CONTRATO DEFENSOR DEL PARTÍCIPE

BUY & HOLD SGIIC, S.A.

D. A. DEFENSOR

En Madrid, a 4 de octubre de 2017

REUNIDOS

De una parte, **D... Rafael Valera de Vargas,** mayor de edad, con domicilio, a estos efectos, en Madrid, C/ Monte Esquinza nº 13 – bajo izquierda.

Y de otra, **D. RICARDO MARTÍNEZ GALÁN**, mayor de edad, con domicilio en Madrid, C/ Velázquez, nº 80- 1º Dcha.

INTERVIENEN

El primero de ellos en nombre y representación de BUY & HOLD, SGGIIC, S.A., C.I.F. nº A98474208, apoderado suficiente al efecto, conforme consta en el poder otorgado ante el Notario de Madrid, D. JAVIER-MÁXIMO JUÁREZ GONZÁLEZ, el 11 de mayo de 2017, nº de protocolo 1676.

El segundo, en nombre y representación de **D.A. DEFENSOR, S.L.**, C.I.F. nº B-81414443, asimismo apoderado suficiente para este acto, según escritura otorgada ante el Notario de Madrid, D. Andrés Sanz Tobes, el 11 de mayo de 2004, nº de protocolo 969.

MANIFIESTAN

1º.- Que de acuerdo con las conversaciones mantenidas previamente a este acto, BUY & HOLD, SGIIC, S.A. ha manifestado su interés en contratar los servicios de D.A. DEFENSOR como Defensor del Partícipe y ésta en prestarlos, por lo que han acordado celebrar el presente contrato, que se regirá por las siguientes:

ESTIPULACIONES

Primera.- OBLIGACIONES DE D.A.DEFENSOR.

1.- Atención, tramitación y resolución de quejas y reclamaciones:

D.A. DEFENSOR tramitará y resolverá cuantas reclamaciones le sean formuladas en relación con B&H JUBILACIÓN, PLAN DE PENSIONES, promovidos por la Entidad, de acuerdo con las normas de actuación contenidas en su Reglamento para la Defensa del Cliente.

La Entidad podrá incorporar otros planes al presente contrato, en los términos económicos previstos en la estipulación tercera. A estos fines, se entenderán incluidos todos los planes de pensiones promovidos por B&H respecto a los cuales D.A. DEFENSOR haya emitido aceptación.

2.- Atención directa:

D.A. DEFENSOR atenderá, por vía telefónica o presencialmente, las consultas de los partícipes y beneficiarios de los planes de pensiones en los que aquél ejerza como Defensor del Partícipe.

3.- Informe anual:

D.A. DEFENSOR se compromete a entregar a la Entidad la Memoria Anual dentro del primer trimestre de cada año, en la que se informará sobre las actividades desarrolladas por aquél. En dicha Memoria se incluirá un informe relativo a las actividades realizadas para B&H en el cumplimiento del presente contrato, incluyendo propuesta sobre las medidas que, en su caso, se consideren oportunas para la mejora en el servicio a los clientes.

El informe citado podrá ser sustituido, en su caso, por una certificación expedida por D.A. DEFENSOR en la que se indique la ausencia de reclamaciones en el periodo.

Segunda. - OBLIGACIONES DE B&H.

1.- La Entidad se obliga al pago de los honorarios acordados en la cláusula tercera, en contraprestación a los servicios desarrollados por el Defensor en el marco del presente contrato.

2.- Asimismo, se compromete a prestar la colaboración necesaria en la instrucción de los procedimientos de resolución de las quejas y reclamaciones planteadas ante el Defensor, de acuerdo con las normas de actuación contenidas en su Reglamento. A este fin, la Entidad nombrará un interlocutor que dispondrá de capacidad operativa suficiente para el suministro de la información referida.

3.- Por otro lado, la Entidad se compromete a aceptar las resoluciones dictadas por el Defensor siempre y cuando éstas resulten vinculantes para la misma, de acuerdo con las competencias reconocidas en el Reglamento para la Defensa del Cliente.

Tercera.- HONORARIOS.

En pago de los servicios acordados, B&H abonará a D.A. DEFENSOR la cantidad de TRESCIENTOS EUROS (300,00 €) TRIMESTRALES.

En caso de que la Entidad decidiera extender la designación de D.A. DEFENSOR como Defensor del Partícipe a otros planes de pensiones promovidos por ella, distintos de los especificados en la estipulación primera, los honorarios anteriores se incrementarían en CIENTO CINCUENTA EUROS (150,00 €) trimestrales por cada uno de ellos, con un tope máximo de MIL EUROS (1.000,00 €), cualquiera que fuera el número de planes.

No obstante, cuando el número de reclamaciones anuales recibidas sea superior a TRES, a partir de dicha cantidad, por cada reclamación que sea tramitada por D.A. DEFENSOR, se facturará una cantidad adicional de CIENTO VEINTE EUROS (120,00 €) por expediente. Las cantidades que correspondan por este concepto se liquidarán una vez concluido el ejercicio.

Los honorarios indicados en el presente apartado se verán incrementados con el correspondiente I.V.A. o los impuestos que sean aplicables en cada momento.

Anualmente se procederá a la actualización de los honorarios vigentes durante el año inmediatamente transcurrido, conforme a las variaciones experimentadas por el IPC publicado por el INE para el periodo de los doce meses anteriores. La primera actualización tendrá lugar en el mes de enero de 2018.

Cuarta. - DURACIÓN Y RESOLUCIÓN.

El presente contrato se pacta por una duración de dos años a contar desde el día de la fecha, prorrogándose por periodos sucesivos iguales.

No obstante, cualquiera de las partes podrá instar la resolución del contrato por cualquier medio que deje constancia de la decisión, comunicada con un plazo de preaviso de un mes a la fecha en que pretenda hacerse efectiva la resolución del contrato.

La resolución anticipada conforme a lo acordado en el párrafo anterior no dará derecho a la otra parte a exigir indemnización alguna, sin perjuicio de la liquidación de honorarios que correspondan a D.A. DEFENSOR en función del periodo transcurrido.

Quinta.- PROMOCIÓN Y PUBLICIDAD.

Sin perjuicio de las obligaciones de información al cliente que le competen, la Entidad podrá dar publicidad del Defensor en toda su documentación contractual, y en cuantos medios considere idóneos, con objeto de promocionar esta figura.

Sexta.- CLÁUSULA DE CONFIDENCIALIDAD.

El Defensor se compromete a utilizar, con carácter exclusivo, en el ejercicio de las actividades propias de la relación contractual establecida, los materiales, información y cuanta documentación disponga durante la vigencia del contrato con B&H, reconociendo que todo ello constituye propiedad exclusiva de la misma.

Asimismo, el Defensor, tanto a través de sus empleados y directivos, asume el compromiso formal e irrevocable de mantener la más estricta confidencialidad respecto a la forma de actuación comercial de B&H, así como de los métodos y procedimientos que dicha compañía emplea, tanto en la captación de clientes como en la atención de los mismos en caso de pago de prestaciones.

Por lo tanto, si una vez extinguida la relación contractual con B&H o incluso durante la vigencia del contrato, el Defensor estableciese relaciones contractuales con otras compañías del sector, se compromete a no hacer uso, ni por sí, ni por medio de terceros de la citada información.

Ambas partes convienen que los citados métodos de funcionamiento constituyen secretos empresariales sometidos al deber de reserva, a los efectos de lo dispuesto en el artículo 13 de la Ley 3/91 de 10 de enero de Competencia Desleal.

Séptima.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

El presente contrato se suscribe al amparo de lo dispuesto en el artículo 29 de la Ley 44/2002, de 22 de Noviembre, de Medidas de Reforma del Sistema Financiero, que prevé la designación por las entidades aseguradoras de un Defensor del Cliente, y se acoge a lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, toda vez que la colaboración de las partes en la prestación por el Defensor de los servicios previstos en este contrato conlleva necesariamente el tratamiento por ambas partes de datos de carácter personal.

En cumplimiento de dicha disposición, ambas partes acuerdan que el acceso y consiguiente tratamiento de los datos de carácter personal que el presente contrato implica se lleve a efecto de conformidad con lo establecido en el Anexo I.

Octava.- JURISDICCIÓN.

Para la resolución de cuantas cuestiones pudieran surgir de la aplicación o interpretación de este contrato, por la presente ambas partes acuerdan someterse a la jurisdicción de los Juzgados y Tribunales de Madrid.

Y en prueba de conformidad, ambas partes llevan a cabo la firma del presente contrato por duplicado ejemplar y a un solo efecto, en el lugar y la fecha señalados en el encabezamiento.

Por B&H

Rafael Valera de Vargas

Por D.A. DEFENSOR

Ricardo Martínez Galán

ANEXO I
CLÁUSULA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1.- Tratamiento de datos de carácter personal

1.1. Las partes podrán acceder y proceder al tratamiento de datos de carácter personal contenidos en determinados ficheros a los exclusivos fines previstos en este contrato, lo que se llevará a efecto con sujeción en todo momento a lo dispuesto en la legislación vigente en materia de Protección de Datos de Carácter Personal.

1.2. La titularidad de los ficheros de datos de carácter personal, a efectos de lo previsto en la Ley, corresponde a B&H que será, por tanto, quien decida en todo momento sobre la finalidad, contenido y uso del tratamiento.

1.3. D.A. DEFENSOR, como encargado del tratamiento, tratará los datos ajustándose en todo momento a lo previsto en el presente anexo y a las instrucciones escritas que al respecto reciba del responsable del tratamiento.

1.4. D.A. DEFENSOR custodiará con la máxima diligencia los datos proporcionados para su tratamiento por el responsable del fichero, adoptando los controles de seguridad exigidos por la LOPD, por su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre, o por cualesquiera otras normas que vengan a modificar, a sustituir o complementarlas.

En consecuencia, D.A. DEFENSOR deberá cumplir y tener implementadas en todo momento las medidas de seguridad legalmente exigidas para el nivel alto, que al día de hoy son las siguientes:

1.4.1. Elaborar e implantar las medidas de seguridad mediante un Documento de Seguridad de obligado cumplimiento para el personal con acceso a los datos y a los sistemas de información, con los requerimientos legalmente establecidos al respecto en cada momento, en concreto las previstas en los artículos 89 y siguientes del Reglamento de desarrollo de la LOPD. En cualquier caso, las medidas de seguridad serán como mínimo las descritas en el apartado 2 del presente anexo.

1.4.2. Establecer el procedimiento de notificación y gestión de incidencias, así como el registro de las mismas.

1.4.3. Establecer los procedimientos de identificación inequívoca y personalizada y de autentificación de los usuarios para su acceso a los datos de carácter personal, limitando la posibilidad de intentar reiteradamente los accesos no autorizados.

1.4.4. Establecer el control y registro del acceso a los datos y recursos, evitando en todo caso que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.

1.4.5. Establecer el procedimiento de gestión de soportes, impidiendo la salida de soportes informáticos que contengan datos de carácter personal fuera de los locales del encargado del tratamiento.

1.4.6. Designar un responsable de seguridad.

1.4.7. Someter, en caso de prórroga del contrato, cada dos años a una auditoria los sistemas de información e instalaciones de tratamiento de datos, de cuyas conclusiones informará al responsable del tratamiento.

1.4.8. Impedir el acceso del personal no autorizado a los locales donde se encuentren los sistemas de información con datos de carácter general.

1.4.9. En caso de transmisión de datos de carácter personal a través de redes de telecomunicaciones, se garantizará que los mismos no sean inteligibles ni manipulados por terceros.

Y, en general, cualquier otra medida de seguridad que legalmente sea de aplicación a los datos de carácter personal que sean objeto de acceso en virtud del presente contrato.

1.5. D.A. DEFENSOR mantendrá informado en todo momento a todos sus empleados, incluidos los trabajadores de empresas de trabajo temporal, las obligaciones que les competen en cuanto al cumplimiento de lo establecido en materia de protección de datos de carácter personal tanto en la legislación vigente como en el presente contrato, obligándoles contractualmente a cumplir las medidas de seguridad legal y contractualmente exigibles.

1.6. D.A. DEFENSOR informará inmediatamente al responsable del tratamiento de cualquier incidencia que se produzca en el tratamiento de los datos.

1.7. Los derechos de acceso, rectificación, cancelación y oposición se ejercitarán por los afectados ante el responsable del tratamiento, debiendo el encargado del tratamiento remitir de forma inmediata cualquier solicitud que reciba al respecto.

1.8. Una vez cumplida la prestación contractual, D.A. DEFENSOR deberá devolver al responsable del tratamiento, en el plazo máximo de un mes, todos los documentos o soportes que contengan datos de carácter personal a los que haya tenido acceso o tratado en virtud del presente contrato, procediendo a su borrado o destrucción cuando tal devolución no sea posible, obligándose expresamente a no guardar en ningún caso copia de los mismos.

1.9. D.A. DEFENSOR se obliga al secreto profesional respecto a los datos de carácter personal que hayan sido objeto del tratamiento, tanto durante la vigencia del contrato como después de su finalización.

2.- Medidas de seguridad

Se reproducen a continuación las medidas de seguridad establecidas por el Reglamento de desarrollo de la Ley Orgánica 13/1999, de 15 de diciembre, de Protección de Datos de Carácter personal, aprobado por R.D. 1720/2007, de 21 de diciembre, que deben aplicarse en el tratamiento previsto en el contrato.

2.1.- MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

2.1.1. Medidas de seguridad de nivel básico

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

2.1.2. Medidas de seguridad de nivel medio

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede

ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

2.1.3. Medidas de seguridad de nivel alto

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este

título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

2.2. MEDIDAS DE SEGURIDAD APLICABLES A LOS FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

2.2.1. Medidas de seguridad de nivel básico

Artículo 105. Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a) Funciones y obligaciones del personal.
b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

2.2.2. Medidas de seguridad de nivel medio

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

2.2.3. Medidas de seguridad de nivel alto

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.