2 Renovación del servicio.....	7
6.3 Cancelación anticipada del contrato	7
7 Propuesta económica	8
7.1 Coste del servicio	8
7.2 Facturación	8
7.3 Gastos de desplazamiento	9
8 Garantía.....	9
9 Requerimientos y condiciones del servicio.....	9
10 Aplicación de sanciones financieras	10
11 Obligaciones laborales de CONVISTA	10
12 Notificaciones	11
13 Cláusula de prevención frente al fraude, soborno y corrupción.....	12
14 Independencia de las Partes.....	12
15 Cesión y subcontratación	13
16 Términos y condiciones.....	13
16.1 Confidencialidad.....	13
16.2 Protección de datos.....	14
16.3 Datos personales de los firmantes.....	14
16.4 Obligaciones del Cliente.....	15
16.5 Obligaciones de CONVISTA.....	15
16.6 Información propiedad de CONVISTA	16

16.7 Propiedad del sistema y de la solución.....	16
16.8 Causas de terminación anormal.....	16
17 Nulidad o anulabilidad	17
18 Legislación aplicable.....	17
19 Jurisdicción aplicable	17
20 Contrato completo.....	17
21 Firma del Contrato.....	18

1 INTRODUCCIÓN

1.1 Marco previo

CNP CAUTION, SUCURSAL EN ESPAÑA y CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA desean formalizar la petición de servicios realizada a CONVISTA para cubrir los servicios que se describen a continuación necesarios para el desarrollo del proyecto denominado "*Proyecto de Implantación sucursales francesas en SAP*" (en adelante, el "Proyecto") que están llevando a cabo.

CONVISTA es una empresa especializada, entre otros, en la prestación de servicios de consultoría de management y software en general y consultoría informática cuya actividad cubre las necesidades de CNP CAUTION, SUCURSAL EN ESPAÑA y CNP ASSURANCES, S.A., SUCURSAL EN ESPAÑA para la realización del Proyecto.

REUNIDOS

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

Ambas denominadas conjuntamente 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

CNP ASSURANCES y CNP CAUTION solicitan a CONVISTA la prestación de sus servicios de consultoría SAP en el ámbito financiero y tecnológico.

El objetivo del Proyecto es la puesta en marcha de un nuevo sistema tecnológico SAP S/4HANA, con entornos de Desarrollo, Implantación y Producción y la puesta en marcha de un entorno SAP Router y un entorno SAP Solution Manager.

2 Descripción del servicio

El servicio que CONVISTA se compromete a prestar contiene las siguientes tareas:

- Instalación de entornos de Desarrollo, Integración y Producción.
- Instalación del SAP Router.
- Instalación del SAP Solution Manager.
- Inicialización del sistema SAP S/4HANA.
- Inicialización del entorno Fiori.
- Implantación de los módulos de SAP FI, SAP AF, SAP CO para las sociedades 802 y 803 y planes de cuentas P801 – CNP IAM S.A. Sucursal, P802 – CNP ASSURANCES S.A. Sucursal, PSUC – Plan Sucursales Francia.
- Implantación de CONVISTA ELECTRONIC BANK STATEMENT.
- Norma 34 Transferencias bancarias ISO20022 – SEPA CT.
- Norma 43 Para la recepción y carga del extracto bancario.
- Informe de sumas y saldos.
- Transacciones y programas a medida a implantar (como copia de lo actualmente implantado en la máquina actual de SAP ECC).
- ZCNP_DISTRIBUIR_GAST – Reclasificación Gastos Destino.
- ZCNP_ADD_PORC_RECLAS – Tratar Fichero Gastos Destino.
- ZCARTERA – Mantenimiento de ZCARTERA.
- ZFI_EXCEL_FB01 – Carga asientos FI.
- Programa: ZCNP_FI_CARGA_EXCEL_MULT.
- CONVISTA implementará la configuración de los roles y autorizaciones de usuario necesarios según la definición realizada.
- Se realizará la puesta en marcha de un entorno Fiori, pero no se realizarán la implantación de Fiori apps que no vengan con el estándar de inicio.

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 Delimitación del alcance

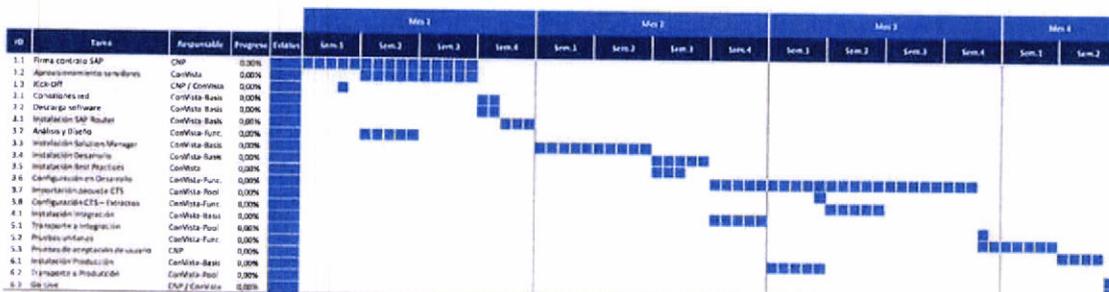
El servicio prestado por CONVISTA no incluirá los siguientes servicios:

- Mantenimiento de hardware (servidores, almacenamiento, redes).
- 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.
- Revisión / supervisión de las instalaciones propias del CPD del cliente (comunicaciones, almacenamiento, ...).
- Dentro de esta propuesta no se encuentran valorado el desarrollo de informes propios del negocio de CNP ASSURANCES y CNP CAUTION que no hayan quedado descritos en la misma. Cualquier otro informe propio del negocio de CNP ASSURANCES y CNP CAUTION que sea adicionalmente necesario deberá ser primero analizado para ver su posible encaje en el estándar de SAP. Todos aquellos informes que no se adapten al estándar de SAP y se soliciten serán valorados por adicionalmente para su implantación.
- No se realizarán adaptaciones al estándar. Cualquier necesidad adicional será estimada adicionalmente.
- No se realizará migración de saldos de cuentas. La inicialización de los saldos de cuentas se realizará mediante un apunte de apertura de cuenta contra una cuenta no relevante.
- No se contemplan actividades relacionadas con los módulos de SAP FAM, SAP BCM, SAP CM ni ningún otro no descrito en la presente oferta.
- No se llevarán a cabo ningún tipo de integración con otros sistemas SAP y no SAP.
- CONVISTA no realizará tareas dentro de los entornos de SAP ECC o cualquier otro que no haya sido descrito en la presente oferta. Si fuera de necesidad que CONVISTA los realizase de estimará adicionalmente.
- CONVISTA realizará la inicialización financiera necesaria en el nuevo sistema SAP S/4HANA para la puesta en marcha de las sociedades descritas en la presente oferta, no realizando ningún tipo de integración contable técnica y o funcional.

5 Organización del servicio

5.1 Planificación

El plan de Proyecto será el siguiente:



5.2 Entregables

A continuación, se presenta el listado de los entregables previstos durante la ejecución del Proyecto, los cuales serán realizados en castellano.

Entregable	Detalle
Documentación de gestión del Proyecto (Informes de seguimiento)	Estos informes tienen como objetivo que los Comités de Gobierno del Proyecto puedan tener conocimiento del estado real del Proyecto y permiten la toma de decisiones que pueda afectar a los objetivos del mismo.
Guías de parametrización	Guías de Parametrización de toda la configuración realizada.
Mapa de sistemas y de integraciones objetivo	Documento con el detalle del mapa de soluciones y sistemas.
Plan de pruebas	Plan de pruebas detallado

6 Duración del servicio

6.1 Período de contratación del servicio

El presente Contrato entre CNP ASSURANCES y CNP CAUTION y CONVISTA entrará en vigor el día 13 de junio de 2022 (fecha de inicio del Proyecto) y será válido hasta poner en marcha las dos sociedades en el sistema productivo (previsto para el día 30 de septiembre de 2022).

No obstante lo anterior, si por causas no imputables al Cliente, el proyecto no pudiera finalizarse a la fecha prevista (30 de septiembre de 2022) CONVISTA tendrá el plazo de un (1) mes de gracia para finalizar dicho proyecto. Consecuentemente, si a fecha 30 de octubre de 2022, CONVISTA no entregase el proyecto al Cliente, se establece como penalización un importe equivalente al 50% del importe que a dicha fecha quedase pendiente de facturar al Cliente. .

6.2 Renovación del servicio

No está prevista una renovación del Contrato , al tratarse de un Proyecto.

6.3 Cancelación anticipada del contrato

En el caso en que el Cliente decidiera cancelar el Contrato de forma unilateral, deberán notificarlo por escrito a CONVISTA con un plazo de antelación suficiente, entendiéndose como tal, al menos, UN (1) mes.

En el supuesto de que CONVISTA incumpliera cualquiera de las obligaciones asumidas en el presente Contrato, el CLIENTE podrá denunciar el Contrato en cualquier momento sin necesidad de preaviso, pudiendo poner fin al mismo de manera inmediata sin que CONVISTA tenga derecho a reclamar indemnización alguna y reservándose su derecho a reclamar aquellos conceptos o daños y perjuicios a los que el Cliente tenga derecho.

En cualquier caso, CNP ASSURANCES SA. SUC abonará el 100% del importe de los servicios que hasta el momento de la resolución efectiva hubieran sido efectivamente realizados.

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 a continuación:

Concepto	Importe
Por grupos de funcionalidades propuestas por CONVISTA	
Gestión del Proyecto	8.400,00 €
Tareas Funcionales / Técnicas	27.000,00 €
Tareas Basis	20.500,00 €
Migración del histórico	5.500,00 €
Tareas de Seguridad	5.000,00 €
Total servicios para la implantación en SAP S/4HANA	66.400,00 €
Descuento de un 5 % sobre los servicios de CONVISTA	-3.162,00 €
Licencia CONVISTA ELECTRONIC BANK STATEMENT	10.000,00 €
Descuento de un 50 % sobre la licencia CTS	-5.000,00 €
TOTAL DE LA PRESENTE OFERTA	68.238,00 €

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.

7.2 Facturación

- Los precios de la presente propuesta no incluyen el Impuesto sobre el Valor Añadido.
- El pago de las facturas se realizará a 30 días desde la fecha de recepción de las facturas en el email indicado a continuación.

- La forma de pago a través de la cual CNP ASSURANCES y CNP CAUTION abonarán el Precio será mediante transferencia bancaria al número de cuenta que conste en las facturas emitidas por CONVISTA para cada una de las entidades..
- Todas las facturas deberán abonarse en el plazo acordado.

El proveedor percibirá los honorarios conforme a los siguientes pagos parciales:

1. 25% del Precio en el momento de la firma del presente Contrato.
2. 25% del Precio en el momento de terminar la instalación de la máquina de SAP Desarrollo
3. 25% del Precio restante en el momento de PRUEBA DE (5.3) terminación del proyecto y su validación por parte del Cliente.
4. 25% restante en el momento de validación de la puesta en producción (Go Live).

El PROVEEDOR girará las pertinentes facturas, una para cada empresa, y las remitirá al email: facturas@cnp.es

7.3 Gastos de desplazamiento

No habrá gastos de desplazamiento.

8 Garantía

El período de garantía del Proyecto comenzará a partir de su aceptación y se extenderá por un periodo de 6 meses a contar desde la terminación del mismo (Go live) sobre errores detectados imputables a los servicios de CONVISTA (no incluyéndose en los mismos cambios o ampliaciones de alcance) o hasta el momento en que se hayan subsanado los mencionados errores, el sistema se encuentre funcionando en perfectas condiciones y haya sido validado por el CLIENTE.

Asimismo, esta garantía solo tendrá valor mientras no se produzcan modificaciones en la solución de gestión de tesorería no controladas por CONVISTA.

9 Requerimientos y condiciones del servicio

- CONVISTA se ceñirá a los requerimientos realizados por el CLIENTE, donde se establece rigurosamente lo cubierto por el estándar y los servicios a desarrollar.
- 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 el Proyecto.
- El cliente designará una persona interna que realice tareas de interlocución con los diferentes departamentos que pudieran verse involucrados en el Proyecto y para la documentación de las solicitudes de adaptación o modificación solicitadas.
- Los retrasos que pudiesen producirse por circunstancias no atribuibles a CONVISTA o a sus proveedores no serán asumidos por CONVISTA.

- Los retrasos que pudieran producirse por culpa de las acciones u omisiones de CONVISTA o de cualquiera de sus proveedores serán asumidos en todo caso por CONVISTA, siendo plenamente responsable de los daños y/o perjuicios que se pudieran irrogar de las mismas que afectaran a CNP ASSURANCES y/o CNP CAUTION o a terceros.
- En los casos en los que fuera necesario para la ejecución de los servicios CNP ASSURANCES SA. SUC habilitará a CONVISTA el acceso a sus sistemas mediante las herramientas y procedimientos.
- Para la prestación de los servicios contratados no es necesario conceder licencias software ni hardware sobre ninguno de los aplicativos o dispositivos a utilizar.
- CONVISTA no se responsabilizará de ninguna acción o mejora que CNP ASSURANCES y CNP CAUTION precisen realizar en sus sistemas corporativos y que no haya sido contemplada expresamente en el presente 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 actuará sin la debida aprobación del Cliente, CONVISTA será plenamente responsable de dicha acción o mejora y asumirá su coste.

10 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 adquiriera 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.

11 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 de CNP ASSURANCES o de CNP CAUTION, no dependiendo ni funcional ni orgánicamente y no asumiendo CNP ASSURANCES y CNP CAUTION responsabilidad alguna en materia laboral respecto de los mismos. Para el supuesto de que, por resolución judicial firme el CLIENTE fuera condenada a hacerse cargo de personal que hubiera pertenecido a la plantilla del PROVEEDOR el mismo

deberá pagar a CNP ASSURANCES una cantidad igual a la que CNP ASSURANCES debiera pagar a ese personal en concepto de indemnización por despido improcedente.

En caso de baja de alguno de los empleados de CONVISTA, éste se compromete a reemplazarlo en el plazo máximo de DOS (2) días hábiles.

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 de CNP ASSURANCES y de CNP CAUTION y deberá disponer de una persona encargada de la vigilancia y cumplimiento de tales obligaciones.

CONVISTA deberá entregar a CNP ASSURANCES y CNP CAUTION, 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 soliciten CNP ASSURANCES y CNP CAUTION, 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 a CNP ASSURANCES y a CNP CAUTION 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.

12 Notificaciones

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

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

CNP CAUTION, Sucursal en España/CNP ASSURANCES, S.A. 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.

13 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 4 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.

14 Independencia de las Partes

Este Contrato no convierte a ninguna de las Partes en agente o 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.

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

16 Términos y condiciones

16.1 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 sí misma o a través de sobre cualquier información de CNP ASSURANCES y CNP CAUTION 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.

CNP ASSURANCES y CNP CAUTION estarán 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.

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

16.3 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:

<p>¿Quién es el Responsable del Tratamiento de sus Datos Personales?</p>	<p>Por parte de CONVISTA:</p> <p>ConVista Consulting:</p> <p>Dirección postal:</p> <p>C/Josep Pla 2, Edificio B3 – Planta 4, E-08019 Barcelona Delegado de Protección de Datos: Oscar.Barrios@convista.com</p> <p>Por parte de CNP ASSURANCES y CNP CAUTION:</p> <p>CNP ASSURANCES SUCURSAL EN ESPAÑA Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpSpain.eu</p> <p>CNP CAUTION SUCURSAL EN ESPAÑA: Dirección postal: Carrera San Jerónimo 21, 28014 Madrid Delegado de Protección de Datos: dpd.es@cnpSpain.eu</p>
<p>¿Con qué finalidad se tratan sus Datos personales?</p>	<p>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.</p> <p>Los Datos Personales serán conservados mientras sean necesarios para cumplir con las obligaciones contractuales y legales asumidas.</p>
<p>¿Cuál es la legitimación para el Tratamiento de sus Datos Personales?</p>	<p>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.</p>

<p>¿Cuáles son sus derechos cuando facilita sus Datos Personales?</p>	<p>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:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p> <p>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.</p>
---	--

16.4 Obligaciones del Cliente

En el marco de sus actividades empresariales, CNP ASSURANCES y CNP CAUTION estarán obligados 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 de la cual CNP ASSURANCES y CNP CAUTION dispongan en dicho momento. En el supuesto de que no dispusieran de la información solicitada, CNP ASSURANCES y CNP CAUTION dispondrán de un plazo razonable de tiempo para la entrega de la misma, sin dilación indebida.

16.5 Obligaciones de CONVISTA

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

16.6 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 CNP ASSURANCES y CNP CAUTION o terceros ni cedido a terceros por parte de CNP ASSURANCES y CNP CAUTION sin autorización expresa y por escrito de CONVISTA. En caso de utilizar estos elementos, CONVISTA informará por escrito a CNP ASSURANCES y CNP CAUTION sobre la existencia de este tipo de información de su propiedad durante la ejecución del Proyecto.

16.7 Propiedad del sistema y de la solución

CNP ASSURANCES y CNP CAUTION serán titulares 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 de CNP ASSURANCES y CNP CAUTION su uso, no pudiendo reutilizarse por parte de CONVISTA en otros clientes salvo que medio consentimiento previo, expreso y por escrito de CNP ASSURANCES y CNP CAUTION.

CONVISTA garantiza que los trabajos y servicios prestados a CNP ASSURANCES y CNP CAUTION 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.

16.8 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 CNP ASSURANCES y CNP CAUTION no hubieran 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 CNP ASSURANCES y CNP CAUTION, incluso cesar la prestación del control remoto, como el mantenimiento en uso de los servidores contratados con CONVISTA, quedando a su vez liberados CNP ASSURANCES y CNP CAUTION 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 decretado 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.

17 Nulidad o anulabilidad

Cualquier modificación de los presentes Términos y Condiciones Generales o los anexos, si los hubiera, 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 siendo vinculantes para las Partes

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.

18 Legislación aplicable

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

19 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.

20 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.

21 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**

"Proyecto de Implantación
sucursales francesas en SAP"

(Principios Éticos Grupo CNP)

ENTRE

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

Y

**CONVISTA CONSULTING
& ADVISORS S.L.U.**

ANEXO 1 AL CONTRATO DE PRESTACIÓN DE SERVICIOS Proyecto de Implantación sucursales francesas en SAP

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 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

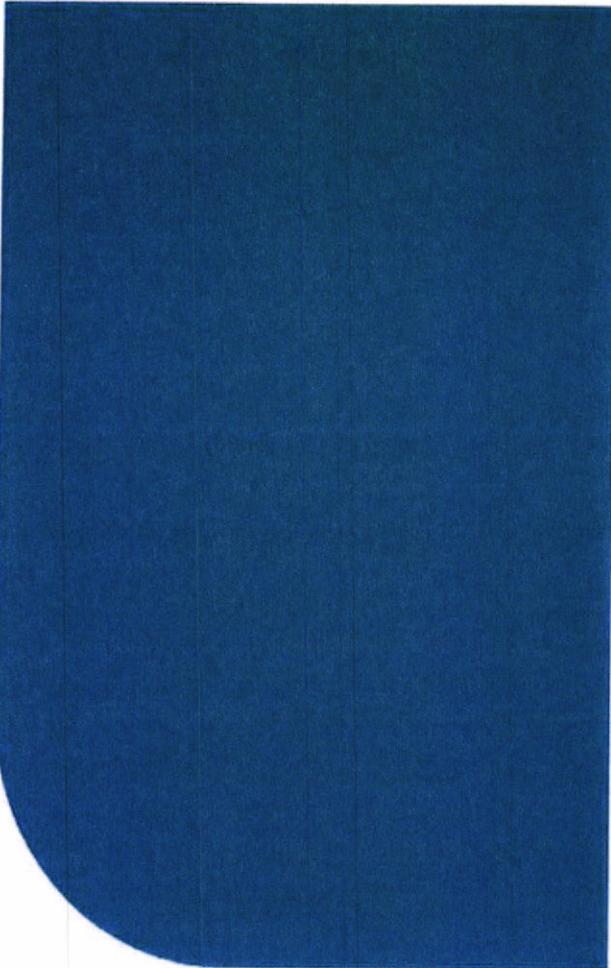
Evelyn TORTOSA
Director Conformidad Grupo

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.

**CONVISTA CONSULTING & ADVISORS
S.L.U.**

Fdo.: Norbert Nielsen



**ANEXO 2 AL CONTRATO
DE PRESTACIÓN DE
SERVICIOS**

“Proyecto de Implantación
sucursales francesas en SAP”

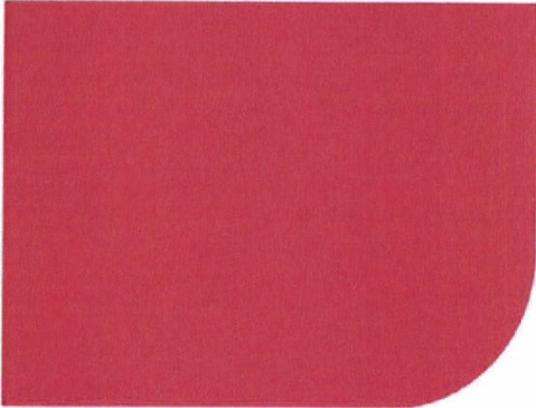
*(Protección de datos
personales)*

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

“Proyecto de Implantación sucursales francesas en SAP”

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

A los efectos de esta cláusula:

‘Responsable de tratamiento’ significa: **CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA y CNP CAUTION, SUCURSAL EN ESPAÑA (en adelante, el CLIENTE).**

‘Encargado de tratamiento’ significa: **CONVISTA CONSULTING & ADVISORS S.L.U. (en adelante, PROVEEDOR).**

1. Objeto del encargo del tratamiento

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

- | | |
|--|---|
| <input type="checkbox"/> Recogida | <input checked="" type="checkbox"/> Registro |
| <input type="checkbox"/> Estructuración | <input type="checkbox"/> Modificación |
| <input type="checkbox"/> Conservación | <input type="checkbox"/> Extracción |
| <input checked="" type="checkbox"/> Consulta | <input type="checkbox"/> Comunicación por transmisión |
| <input type="checkbox"/> Difusión | <input type="checkbox"/> Interconexión |
| <input type="checkbox"/> Cotejo | <input type="checkbox"/> Limitación |
| <input type="checkbox"/> Supresión | <input type="checkbox"/> Destrucción |
| <input type="checkbox"/> Conservación | <input type="checkbox"/> Comunicación |
| <input type="checkbox"/> Otros: | |

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

2. Identificación de la información afectada

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

- IBAN
- NIF

3. Duración

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

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

4. Obligaciones del encargado del tratamiento

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

- Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

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

- Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:
 - El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos (éste último, en el caso de que sea obligatoria su designación de acuerdo a lo dispuesto en la normativa).
 - Las categorías de tratamientos efectuados por cuenta de cada responsable.
 - En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49.1 párrafo segundo del RGPD, la documentación de garantías adecuadas. En todo caso, queda prohibido realizar una transferencia internacional de los datos propiedad del CLIENTE, a un tercer país que no cuente con unas garantías adecuadas.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

- i) La seudoanonimización y el cifrado de datos personales.
- ii) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- iii) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- iv) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

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

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

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

e. Subcontratación

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

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

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

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

- g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- j. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:
 - 1. Acceso, rectificación, supresión y oposición
 - 2. Limitación del tratamiento
 - 3. Portabilidad de datos
 - 4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

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

- k. Derecho de información

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

- l. Notificación de violaciones de la seguridad de los datos

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

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

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

- a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

UC

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

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

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

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

- m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.
- o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- p. Implementar las medidas de seguridad siguientes:

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

En todo caso, deberá implementar mecanismos para:

- (i) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- (ii) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- (iii) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento.
- (iv) Seudonimizar y cifrar los datos personales, en su caso.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

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

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

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

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

- a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
- b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
- c) Realizar las consultas previas que corresponda.
- d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
- e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.
- f) Facilitar al encargado la descripción de las medidas de seguridad que debe implementar.

6. Responsabilidad

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

7. Inspección de la Agencia Española de Protección de Datos

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

8. Obligación de cumplimiento

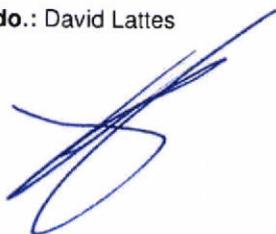
Todo el personal del PROVEEDOR, en su caso, colaboradores y/o subcontratistas, que puedan tener acceso a datos de carácter personal cuyo responsable es CNP ASSURANCES, S.A., Sucursal en España y CNP CAUTION, Sucursal en España deberá cumplir lo establecido en la presente cláusula, cuya obligación subsistirá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

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

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

POR CONVISTA CONSULTING & ADVISORS
S.L.U.

Fdo.: David Lattes



Fdo.: Norbert Nielsen

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

“Proyecto de Implantación sucursales francesas en SAP”

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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 instaure 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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 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 de hacking ético y/o penetration test del CLIENTE gestionados por EL PROVEEDOR, mediando un preaviso escrito remitido por EL CLIENTE al

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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.

Dstrucción 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:

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

- 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 entorno compartido dedicado a los Servicios los empleados, subcontratistas o agentes del PROVEEDOR que intervengan en la prestación de los Servicios.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 el acceso y/o 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.

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

"Proyecto de Implantación sucursales francesas en SAP"

Documentación de la Red

Los sistemas DEL CLIENTE gestionados por EL PROVEEDOR estarán respaldados por diagramas precisos y actualizados y por obligaciones y procedimientos de control documentados.

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

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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.

30

ANEXO 2 AL CONTRATO DE PRESTACIÓN DE SERVICIOS

“Proyecto de Implantación sucursales francesas en SAP”

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 podrán 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