CONTRATO DE ENCARGO DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016

En Guadalajara 04/jul/2023

REUNIDOS

DE UNA PARTE

De una parte, parte BRAVO GARCIA, ALVARO(en adelante, el Responsable del Tratamiento), con CIF 03208259N y con domicilio en CALLE LAGUNA CHICA NUM 19005-GUADALAJARA, representada por el abajo firmante en calidad de apoderado.

DE OTRA PARTE

De otra parte Informática Administrativa, S.A. (en adelante, el Encargado del Tratamiento), con CIF A19010669 y con domicilio en AVDA SANTA MARIA MICAELA 110-112, 19003 GUADALAJARA representada por D.RICARDO SANCHEZ CAUSAPIÉ, abajo firmante en calidad de apoderado.

MANIFIESTAN

I. Que el responsable del tratamiento ha contratado con el encargado del tratamiento contrato de prestación de servicios relativos a la prestación de servicios de gestión fiscal, laboral, gestoría administrativa, financieros, de seguros y de asesoramiento/defensa legal.

II. Que dicho contrato de prestación de servicios se estima adecuado modificar a la vista de la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

III. Que, ambas partes se reconocen mutuamente la capacidad legal necesaria para contratar y obligarse, y, en especial, para celebrar el presente contrato de encargo de tratamiento de datos de carácter personal, llevándolo a efecto conforme a las siguientes

ESTIPULACIONES

1. OBJETO DEL ENCARGO DEL TRATAMIENTO

Mediante las presentes cláusulas se habilita al encargado del tratamiento para tratar por cuenta del responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio detallado en la manifestación primera.
El tratamiento consistirá en la recogida, estructuración, consulta, registro, modificación conservación, extracción, comunicación por transmisión, difusión, interconexión, cotejo, limitación, supresión, destrucción, conservación y comunicación de los datos de carácter personal, todos ellos tipos de tratamiento que son o puedan ser necesarios para la adecuada prestación del servicio.

2. IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento, los datos de carácter personal de clientes, empleados y proveedores.

3. DURACIÓN

El presente contrato tiene la misma duración que la del contrato de prestación de servicios firmado entre las partes. Una vez finalizado el mismo, el encargado del tratamiento debe, conforme a las instrucciones del Responsable del Tratamiento, devolver al responsable los datos personales o suprimir cualquier copia que esté en su poder. Si por normativa legal o responsabilidad frente a terceros que pudiera derivarse del servicio prestado el encargado de tratamiento decidiera mantener una copia de los datos personales, comunicará dicha circunstancia al responsable del tratamiento y mantendrá dicha copia debidamente bloqueada evitando en todo momento el acceso no autorizado.

4. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

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

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios o de terceros.
b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.
Si el encargado del tratamiento considera que alguna de las instrucciones facilitadas por el responsable del tratamiento infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.
c. Registrar, por escrito, todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable. Dicho registro debe contener:

1. El nombre y los datos de contacto del encargado o encargados y de cada

responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

    a) La seudonimización y el cifrado de datos personales.
    b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
    d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
    e) Las medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento.

Las obligaciones indicadas en el presente apartado c) no serán de aplicación en caso de que el encargado del tratamiento emplee a menos de 250 personas, salvo que la prestación que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.

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 o de los Estados miembros que le

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. El encargado del tratamiento se obliga a 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, sin el consentimiento previo del responsable.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 15 días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratada y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en ese plazo de tiempo.

El subcontratado, 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 sub-encargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Se prevén y son aprobadas por las partes las subcontrataciones, con acceso a datos, previstas en el Anexo II de este contrato.

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

g. Garantizar que las personas autorizadas para tratar datos personales se comprometen, 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, respecto a los datos objeto de este encargo y ante el encargado del tratamiento, éste debe comunicarlo por correo electrónico a la dirección *indicada en el encabezado de este acuerdo*. 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

1. El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través correo electrónico a la dirección *indicada en el encabezado de este acuerdo*, 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 violación de seguridad.

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

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

   a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
   b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
   c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
   d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

2. Corresponde al encargado del tratamiento comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos.

   La comunicación contendrá, 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) Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
   c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
   d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

3. Corresponde al encargado del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

   La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

   a) Explicar la naturaleza de la violación de datos.
   b) Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
   c) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
   d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.

m. Dar apoyo al responsable de 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. Implantar las medidas de seguridad derivadas de la evaluación de riesgos realizada por el encargado. Dicha evaluación de riesgos quedará a disposición del responsable a partir de la firma del presente contrato. Si el encargado se adhiere a un código de conducta, dispone de un sello de certificación u otro estándar donde estén definidas las medidas aplicables, deberá entregar al responsable documento de adhesión al código o certificación disponible.

En todo caso, deberá implantar mecanismos para:

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

En todo caso, el Encargado de Tratamiento se compromete al cumplimiento, al menos, de las medidas de seguridad contempladas en el Anexo I de este acuerdo.

q. El Encargado de Tratamiento establece como Delegado de Protección de Datos a: IS Delgado Info Security, S.L.U., cuyo contacto se realizará por la dirección de correo electrónico *juanjo.delgado@isdelgado.es* .

r. Destino de los datos al finalizar la prestación.

A la finalización del contrato de prestación de servicios el encargado tendrá que llevar a cabo una de las siguientes acciones, a elección del responsable:

1. Devolver al responsable del tratamiento 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.

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

2. Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación.

   La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

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

3. 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, el encargado puede conservar una copia, con los datos debidamente boqueados, 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, en los casos que determine la AEPD.
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.

6. INFORMACIÓN SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En cumplimiento del artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, le facilitamos la siguiente información sobre los datos de carácter personal que obran en este contrato y sobre los que se pudieran necesitar para llevar a cabo la ejecución del mismo.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS	
Responsable	Informática Administrativa, S.A.
Finalidad	Consecución y gestión administrativa de la relación jurídica establecida con el titular de los datos y/o la entidad a la que pertenece/representa y prestación de los servicios propios del responsable de tratamiento.

Legitimación	Consentimiento del interesado: ejecución de un contrato entre las partes
Destinatarios	Se comunicarán datos a terceros para poder llevar a cabo las finalidades objeto de este contrato y en concreto a la Administración pública competente. En ningún caso se cederán datos a terceros para finalidades diferentes a las descritas en este documento.
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Delegado de protección de datos	La dirección de correo electrónico del Delegado de Protección de datos es: juanjo.delgado@isdelgado.es .

FIRMAS

EL RESPONSABLE

EL ENCARGADO

Fdo. Ricardo Sánchez Causapié
Gerente

Firmado digitalmente por: 03097911H RICARDO SANCHEZ (R: A19010669)
2023.07.04 11:33:46 +02'00'

ANEXO I
SEGURIDAD SOBRE LOS SISTEMAS QUE DESARROLLAN EL TRATAMIENTO DE DATOS PERSONALES

El Encargado del Tratamiento (ET en adelante) se compromete a llevar a implementar las siguientes medidas de seguridad de carácter técnico y organizativo, a fin dar satisfacción a las exigencias del RGPD.

I. CONTROL DE ACCESO:

El ET establecerá mecanismos para garantizar la limitación de acceso a los datos de carácter personal implicados en los tratamientos de datos objeto de este contrato, conforme a los siguientes criterios de acceso mínimo y habilitación conforme a la necesidad de conocer la información por parte del usuario, en relación con su rol en la Organización del ET y la participación necesaria del mismo en el tratamiento.

II.- IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS:

El sistema de acceso al tratamiento de datos personales deberá disponer de mecanismos efectivos y acordes al estado de la tecnología que garanticen la identificación y autenticación inequívoca del usuario.

Las claves de acceso serán conformadas conforme a criterios de complejidad (mínimo 8 caracteres, alfanuméricos, combinando mayúsculas, minúsculas y símbolos).

La caducidad de las claves no será nunca superior a 90 días.

La conservación de las claves en los sistemas operativos y aplicaciones se realizará de forma protegida para cualquier usuario o personal de la empresa (incluido los usuarios administradores), mediante métodos de cifrado o hash de reconocida eficacia.

El diálogo automatizado del proceso de identificación-autenticación de usuarios se realizará siempre por garantizando la confidencialidad de las claves e identidad del usuario.

Se establecerá un límite de intentos de accesos fallidos de inicio de sesión no superior a 6 (recomendable 3).

El ET se compromete a disponer de un procedimiento adecuado de distribución de las claves que garantice la confidencialidad de las mismas y su exclusivo conocimiento por parte del usuario.

Se establecerán políticas corporativas para garantizar la confidencialidad y secreto de las claves.

No se admitirán usuarios genéricos y/o claves compartidas.

Se consideran recomendables y preferibles los sistemas de doble factor de autenticación del usuario.

III. ACCESO POR REDES DE TELECOMUNICACIONES:

Todo acceso a datos personales, objeto de los tratamientos protegidos por el acuerdo del que este documento es anexo y conforma parte indivisible, empleando redes de telecomunicaciones y en especial a través de redes públicas, deberá llevarse a cabo garantizando, al menos, el mismo nivel de seguridad que en el entorno local.

Todo tratamiento de datos personales a través de redes públicas e Internet se desarrollará por canales cifrados.

Se garantizará el uso de estándares de cifrado y protocolos de reconocido prestigio y seguridad.

Se evitará la comunicación de documentos confidenciales por correo electrónico, sin emplear sistemas de cifrado que garanticen la seguridad de extremo a extremo. Esta medida de seguridad únicamente será excepcionada previa petición expresa y bajo la responsabilidad del Responsable del Fichero.

Se prohíbe el acceso remoto a los sistemas del ET por medios no cifrados. Todo acceso remoto debe ser expresamente autorizado y debe disponerse de un registro del personal autorizado.

IV. POLÍTICA DE SEGURIDAD

El ET se compromete a elaborar, difundir y establecer las medidas necesarias de aplicación efectiva de una política de seguridad corporativa que garantice la seguridad de los datos personales objeto de tratamiento, respetando los contenidos de este acuerdo, así como cualquier disposición legal de aplicación.

La política de seguridad incorporará medidas que garanticen la seguridad de los datos tratados en medios analógicos.

V. CONTROL DE ACCESO FÍSICO:

El ET establecerá las medidas necesarias para garantizar el control de acceso físico únicamente al personal expresamente habilitado, a las ubicaciones en las que se localizan la información de carácter personal y/o se llevan a cabo los tratamientos de los datos.

Deberá considerarse especialmente la restricción de acceso físico a las dependencias en las que se ubiquen los principales sistemas informáticos de tratamiento (Centros de Proceso de Datos y Salas de Servidores).

El ET dispondrá de un listado de personal habilitado para el acceso a dichas dependencias.

VI. GESTIÓN DE SOPORTES

El ET dispondrá de una política adecuada y de plena aplicación en su Organización al respecto del uso de soportes en los que pueda encontrarse información de carácter personal objeto de los tratamientos protegidos por este acuerdo.

La política contendrá medidas que garanticen la seguridad de los datos durante todo el ciclo de vida del soporte y la información.

Se garantizará la destrucción segura de soportes desecho.

Se establecerán medidas de seguridad para evitar el uso de soportes no autorizados en los sistemas del ET.

El personal con acceso a soportes no automatizados con datos de categorías especiales de conformidad con el art. 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, deberá ser expresamente autorizado y conservarse un registro documentado y actualizado del mismo.

VII REGISTRO DE INCIDENCIAS Y LOGS DE AUDITORÍA

El ET se compromete a disponer de un registro de incidencias ocurridas sobre el tratamiento de los datos personales y los recursos en el implicados. Este registro será conservado, al menos 2 años.

El ET dispondrá de sistemas de registro y log de auditoría de la actividad de los usuarios, así como de los principales de eventos de seguridad del sistema.

Los logs serán conservados de manera segura evitando que estos puedan ser alterados por el personal usuario o administrador.

VIII COPIAS DE RESPALDO

El ET dispondrá de un sistema de copias de respaldo/copias de seguridad que garantice la recuperación de los datos implicados en los tratamientos objeto de este acuerdo.

El procedimiento de copias de respaldo deberá contemplar, al menos una copia diaria de los datos.

Se conservará una copia de seguridad, al menos semanal, en lugar diferenciado de la ubicación de los sistemas de tratamiento salvaguardados.

Las copias de respaldo serán custodiadas de manera efectiva por el personal habilitado al efecto y dispondrán de mecanismos que eviten el acceso no autorizado a la información en ellas contenida, preferentemente por medio de métodos de cifrado.

El ET se compromete a realizar simulacros de recuperación, al menos semestralmente.

IX COPIAS TEMPORALES

El ET adoptará las medidas adecuadas para garantizar que las copias temporales de datos sean sometidas a medidas de seguridad equivalentes a las establecidas en los medios en producción.

X AUDITORÍA

El ET dispondrá de un plan de auditorías en materia de cumplimiento de la legislación de protección de datos, al menos de carácter bianual.

Los resultados de las auditorías podrán ser solicitados y revisados por el Responsable del Tratamiento.

ANEXO II
SUBCONTRATACIONES PREVISTAS Y ADMITIDAS

- **IS DELGADO INFO SECURITY, S.L.U., con CIF B-19259639 a los efectos de prestación de los servicios de Delegado de Protección de Datos.**
- **INFORMADSA SERVICIOS INFORMÁTICOS, S.L. con CIF B19166776 a los efectos de la prestación de los servicios de provisión y mantenimiento de sistemas informáticos.**
- **INFORMADSA GESTORÍA, S.L., con CIF B19152172 a los efectos de la prestación de servicios de gestoría administrativa.**
- **INFORMADSA FINANCIEROS, S.L., con CIF B19257427 a los efectos de la prestación de servicios financieros.**
- **GEYCE AGP SOFTWARE S.L., con CIF B64206634 a los efectos de provisión, mantenimiento y soporte de aplicativos de gestión.**