DOCUMENTO DE SEGURIDAD DE:

ALBERTO RODRIGUEZ PALOMINO

Para el cumplimiento de la Ley 15/1999 y el RD. 1720/2007

Ley Orgánica de Protección de Datos (LOPD)

Adaptación realizada por:

Soluciones en LOPD

Versión: 1 **Fecha: 06 / 11 / 2017**

INTRODUCCIÓN

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) establece en su artículo 9 el principio de seguridad según el cual "Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de datos".

En fecha 19 de Enero de 2008, se publicó el Real Decreto 1720/2007, por el que se desarrolla LOPD y se establecen las medidas de seguridad a cumplir para sistemas de información, ya sean automatizados o manuales.

El objeto del presente documento es recoger la normativa de la empresa referente a las medidas de seguridad de obligado cumplimento para todo el personal con acceso a los datos de carácter personal que se mantienen automatizados y en soporte papel, así como para los sistemas de información, tal y como prevé el Real Decreto 1720/2007.

Debido a la continua evolución y cambios intrínsecos de los sistemas de información y a la propia complejidad de la organización, el documento intentará ser un marco estable, y a su vez, flexible, en lugar de una descripción estática, en cuyo caso se vería sometido a continuas actualizaciones.

El presente documento se mantendrá en todo momento actualizado por el Responsable de Seguridad y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

De igual forma, el Documento de Seguridad se adecuará, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El Real Decreto 1720/2007, especifica que se puede disponer de un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido. Cualquiera de las opciones puede ser válida. En este caso se ha optado por el primer tipo, organizando el "documento de seguridad" en dos partes: en la primera se recogen las medidas que afectan a todos los sistemas de información de forma común con independencia del sistema de tratamiento sobre el que se organizan: informatizado, manual o mixto, y en la segunda se incluye el Anexo A con la descripción de cada fichero y siguientes Anexos con la descripción del sistema de información y medidas de seguridad aplicadas por la empresa.

DOCUMENTO DE SEGURIDAD

Artículo 88 RDLOPD. El documento de seguridad.

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.
2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.
3. El documento deberá contener, como mínimo, los siguientes aspectos:
-Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
-Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
-Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
-Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
-Procedimiento de notificación, gestión y respuesta ante las incidencias.
-Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
-Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.
4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:
-La identificación del responsable o responsables de seguridad.
-Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.
5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.
6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.
7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.
8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento 1720/2007 (RLOPD) y en la Ley orgánica 13/1999 de Protección de Datos de Carácter Personal (LOPD).

Con relación a las medidas de seguridad exigidas por ley, se distinguen tres niveles de seguridad aplicables a los Ficheros de datos de carácter personal, nivel de seguridad alto, nivel de seguridad medio y nivel de seguridad básico, niveles que se aplicarán en función de los tipos de datos tratados en los Ficheros objeto del presente documento, por tanto:

NIVEL ALTO. Ficheros o tratamientos con datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico; recabados con fines policiales sin consentimiento de las personas afectadas; y derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos relativos a la comisión de infracciones administrativas o penales; que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito); de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias; de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros; de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias; de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal, como nombre, dirección, teléfono, estado civil,..... También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros; se trate de ficheros o tratamientos de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero; y en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

Las medidas de seguridad de nivel básico son exigibles en todos los casos. Las medidas de nivel medio complementan a las anteriores en el caso de ficheros clasificados en este nivel, y las de nivel alto, cuando deban adoptarse, incluyen también las de nivel básico y medio.

INDICE GENERAL

6) CLAUSULAS

Descripción de las cláusulas jurídicas.

1. Cláusulas para trabajadores.
2. Cláusulas acciones comerciales y publicitarias.
3. Cláusulas para recabar datos de trabajadores.
4. Cláusulas para recabar datos de clientes.
5. Cláusula obtención consentimiento clientes.
6. Cláusula informativa para el e-mail.
7. Cláusula para documentos de clientes.
8. Circular informativa implantación LOPD.
9. Circular currículum vitae.
10. Rótulo informativo. (Derecho de Información.)

7) LSSICE (sólo visible si se tiene web)

1. Cláusulas sitio web. (Aviso legal, LSSICE, Anexo y formularios web.)

8) Video vigilancia (sólo visible si se tienen ficheros de video)

1. Impreso video vigilancia. (Plantilla afectado video vigilancia.)
2. Cartel video vigilancia.

9) Usos y recomendaciones

1. Manual de usos y recomendaciones. (Para todos los usuarios con acceso.)

10) Medidas de seguridad

1. Manual de medidas de seguridad y organizativas.
2. Medidas de destrucción. (Desechos informáticos.)

11) Registros de actualizaciones, auditoría y accesos

1. Registro de modificaciones y actualizaciones del Doc. de Seguridad y Anexos.
2. Registro de auditorías y controles periódicos.
3. Registro de accesos.
4. Incidencias, peticiones, formularios, registros y anotaciones cumplimentados.

12) CONTRATOS

Prestación de servicios con acceso a datos:

1. Contratos de Encargados de tratamiento (si existieran) debidamente firmados.
2. Contratos de tratamientos (si existieran) debidamente firmados.

Prestación de servicios sin acceso a datos:

1. Documentos confidencialidad colaboradores. (si existieran) debidamente firmados.

Acuerdo de cesiones:

1. Contrato de acuerdo de cesión de datos (si existieran) debidamente firmados.

13) PERSONAL

Documentos, impresos y recibos cumplimentados.

1. Impresos para trabajadores (si existieran) debidamente firmados.
2. Recibos del manual de usos y recomendaciones (si existieran) debidamente firmados.

14) AEPD

Cartas de Inscripción (Ficheros), modificación o supresión del fichero/s que remitirá la AEPD con el número identificativo de los fichero/s.

15) Soluciones LOPD

Documentación relativa al consultor, profesional o empresa que realiza la adaptación.

3) DOCUMENTO DE SEGURIDAD

1. Ámbito de aplicación del documento.
2. Funciones / obligaciones del personal.
3. Medidas, normas y procedimientos.
4. Gestión de Incidencias.
5. Contraseñas y copias de seguridad.
6. Gestión de soportes y documentos.
7. Ficheros NOTA.
8. Controles periódicos / auditorías.
9. Encargados de tratamiento.
10. Tratamiento de ficheros, sistemas y soportes.

1) ÁMBITO DE APLICACIÓN DEL DOCUMENTO

ALBERTO RODRIGUEZ PALOMINO, como consecuencia de las actividades desarrolladas dentro de su actividad, necesariamente trata información y datos de carácter personal.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los datos de carácter personal sometidos a tratamiento por ALBERTO RODRIGUEZ PALOMINO.

Por consiguiente, los recursos comprendidos en el ámbito de aplicación de este documento serán todos los datos de carácter personal que componen los ficheros inscritos en el Registro General de Protección de Datos (automatizados y en soporte papel) y los tratamientos de datos que realiza ALBERTO RODRIGUEZ PALOMINO como Encargado de tratamiento.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger las aplicaciones, herramientas de actualización y consulta, y sistemas que tratan los datos de carácter personal, los equipos informáticos que las soportan, los dispositivos de archivo y los locales donde estos se ubican.

En los anexos del presente Documento se recoge:

- Información de los ficheros declarados en el Registro General de Protección de Datos, indicando el entorno donde se encuentran ubicados y las aplicaciones que los gestionan.

- Descripción de los sistemas de información existentes en ALBERTO RODRIGUEZ PALOMINO en sus aspectos más relevantes: dispositivos de archivo, servidores, bases de datos, aplicaciones, accesos a red, dispositivos de control de acceso, método y frecuencia de las copias de seguridad, etc...

- Relación de las aplicaciones existentes que tratan datos de carácter personal, en cada uno de los diferentes equipos informáticos existentes en ALBERTO RODRIGUEZ PALOMINO.

Este documento ha sido elaborado bajo la responsabilidad de ALBERTO RODRIGUEZ PALOMINO, quien, como Responsable del Fichero, se compromete a implantar y actualizar la normativa de Seguridad que de él se desprende. Dicha normativa será de obligado cumplimiento para todo el personal que tenga acceso a los datos de carácter personal y/o a los sistemas de información que permiten el acceso a los mismos.

Los datos de identificación del RESPONSABLE DEL FICHERO son los siguientes:

- **RAZÓN SOCIAL:** ALBERTO RODRIGUEZ PALOMINO
- **NIF/CIF:** 51126442H
- **DOMICILIO:** C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID
- **DIRECCIÓN DE ACCESO DE LOS FICHEROS:** La especificada en el **ANEXO D (Locales)**
- **ACTIVIDAD:** COMERCIO

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

Nombre fichero	**Fecha inscripción o modificación**	**Código inscripción**	**Sistema Tratamiento**	**Nivel seguridad**
CLIENTES/PROVEEDORES			Mixto	Básico
USUARIOS WEB			Automático	Básico
LISTAS DE CORREO			Automático	Básico
EMPLEADOS			Mixto	Básico

También se incluyen los tratamientos detallados en el **ANEXO A.**

Como recursos protegidos de la Entidad se han tenido en cuenta los siguientes componentes:

- Ficheros automatizados / no automatizados
- Aplicaciones Informáticas con acceso a datos personales
- Soportes informáticos y papel
- Equipos de almacenamiento
- Equipos de tratamiento
- Comunicaciones y sistemas de acceso remoto
- Oficinas y edificios
- Sistemas de Validación
- Personas

2) FUNCIONES / OBLIGACIONES DEL PERSONAL

Todas las personas que tengan acceso a los ficheros protegidos, a través del sistema informático o a través de cualquier otro medio automatizado de acceso, están obligadas por ley a cumplir lo establecido en este documento, y por lo tanto, sujetas a las consecuencias que puedan derivar en caso de incumplimiento. El incumplimiento de las políticas, prácticas y procedimientos de seguridad estará sujeto a una acción disciplinaria, pudiendo conllevar una acción civil y/o penal.

Sin embargo, una eventual vulneración de la normativa de seguridad por parte de algún usuario, no eximirá de responsabilidad al Responsable del Fichero, sin perjuicio de las acciones que pueda éste ejercitar contra dicho usuario por el incumplimiento de sus obligaciones con respecto al mismo.

Las medidas de índole organizativas afectan en primera instancia a la actividad propia de la organización y a la asignación de funciones relacionadas con la seguridad. Por tanto, el responsable del fichero debe asegurar la implantación de las medidas técnicas y organizativas en sus sistemas de información y delimitar el acceso a los datos de carácter personal mediante la asignación de perfiles entre su personal. Dicha división conlleva a su vez una imposición de responsabilidades directamente relacionadas con la función a desempeñar dentro de la entidad. Los perfiles son básicamente los siguientes:

• **Responsable del fichero:** persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento de los ficheros con datos de carácter personal.

• **Responsable/s de seguridad:** persona o personas físicas, designadas por el responsable del fichero, con la misión de coordinar y controlar las medidas de seguridad aplicables. Aunque esta figura no es obligatoria para aquellos ficheros donde apliquen medidas de nivel básico, es muy recomendable como elemento clave para garantizar el cumplimiento de las medidas de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero o del tratamiento.

Las funciones principales del Responsable de Seguridad respecto el Documento serán:

- Coordinar la actualización del documento.
- Coordinar y controlar la implantación y aplicación de las medidas definidas en el Documento de Seguridad.
- Poner en conocimiento de los usuarios de los datos las medidas y procedimientos de seguridad que les afectan.
- Realizar controles periódicos para verificar el cumplimiento de las medidas.
- Analizar los informes de auditoría y elevar las conclusiones al responsable adecuado.

• **Administrador/es de Sistemas:** personas físicas encargadas de implantar y mantener las medidas técnicas de seguridad, una vez autorizadas por el responsable de seguridad.

• **Usuarios de los Ficheros:** Aquellos que, en ejercicio de sus funciones contractuales, tratan datos de carácter personal bajo el criterio de "necesidad de saber" establecido por el responsable del fichero o responsable de seguridad. Los usuarios, así como el resto de personal con acceso y tratamiento de datos de carácter personal, deberán conocer sus responsabilidades, siendo para ello necesario que se articulen mecanismos para garantizar un conocimiento comprensible de dichas normas. La relación de los diferentes usuarios con su perfil correspondiente se cita en el **ANEXO E (Nombramientos y Autorizaciones).**

En este Documento aparecen las normas que afectaran básicamente al Responsable de Seguridad y al Administrador de Sistemas pero es muy importante que los usuarios de los datos conozcan toda la normativa que les pueda afectar. Es por ello, que junto con el Documento de Seguridad formando parte del proyecto se entrega una normativa específica para usuarios donde figuran todas las normas referentes a la LOPD que afectan a todos los empleados que puedan tratar datos.

Esta normativa debe difundirse a todos los empleados ya sea entregándola en la incorporación de un empleado o publicándola en algún sitio público como la intranet o similar.

En la empresa, se procede a entregar la normativa en forma de recomendaciones a todo el personal implicado, a través del Documento (Usos y Recomendaciones) que se entregará a los diferentes perfiles de usuarios y responsables.

A los nuevos trabajadores se les haría entrega de la documentación, en el momento de la firma del contrato de trabajo.

3) MEDIDAS, NORMAS Y PROCEDIMIENTOS

En este apartado reflejamos todas las medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Reglamento derivado del RD 1720/2007.

Al margen del cumplimiento de esta normativa, el Responsable del Fichero deberá adoptar en cada momento aquellas medidas de índole técnica y organizativa que crea necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

Cabe decir que, si el cumplimiento estricto de alguna de las normas expuestas supusiera un coste desproporcionado para el Responsable del Fichero, éste podrá modular su cumplimiento, sin que en ningún caso pueda verse afectada la protección de datos de carácter personal.

FICHEROS AUTOMATIZADOS

Control de Acceso

El control de acceso es aquella medida destinada a garantizar la identidad de cada persona que accede a los sistemas de información (identificación/autenticación), así como a asegurar que el acceso de cada usuario corresponda exclusivamente al perfil y permisos asignados por el responsable del fichero, con el objeto de evitar accesos no autorizados al sistema que contiene datos personales automatizados.

Sólo las personas relacionadas autorizadas podrán tener acceso a los ficheros nombrados en este documento.

Exclusivamente el personal responsable de sistemas podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable de fichero.

Deberá existir una relación actualizada de usuarios y sus correspondientes perfiles, así como los accesos autorizados para cada uno de ellos.

Las aplicaciones deberán estar hechas de tal forma que se garantice que los usuarios sólo tendrán acceso a los datos que precisen para el desarrollo de sus funciones. El administrador de sistemas establecerá mecanismos para evitar que un usuario pueda acceder a datos sin estar debidamente autorizado.

En caso de que exista personal ajeno al responsable del fichero que tenga acceso puntual a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal interno. Es recomendable crear cuentas de usuario específicas en los sistemas de información para este tipo de usuarios.

Identificación y autenticación

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

Será obligatorio establecer 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.

Si el mecanismo de autenticación se basa en contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Estas contraseñas se deberán almacenar de forma ininteligible y tendrán que cambiarse con una periodicidad no superior al año.

Si se tratan datos de **nivel medio**, además, se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

En el apartado 5 del Documento de Seguridad se dedica un apartado específico a este tema (Contraseñas y Copias de Seguridad).

Control de acceso físico

Las instalaciones donde se ubiquen los ficheros deberán contar con los medios mínimos de seguridad, que garanticen que los datos protegidos están a salvo de riesgos por incidencias fortuitas o intencionadas.

La estancia donde se ubiquen los servidores será objeto de especial protección, garantizándose en todo momento que están a salvo la disponibilidad, la integridad y confidencialidad de los datos.

El acceso a la ubicación donde se encuentra el Servidor, deberá estar restringido exclusivamente al personal autorizado, y a aquel que deba realizar labores de mantenimiento del mismo.

Registro de Accesos

De cada acceso que se produzca a archivos de **nivel alto** se deberán guardar como mínimo la siguiente información: identificación usuario, fecha y hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado. Si el acceso ha sido autorizado será preciso guardar la información que permita identificar el registro accedido.

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.

El periodo de conservación de esta información será, como mínimo, de dos años siendo el Responsable de Seguridad el encargado de controlar el acceso a los registros de acceso, examinando una vez al mes dicha información y realizando un informe al respecto con las revisiones realizadas y los problemas detectados.

En el caso de que el responsable del fichero fuese una persona física y que se garantizase que únicamente esta tiene acceso y trata con los datos personales, no sería necesaria la llevanza del control de acceso.

Telecomunicaciones

La transmisión de datos de carácter personal de nivel alto que se realicen a través de redes públicas o redes inalámbricas de comunicaciones electrónicas deberá realizarse cifrando dicha información o utilizando cualquier otro medio que garantice que la información no sea inteligible ni manipulada por terceros. Las medidas habituales consisten en la existencia de redes VPN (IPSEC o SSL) que garantizan la confidencialidad de la información transmitida normalmente mediante protocolos seguros, así como otras tecnologías para la securización de los accesos vía web a las aplicaciones de intranet o internet. Otras opciones consisten en el cifrado de origen a extremo llevado a cabo por los propios usuarios mediante el uso de software específico, certificados digitales, etc.

Puestos de trabajo

Los puestos de trabajo están bajo la responsabilidad de las personas autorizadas, que deberá garantizar que la información que puede mostrarse desde dicho puesto no podrá ser vista por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras y otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Configuración Aplicaciones

Los puestos de trabajo desde los que se tenga acceso a los ficheros tendrán una configuración fija en sus aplicaciones y sistemas operativos, que sólo podrá ser cambiada bajo la autorización del Administrador del sistema. Ningún usuario podrá instalar una aplicación sin autorización del Administrador del sistema, quien analizará si dicha aplicación puede perjudicar otras que traten datos de carácter personal.

Todos los ordenadores deberán tener instalados programas antivirus que deberán, asimismo, estar actualizados diariamente (a ser posible desde un servidor de firmas), para así garantizar la protección y detección inmediata de la entrada de virus informático en el sistema.

FICHEROS NO AUTOMATIZADOS O MANUALES

El RD. 1720/2007 ha establecido medidas específicas para la documentación en papel, de estas, encontramos tres medidas específicas para la documentación que contiene datos de nivel básico y que se complementan con otras cuatro medidas enumeradas establecidas únicamente para los datos de nivel alto en soporte no automatizado. En los ficheros de nivel medio se aplicarán las medidas generales, ya existentes en la normativa.

Pasamos a desglosar las medidas específicas de los soportes no automatizados, a continuación:

Procedimiento de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos deberán garantizar la correcta conservación de los mismos, 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 que no exista norma aplicable, el responsable del fichero establecerá los criterios y procedimientos de actuación que deban seguirse para el archivo.

Procedimiento para dispositivos de almacenamiento y acceso a la documentación

El responsable del fichero o, en su defecto, un tercero autorizado, deberá establecer mecanismos que obstaculicen la apertura de dispositivos o medios de almacenamiento. Asimismo, en caso de que la naturaleza de los mismos impida su aplicación, se deberían fijar medidas que impidan el acceso a personas no autorizadas al lugar de almacenamiento, en la medida de lo posible. Habitualmente, estos procedimientos podrán llevarse a cabo mediante la aplicación de controles de acceso físico (llaves, tarjetas de entrada, biometría, etc.).

Para la información especialmente protegida **(nivel alto)** se deberán implantar además las siguientes medidas:

- 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 cerradas con llave o dispositivos equivalentes. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a dichos documentos.

- Si no fuera posible cumplir con lo establecido en el párrafo anterior, el responsable adoptará las medidas alternativas que considere adecuadas.

Procedimiento de custodia de soportes

En los casos en los que la documentación no se encuentra en dispositivos debidamente protegidos sea con motivo de procesos de revisión, tramitación, previo o posterior a su archivo, el responsable a cargo de la misma deberá custodiarla impidiendo el acceso a terceros no autorizados.

Para ello, entre otras, se deberán tener en cuenta las siguientes recomendaciones:

- Se almacenará de forma protegida la información sensible en papel especialmente cuando se abandone el puesto de trabajo.
- Los puntos de correo, envío fax, fotocopiadoras, escáner, etc. Deberán estar protegidos para evitar un uso no autorizado.
- Se deben recoger inmediatamente los documentos impresos o enviados a una impresora, fotocopiadora o fax con datos de carácter personal.

Procedimiento de copia o reproducción de documentos

Para los datos especialmente protegidos, se indicarán, asimismo, las personas autorizadas para la realización de copias o reproducción de los mismos, además de garantizar la destrucción de dicha información para evitar así el acceso no autorizado o su recuperación posterior.

Para ello es fundamental dotar de dispositivos de destrucción de documentos a todas las personas con acceso a la documentación y autorizadas para ello.

Procedimiento de acceso a la documentación

Además de la obligación de restricción de accesos a la información contenida en soportes no automatizados por personal no autorizado, en el caso de acceso a la documentación con datos de nivel alto se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

Registraremos en el formulario habilitado para ello la: identificación del usuario, fecha y hora, fichero accedido, tipo de acceso y si ha sido autorizado o denegado. Si el acceso ha sido autorizado será preciso guardar la información que permita identificar el registro accedido, cambios realizados y con qué fin.

Mediante el **(Formulario para el Registro de accesos a los Ficheros o Documentos no Automatizados)** se facilita un modelo de registro de acceso para la documentación no automatizada.

Traslado de la documentación

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

4) GESTIÓN DE INCIDENCIAS

Se considerarán como incidencias de seguridad, entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal del responsable del fichero.

Asimismo el responsable del fichero intentará contemplar el sentido más amplio del concepto de incidencia, entendiendo por tal cualquier situación contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de los medios físicos y lógicos que pueda afectar a su disponibilidad y a la seguridad de la información que gestionan.

A continuación se presenta una lista de incidencias que serán inexcusablemente registradas. Esta lista no debe entenderse como limitativa, sino que podrá ser ampliada con cualquier otro tipo de incidencias que hubieran quedado omitidas:

Incidencias que afecten a la identificación y autenticación de los usuarios:
• Pérdida de confidencialidad de contraseñas.
• Asignación o modificación de derechos sobre herramientas de control de acceso y utilidades con accesos privilegiados.
• Períodos de desactivación de las herramientas de seguridad.

Incidencias que afecten a los derechos de acceso a los datos:
• Revisión de logs sobre intentos fallidos de accesos, accesos fuera de horas de oficina, etc.
• Comunicación de los usuarios de sospechas de que alguien ha suplantado su personalidad.
• Detección de puntos de acceso desatendidos y sin protección de pantalla activada.
• Detección de contraseñas escritas en los puestos de trabajo.
• Revisión de los informes de seguridad

Incidencias que afecten a la gestión de soportes:
• Comunicación de pérdida de soportes.
• Comunicación de localización de soportes en lugares inadecuados.
• Errores de contenido en soportes recibidos.

Incidencias que afecten a los procedimientos de copias de salvaguarda y recuperación:
• Errores en los procesos de realización de copias de salvaguarda.
• Recuperaciones de datos realizadas.

Cualquier otra de las observadas como consecuencia de la ejecución de los controles definidos para garantizar el cumplimiento de lo dispuesto en el Documento de Seguridad.

La aplicación del presente Procedimiento se establece para todas las Áreas del responsable del fichero, empleados y colaboradores externos.

Responsabilidades

El Responsable de Seguridad es el responsable de la redacción y mantenimiento de este procedimiento; así como de su custodia y archivo.

Todos los usuarios de la EMPRESA deben informar de cualquier incidencia producida en materia de seguridad.
El Responsable de Seguridad debe ocuparse del seguimiento de las incidencias en materia de seguridad.

Los usuarios de los sistemas de información, empleados y colaboradores externos, deben participar en la implantación y seguimiento de la política de seguridad, aceptando formalmente sus obligaciones.

Comunicación de Incidencias de Seguridad por Usuarios

Cualquier usuario que tenga conocimiento directa o indirectamente de cualquier incidencia de seguridad, actual o posible, lo comunicará con la mayor brevedad tal incidencia y las acciones que se hubiesen tomado de urgencia.

En este momento se procede a incluirse en el registro y, si afecta a la seguridad de los datos de carácter personal, marcarla como tal.

Registro y Distribución de las Incidencias

Con el fin de poder mantener un registro de incidencias que permita su mantenimiento y posterior tratamiento y análisis se centralizará la recepción de las mismas ante el Responsable de Seguridad.

En el caso de incidencias sobre procesos o aplicaciones se comunicarán directamente al Responsable informático, quien se ocupará de informar al Responsable de Seguridad sobre su resolución.

Registros

El registro de incidencias será mantenido en exclusiva por el Responsable de seguridad.
Se facilitará el acceso estrictamente a aquellos departamentos que lo necesiten, para su consulta o análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias.

El registro contendrá los siguientes campos:
• Tipo de incidencia.
• Momento en que se ha producido (en su defecto detección).
• Persona que la notifica.
• Quien la recibe.
• A quien se le notifica.
• Efectos causados por la misma.

En el caso en que se apliquen medidas de nivel medio o alto, además se deberá:

Cuando la acción de respuesta definida incluya recuperación de datos, se indicará el responsable de la recuperación, los datos restaurados y los datos que han sido necesarios grabar manualmente, así como la autorización por parte del responsable de seguridad.

Mediante el ANEXO F se facilitan los formularios que es necesario llevar a cabo para el registro de las incidencias. El conocimiento y la no-notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del Fichero por parte de ese usuario.

5) CONTRASEÑAS Y COPIAS DE SEGURIDAD

Autenticación

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales. Cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al administrador y subsanada en el menor plazo de tiempo posible. Este sistema de autenticación debe venir acompañado por una política de restricción de accesos, esto es, que exista una política en la empresa de controlar los accesos de información únicamente en lo estrictamente necesario al puesto de trabajo concreto y a las funciones que se deben desarrollar en él, siendo consecuente, que a mayor cargo y responsabilidad, mayor será el acceso que pueda obtenerse de la información del sistema, así como la restricción de acceso a la información por áreas o departamentos.

El sistema actual utilizado por el Responsable en el fichero en cuanto a la autenticación de las entradas en el sistema, es el que a continuación se describe:

En cuanto a las claves de acceso, el sistema operativo requiere usuario / contraseña para iniciar la sesión, éstas son dadas por el responsable de sistemas a los usuarios.

El procedimiento que se recomienda seguir para el cambio de contraseña entre los usuarios de EL RESPONSABLE DEL FICHERO es el siguiente:

1) Siempre que sea posible el sistema ha de pedir el cambio de contraseña no permitiendo volver a usar una contraseña ya utilizada anteriormente.

2) Si el punto 1 no es posible por limitaciones del sistema el administrador de sistemas pedirá personalmente a cada usuario la nueva contraseña. El usuario deberá comunicarla al administrador en un plazo máximo de 24 horas y esta comunicación se realizará por medios que garanticen la confidencialidad de la contraseña.

3) Una vez que el administrador de sistemas disponga de todas las contraseñas, validará que no sea una contraseña ya utilizada anteriormente. El administrador de sistemas cambiará la contraseña del usuario para todas las aplicaciones que la requieran junto con la contraseña del sistema operativo y red (recursos compartidos).

4) Se verificará que el cambio de las contraseñas se ha realizado correctamente.

5) Se comunicará a los usuarios el momento del cambio y cuando pueden empezar a utilizar la nuevas contraseñas haciendo hincapié en el tema de la confidencialidad. Para llevar a cabo correctamente este procedimiento será necesario disponer de una lista/fichero protegida/o con las aplicaciones y puntos del sistema informático que requieran contraseña.

A cada usuario del sistema informático de le será asignado un nombre de usuario, que asociado a una contraseña, lo identificará dentro de los sistemas de información y permitirá el acceso a las áreas relacionadas con su actividad profesional.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y solicitar el cambio al Responsable de Seguridad.

Cuando se incorpore un usuario nuevo el responsable de fichero se encargará de comunicarlo al departamento de sistemas para que se le dé de alta conforme a los permisos que le sean asignados. En esta alta se le asignará un nombre de usuario y una contraseña. No está permitida la divulgación de la clave por circunstancia alguna a otras personas integrantes de la plantilla o ajenas a la entidad.

Copias de Seguridad

La seguridad de los datos personales de los Ficheros no sólo supone la confidencialidad de los mismos, sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos de los ficheros con datos de carácter personal.

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.

Procedimiento de respaldo

Debe fijarse y definirse un proceso de copia total de todos los archivos del sistema a través de cualquier medio válido que asegure la recuperación. El Responsable de realizarlas es el Responsable de Copias de Seguridad o el responsable de sistemas, por un medio automatizado. Se aconseja, especialmente, la copia en disco externo para almacenarla fuera del servidor de la empresa.

Procedimiento de recuperación

Cuando se produzca una pérdida total o parcial de datos de cualquiera de los servidores se deberán tener en cuenta los siguientes puntos:

• Formalizar la autorización por escrito del responsable de seguridad para la ejecución de los procedimientos de recuperación.

• Dejar constancia en el libro de incidencias de las manipulaciones que hayan debido realizarse para dichas recuperaciones rellenando el formulario con todos los datos requeridos.

• La recuperación deberá realizarse partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia que permita reconstruir los datos del fichero al estado en que se encontraban antes del momento del fallo o pérdida.

Soportes para los respaldos

Los soportes de las copias de seguridad se podrán reciclar. Aún así, si alguno dejará de ser fiable para su funcionamiento, deberá ser destruido físicamente de forma que sea imposible la recuperación de los datos. Antes de reciclar cualquier soporte el personal autorizado para realizar las copias deberá verificar si es o no óptimo para su funcionamiento. Se designará por el Responsable de Seguridad un recinto donde se guardarán los soportes de las copias de seguridad, que se mantendrá constantemente cerrado con llave y protegido.

Para datos de nivel alto, deberá conservarse una copia de seguridad en un lugar diferente a aquel que se encuentren los equipos que tratan los datos o utilizar elementos que garanticen la integridad y recuperación de la información. Aunque esta medida solo afecta a ficheros que contengan datos de nivel alto es altamente recomendable para todo tipo de ficheros.

6) GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes informáticos son todos aquellos medios físicos susceptibles de ser tratados en los sistemas de información, y sobre los que se pueden grabar y recuperar datos (equipos, discos, cintas, CD, DVD, etc.). El control de estos medios tiene una importancia fundamental, dada la facilidad para su transporte y reproducción.

Inventario

Los soportes o documentos que contengan datos de carácter personal deben estar claramente identificados con una etiqueta externa que permita identificar a través de algún identificador que tipo de datos contienen (salvo que las características físicas del soporte o documento lo impidan).

Dicho sistema debe permitir mantener un inventario de los soportes, donde se pueda registrar otra información adicional, como fecha de creación, fecha de baja, motivo de la baja, etc.

La identificación de los soportes para información especialmente sensible puede establecerse mediante una codificación que dificulte la identificación para usuarios no autorizados. Los soportes o documentos que contengan datos de carácter personal deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para acceder al fichero.

Autorización salida o entrada de soportes

La salida de datos de carácter personal pertenecientes a los ficheros definidos en el presente documento, sea cual sea el medio utilizado (incluye los comprendidos y/o anexos a un correo electrónico), sólo estará permitida cuando sea necesario para el desempeño de las funciones propias de la sociedad, y cuando así lo autorice el Responsable del Fichero garantizándose en todo momento el nivel de seguridad correspondiente al tipo de fichero tratado.

En todo caso, la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales deberá ser autorizada por el responsable del fichero y registrada mediante el ANEXO G.3 (Salida de Soportes).

Los soportes o documentos que deban salir de las ubicaciones habituales deberán ser transportados con la debida protección frente a robos, sustracciones o accesos no autorizados, teniendo en cuenta la sensibilidad de la información.

En caso de tratarse de datos de nivel alto el transporte se realizará de forma codificada o mediante otros mecanismos similares que puedan garantizar su protección durante su salida de la ubicación habitual.

La tecnología de cifrado también es aplicable a los documentos como correo electrónico o equipos portátiles cuando se empleen fuera de las instalaciones.

Registro salida o entrada de soportes

Además de la autorización mencionada cuando se produzca la salida o entrada de soportes o documentos que contengan datos de carácter personal de nivel medio fuera de los locales o hacia donde está ubicado el fichero deberá registrarse expresamente mediante el ANEXO G.3 (Salida de Soportes) y el ANEXO G.4 (Entrada de Soportes).

Este registro deberá contener el tipo de documentos o soportes, 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 o entrega.

Si la salida de dichos soportes o documentos fuera periódica como el caso de portátil, PDA, etc. podrá hacerse un registro/autorización genérico especificándolo en la hoja de registro. El movimiento de soportes entre departamentos no se considerará a estos efectos.

Reutilización o desechado de soportes

Cuando un soporte que contenga datos de carácter personal vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario en caso que no se sustituya por otro soporte destinado a la misma función.

Entrada y Salida de Datos por Red

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merece un tratamiento especial ya que, por sus características, puede ser más vulnerable que los soportes físicos tradicionales.

El envío de datos de los ficheros protegidos por correo electrónico sólo se realizará cuando sea necesario para el desempeño de las funciones propias de la Sociedad. En todo caso, el usuario que realice o pretenda realizar el envío de los datos deberá ser un usuario autorizado en el ANEXO E (Personal Autorizado), para el tratamiento de ese concreto fichero al que pertenezcan los datos.

La obligación de dicho usuario será la de asegurarse de que la entrega o envío de esa información es legítima en virtud de lo establecido en la presente normativa aplicable y en el presente Documento de Seguridad.

El envío de información entre personal interno o entre departamentos, no se considerará entrada y salida de datos a los efectos de la presente normativa.

7) FICHEROS NOTA

Los ficheros detectados deben inscribirse en el Registro General de la Agencia de Protección de Datos, a través de la opción "Ficheros" de la aplicación.

La notificación de la inscripción, junto a la asignación del número de registro, tarda aproximadamente 5 semanas desde su envío, y la publicación en la web de la Agencia, www.agpd.es – apartado: Ficheros Inscritos, algunas semanas más.

En el Anexo A, además, será necesario hacer una descripción de los ficheros según el contenido con el que se hayan declarado. Esto es: denominación del Fichero, contenido, finalidad, nivel de seguridad de los datos, encargados de tratamiento, de haberlos y tipo de tratamiento efectuado.

Además de las aplicaciones mencionadas de cada fichero podrán existir ficheros ofimáticos autónomos derivados de las aplicaciones o bases de datos principales, esto, únicamente, supone un cambio en el sistema del tratamiento, pero no es una modificación susceptible de notificación en la Agencia. No obstante, debemos tener en cuenta que los ficheros deben estar actualizados, es decir, si hay ficheros que desaparecen, otros que se crean, o algunos que pasan a ampliar su finalidad o bien dejan de ser únicamente documentales para ser automatizados, serán variaciones que haya que inscribir en el Registro General de Protección de datos.

En el apartado nº 14 AEPD, del documento de seguridad, se establece que deben quedar archivados y ordenados las notificaciones de la Agencia cuando las hayamos recibido, así como los posibles cambios que vayan a darse en el Documento de Seguridad con incidencia en la declaración de ficheros, como podría ser la declaración de ficheros nuevos, las modificaciones de datos de las primeras declaraciones o la supresión de ficheros por dejar de responder al fin para el que fueron creados.

8) CONTROLES PERIÓDICOS / AUDITORÍAS

El responsable de seguridad llevará a cabo controles periódicos que verifiquen el cumplimiento de las normas establecidas en el reglamento de medidas de seguridad, así como controlar que documentalmente las modificaciones estén actualizadas: nuevos trabajadores que firman el documento de autorización del consentimiento, contratos con los posibles nuevos encargados del tratamiento, rutinas de registros, incidencias, entradas y salidas, etc.

A partir de los datos de nivel medio (aunque muy recomendable también en nivel básico) 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 de las normas establecidas en el reglamento.

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 objeto de verificar la adaptación, adecuación y eficacia de las mismas.

Esta auditoría extraordinaria reiniciará el cómputo de los dos años. Los informes de auditoría serán analizados por el responsable de seguridad competente que elevará las conclusiones al responsable de fichero o tratamiento para que adopte las medidas correctoras adecuadas.

9) ENCARGADOS DE TRATAMIENTO

El Reglamento establece que cuando exista un tratamiento de datos por cuenta de terceros, ya sea de forma parcial o de modo exclusivo, el documento de seguridad deberá contener la identificación de dichos ficheros así como la referencia al contrato que regula las condiciones del encargo.

Esta exigencia se cumple a través de los modelos de contrato de encargo de tratamiento que se facilitan a través de la implantación, ya que mediante la auto cumplimentación de datos, cada uno de los contratos de encargo de tratamiento identificarán además de la empresa con la que se ha contratado los servicios que llevan implícita la comunicación y cesión de datos, es decir, la identificación del Encargo de Tratamiento, así como el resto de información a la que viene referida el artículo 12.2 de la LOPD, se señalarán qué ficheros quedan sujetos a las cesiones o accesos de datos que deba realizar el Encargado de tratamiento para poder prestar el servicio contratado.

Esta identificación, se realizará mediante el Apartado del menú principal **"ENCARGADOS Y CONTRATOS"**.

En un régimen diferente, ya que no se produce un tratamiento de los datos, según se entiende en la Ley de Protección de datos, pero para salvaguardar el posible acceso y conocimiento de datos de carácter personal titularidad del Responsable del fichero, encontramos terceras personas, que por la naturaleza de sus servicios (mantenimiento, mensajería y auxiliar-administrativos) tienen acceso a determinada información del centro, convirtiéndose en cesionarios de la empresa. Normalmente, son autónomos colaboradores y prestadores de algún servicio profesional que acceden a la base de datos del Responsable del Fichero, por lo que se hace necesario firmar el oportuno documento de acceso de datos y confidencialidad.

10) TRATAMIENTO DE FICHEROS, SISTEMAS Y SOPORTES

Sistema informático: Servidores, equipos y software

La relación de servidores de EL RESPONSABLE DEL FICHERO, así como su sistema operativo, características físicas, finalidad y ubicación queda registrada en el ANEXO B (Estructura Informática y Equipamiento), así como la descripción de la red o redes del sistema de tratamiento de información, y el inventario y descripción de los equipos de Sobremesa o Portátiles, Agendas Electrónicas, Pen Drives, Impresoras, Faxes, Fotocopiadoras y cualquier otro soporte automatizado que valga para el almacenamiento y tratamiento de datos.

Se advierte, igualmente, que lo adecuado sería mantener el servidor o servidores de datos en un rack con restricción de acceso y debidamente climatizado.

Asimismo, debería instalarse un SAI para los servidores para prevenir cualquier incidencia de pérdida de datos en caso de problemas con el suministro eléctrico.

En el ANEXO C (Programas y aplicaciones), se enumerarán los programas de gestión utilizados en la empresa para el tratamiento de datos de carácter personal.

Acceso a locales con ficheros documentales

El acceso a las instalaciones donde se almacenen archivos documentales deberá estar restringido a fin de evitar que el personal no autorizado acceda a la información.

La restricción puede ser física, colocando armarios cerrados con llave o despachos que unifican archivos y que permanecen cerrados, o bien que exista personal de recepción o seguridad que no permita el paso a nadie externo sin estar acompañado de personal autorizado.

Hay empresas que optan por la llevanza de un registro de entrada del personal externo y dotan al personal interno autorizado a consultar la información contenida en los archivos documentales de formas de entrada, ya sean llaves enumeradas y registradas, tarjetas identificativas, identificadores de huellas, de DNI para poder entrar en las estancias restringidas, etc.

Para mayor seguridad, las instalaciones deberán estar dotadas de alarmas contra robo y sistemas detectores de humo para la detección de incendios.

Los sitios donde hay datos de carácter personal pertenecientes a los diferentes ficheros que hemos mencionado, se enumerarán y describirán en el ANEXO D (Descripción de los locales).

4) ANEXOS

1. Anexo A
Descripción de los ficheros, tratamientos y relación de encargados de tratamiento.
2. Anexo B
Descripción de la estructura del sistema informático.
3. Anexo C
Programas y aplicaciones que tratan los ficheros.
4. Anexo D
Locales: Sede principal y delegaciones.
5. Anexo E
Nombramientos y autorizaciones:
 1. Lista de responsables.
 2. Lista de autorizaciones.
6. Anexo F
Procedimiento de Notificación y gestión de incidencias. (Plantillas notificaciones de incidencias.)
7. Anexo G
Procedimientos de control y seguridad:
G.1. Procedimiento de respaldo y recuperación.
G.2. Procedimiento de gestión de soportes y registro de copias realizadas.
G.3. Procedimiento de gestión de salida de soportes.
G.4. Procedimiento de gestión de entrada de soportes.
G.5. Autorización para el uso de ordenadores portátiles y trabajo fuera de locales.
G.6. Política de acceso a datos automatizados.

ANEXO A Descripción de los Ficheros y los tratamientos de la empresa

Este anexo contiene una ficha con la descripción de los ficheros y tratamientos de la empresa.

ANEXO A Descripción de los ficheros automatizados y NO automatizados

NOMBRE DEL FICHERO: CLIENTES/PROVEEDORES

Nivel de seguridad: Básico

Responsable del fichero: ALBERTO RODRIGUEZ PALOMINO
Fecha de inscripción o modificación:

Encargado del tratamiento: JAVIER RODRIGUEZ SANTOS Av. de América, 56 - 28028 Madrid Nif: 50804718H Telf: Fax: e-mail:

Responsable de atención a los afectados (derechos ARCO):
ALBERTO RODRIGUEZ PALOMINO C/ CEA BERMUDEZ 14, 5º-5 - 28003 MADRID Nif: 51126442H

Finalidad y usos previstos del fichero: Gestión de clientes, contable, fiscal y administrativa.
Descripción de la finalidad: FICHERO PARA LA GESTION ADMINISTRATIVA Y COMERCIAL DE LA CARTERA DE CLIENTES DE LA EMPRESA

Origen y procedencia de los datos del fichero: Propio interesado o representante legal.

Colectivos de interesados: Clientes y usuarios, Proveedores.

Datos identificativos que contiene el fichero: Cif/nif. Nombre y apellidos. Dirección postal o electrónica. Teléfono. Firma manual, manuscrita o digitalizada.
Otros datos identificativos: Nº colegiado.
Otros tipos de datos tipificados: Económicos, financieros y de seguros.

Sistema de tratamiento: Mixto

Destinatarios de cesiones de datos: Administración tributaria, Bancos, cajas de ahorros y cajas rurales.

Procedimiento utilizado en la recogida de datos: El interesado los entrega personalmente y se introducen en el fichero al momento.

Medidas de seguridad para restringir el acceso a los ficheros No automatizados o soporte papel:
Archivadores ubicados en una oficina con acceso restringido.

Procedimiento de respaldo y recuperación:
La descripción detallada de las copias de respaldo y de los procedimientos de recuperación se encuentra en el **Anexo G.1 Procedimiento de respaldo y recuperación.**

ANEXO A Descripción de los ficheros automatizados y NO automatizados

NOMBRE DEL FICHERO: USUARIOS WEB

Nivel de seguridad: Básico

Responsable del fichero: ALBERTO RODRIGUEZ PALOMINO
Fecha de inscripción o modificación:

Encargado del tratamiento: SOFTWARE DEL SOL, S.A. Geolit Parque Científico y Tecnológico - 23620 Mengíbar Nif: B60260452 Telf: Fax: e-mail:

Responsable de atención a los afectados (derechos ARCO):
ALBERTO RODRIGUEZ PALOMINO C/ CEA BERMUDEZ 14, 5º-5 - 28003 MADRID Nif: 51126442H

Finalidad y usos previstos del fichero: Gestión de clientes, contable, fiscal y administrativa. Publicidad y prospección comercial.
Descripción de la finalidad: FICHERO PARA LA GESTIÓN COMERCIAL, REALIZAR ACCIONES DE MARKETING OFERTAS Y PUBLICIDAD DE LOS PRODUCTOS Y SERVICIOS DE LA EMPRESA.

Origen y procedencia de los datos del fichero: Propio interesado o representante legal.

Colectivos de interesados: Clientes y usuarios, Personas de contacto.

Datos identificativos que contiene el fichero: Nombre y apellidos. Dirección postal o electrónica. Teléfono.

Sistema de tratamiento: Automático

Procedimiento utilizado en la recogida de datos: El interesado rellena un formulario electrónico en la web de la empresa.

Procedimiento de respaldo y recuperación:
La descripción detallada de las copias de respaldo y de los procedimientos de recuperación se encuentra en el **Anexo G.1 Procedimiento de respaldo y recuperación.**

ANEXO A Descripción de los ficheros automatizados y NO automatizados

NOMBRE DEL FICHERO: LISTAS DE CORREO

Nivel de seguridad: Básico

Responsable del fichero: ALBERTO RODRIGUEZ PALOMINO
Fecha de inscripción o modificación:

Encargado del tratamiento: (véase el apartado Contratos)

Responsable de atención a los afectados (derechos ARCO):
ALBERTO RODRIGUEZ PALOMINO C/ CEA BERMUDEZ 14, 5º-5 - 28003 MADRID Nif: 51126442H

Finalidad y usos previstos del fichero: Publicidad y prospección comercial.
Descripción de la finalidad: FICHERO PARA REALIZAR ACCIONES DE MARKETING OFERTAS Y PUBLICIDAD DE LOS PRODUCTOS Y SERVICIOS DE LA EMPRESA.

Origen y procedencia de los datos del fichero: Propio interesado o representante legal.

Colectivos de interesados: Clientes y usuarios, Personas de contacto.

Datos identificativos que contiene el fichero: Nombre y apellidos. Dirección postal o electrónica.

Sistema de tratamiento: Automático

Procedimiento utilizado en la recogida de datos: El interesado los envía al email de contacto de la empresa. El interesado rellena un formulario electrónico en la web de la empresa.

Procedimiento de respaldo y recuperación:
La descripción detallada de las copias de respaldo y de los procedimientos de recuperación se encuentra en el **Anexo G.1 Procedimiento de respaldo y recuperación.**

ANEXO A Descripción de los ficheros automatizados y NO automatizados

NOMBRE DEL FICHERO: EMPLEADOS

Nivel de seguridad: Básico

Responsable del fichero: ALBERTO RODRIGUEZ PALOMINO
Fecha de inscripción o modificación:

Encargado del tratamiento: (véase el apartado Contratos)

Responsable de atención a los afectados (derechos ARCO):
ALBERTO RODRIGUEZ PALOMINO C/ CEA BERMUDEZ 14, 5º-5 - 28003 MADRID Nif: 51126442H

Finalidad y usos previstos del fichero: Recursos humanos. Gestión de nóminas.
Descripción de la finalidad: FICHERO PARA LA CONFECCION DE NOMINAS Y GESTION LABORAL DE LOS TRABAJADORES DE LA EMPRESA

Origen y procedencia de los datos del fichero: Propio interesado o representante legal.

Colectivos de interesados: Empleados.

Datos identificativos que contiene el fichero: Cif/nif. Nº de la seguridad social. Nombre y apellidos. Dirección postal o electrónica. Teléfono. Imagen / voz.
Otros tipos de datos tipificados: Académicos y profesionales. Detalles del empleo. Económicos, financieros y de seguros.

Sistema de tratamiento: Mixto

Destinatarios de cesiones de datos: Organismos de la seguridad social, Administración tributaria, Bancos, cajas de ahorros y cajas rurales.

Procedimiento utilizado en la recogida de datos: El interesado los entrega personalmente y se introducen en el fichero al momento.

Medidas de seguridad para restringir el acceso a los ficheros No automatizados o soporte papel:
Archivadores ubicados en una oficina con acceso restringido.

Procedimiento de respaldo y recuperación:
La descripción detallada de las copias de respaldo y de los procedimientos de recuperación se encuentra en el **Anexo G.1 Procedimiento de respaldo y recuperación.**

Encargados del tratamiento

Listado de encargados del tratamiento

Relación de empresas que prestan algún servicio al responsable del fichero, y dicho servicio implica tratamiento de datos personales.

Encargado con acceso	código: 1

Nombre del encargado: JAVIER RODRIGUEZ SANTOS **Nif:** 50804718H
Dirección: Av. de América, 56
CP: 28028 **Localidad:** Madrid
Servicios prestados:
Otros servicios prestados: Asesor fiscal y contable
Fecha del contrato: 6 de noviembre del 2017

Encargado con acceso	código: 2

Nombre del encargado: INTERNACIONAL VENTUR, S.A. **Nif:** A12093357
Dirección: Calle Luxemburgo, 75
CP: 12006 **Localidad:** Castellón de la Plana
Servicios prestados:
Otros servicios prestados: Proveedor productos dentales
Fecha del contrato: 6 de noviembre del 2017

Encargado con acceso	código: 3

Nombre del encargado: AMERICAN M Y D, S.L. **Nif:** B60260452
Dirección: Plaza de Francesc Macià, 8
CP: 08029 **Localidad:** Barcelona
Servicios prestados:
Otros servicios prestados: Proveedor productos medicos y dentales
Fecha del contrato: 6 de noviembre del 2017

Encargado con acceso	código: 4

Nombre del encargado: ASESORIA DE CONSUMO Y SANIDAD, S.L. **Nif:** B91985978
Dirección: Calle Imagen 7 - 5º derecha
CP: 41003 **Localidad:** Sevilla
Servicios prestados:
Otros servicios prestados: Tecnico garante
Fecha del contrato: 6 de noviembre del 2017

Encargado con acceso	código: 5

Nombre del encargado: SOFTWARE DEL SOL, S.A. **Nif:** B60260452
Dirección: Geolit Parque Científico y Tecnológico
CP: 23620 **Localidad:** Mengíbar
Servicios prestados:
Otros servicios prestados: Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servicios en la Nube)
Fecha del contrato: 6 de noviembre del 2017

Encargado con acceso	código: 6

Nombre del encargado: AGENCIA SERVICIOS MENSAJERIA, S.A. **Nif:** A61441523
Dirección: Avda. Fuentemar, 18
CP: 28823 **Localidad:** Coslada
Servicios prestados:
Otros servicios prestados: Empresa de mensajería
Fecha del contrato: 7 de noviembre del 2017

Encargados sin acceso a datos

No existen datos para este anexo o documento.

Relación de empresas que prestan algún servicio al responsable del fichero, y dicho servicio NO implica tratamiento de datos personales.

ANEXO B Estructura informática

Este anexo contiene la descripción de la estructura del sistema informático, el tipo de red, el entorno de las comunicaciones y certificados digitales.

Estructura informática	Código: 1

Página web: www.alpadental.es
Descripción de la estructura informática: UN ORDENADOR DE SOBREMESA
Esta estructura pertenece al local o locales: OFICINA

ANEXO B Equipamiento

Inventario de los equipos informáticos que posee la empresa.

Características del equipo/s	código: 1

Tipo equipo: Ordenador de sobremesa **Cantidad:** 1
Descripción: MEDION
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS,
Usuarios o perfiles que lo utilizan: ALBERTO RODRIGUEZ PALOMINO,
Local donde se encuentra este equipo: OFICINA,
Sistema operativo: WINDOWS 10
Antivirus: WINDOWS DEFENDER
Fecha de alta: 06/11/2017 **Fecha de baja:**

ANEXO C Programas y aplicaciones que tratan los ficheros

Este anexo contiene los programas Ofimáticos, Gestores de Facturación, Contabilidad, etc.. que traten datos personales de los ficheros.

Programa / Aplicación	código: 1

Nombre: OFFICE 365
Cantidad: 1 **Nivel de seguridad:** BASICO
Finalidad y descripción: OFIMATICA
Ficheros o Tratamientos que trata: CLIENTES/PROVEEDORES, USUARIOS WEB, EMPLEADOS
Usuarios que lo ejecutan: ALBERTO RODRIGUEZ PALOMINO
Equipos donde se ejecuta: Ordenador de sobremesa (MEDION)
Registro de accesos: NO
Fecha de alta: 06/11/2017 **Fecha de baja:**

Programa / Aplicación	código: 2

Nombre: MOZILLA THUNDERBIRD
Cantidad: 1 **Nivel de seguridad:** BASICO
Finalidad y descripción: CORREO
Ficheros o Tratamientos que trata: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS
Usuarios que lo ejecutan: ALBERTO RODRIGUEZ PALOMINO
Equipos donde se ejecuta: Ordenador de sobremesa (MEDION)
Registro de accesos: NO
Fecha de alta: 06/11/2017 **Fecha de baja:**

Programa / Aplicación	código: 3

Nombre: DELSOL 360
Cantidad: 1 **Nivel de seguridad:** BASICO
Finalidad y descripción: CONTABILIDAD
Ficheros o Tratamientos que trata: CLIENTES/PROVEEDORES, EMPLEADOS
Usuarios que lo ejecutan: ALBERTO RODRIGUEZ PALOMINO
Equipos donde se ejecuta: Ordenador de sobremesa (MEDION)
Registro de accesos: NO
Fecha de alta: 06/11/2017 **Fecha de baja:**

ANEXO D Locales donde se ubican los ficheros

Este anexo contiene una relación de los locales donde se ubican los ficheros.

Local	código: 1
Nombre del local: OFICINA **Dirección completa del local:** C/ CEA BERMUDEZ 14, 5º - 5 – 28003 MADRID (MADRID) **Descripción física del local:** OFICINA **Control de acceso:** Personal de la empresa autorizado con llave de la entrada principal **Sistemas de seguridad:** **Ficheros o Tratamientos:** CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS	

Observaciones:

ANEXO E Nombramientos

Este anexo contiene una relación de los diferentes responsables en materia de protección de datos, todos ellos nombrados o autorizados por el Responsable del Fichero: ALBERTO RODRIGUEZ PALOMINO.

Nombramiento	código: 1

Administrador
Nombre y Apellidos: ALBERTO RODRIGUEZ PALOMINO
Dni: 51126442H
Cargo/función en la empresa: Persona designada para conceder, alterar, o anular el acceso autorizado a los datos.
Fecha de Alta: 06/11/2017
Fecha de Baja:
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS

Fdo. Responsable del fichero: **Fdo. Administrador:**

Nombramiento	código: 2

Responsable de seguridad

El responsable de los ficheros ha nombrado en fecha 06/11/2017 a **ALBERTO RODRIGUEZ PALOMINO** con DNI 51126442H como Responsable de Seguridad, asumiendo las funciones y obligaciones contempladas en el Documento de Seguridad. Por la presente declara haber recibido el Documento de Seguridad y haber sido formado e informado de las obligaciones que como tal le corresponden. El incumplimiento por parte del mismo de las obligaciones establecidas en este documento será considerado como falta grave, imponiéndose las sanciones previstas para este tipo de faltas, especificadas en la normativa laboral o funcionarial de aplicación al responsable del fichero. En ningún caso, esta delegación exonera al Responsable del Fichero de su responsabilidad única y final, contemplada en el RLOPD y Ley Orgánica de Protección de Datos 13/1999. Este nombramiento tiene una validez de 4 años, pasados los cuales deberá realizarse uno nuevo.
Ficheros o tratamientos afectados por el nombramiento: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS

Fdo. Responsable del fichero: **Fdo. Responsable de seguridad:**

Nombramiento	código: 3

Responsable de copias de respaldo y recuperación
Nombre y Apellidos: ALBERTO RODRIGUEZ PALOMINO
Dni: 51126442H
Cargo/función en la empresa:
Fecha de Alta: 06/11/2017
Fecha de Baja:
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS

Fdo. Responsable del fichero: **Fdo. Responsable de copias de respaldo y recuperación:**

Nombramiento	código: 4

Responsable de la gestión de incidencias
Nombre y Apellidos: ALBERTO RODRIGUEZ PALOMINO
Dni: 51126442H
Cargo/función en la empresa:
Fecha de Alta: 06/11/2017
Fecha de Baja:
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS

Fdo. Responsable del fichero: **Fdo. Responsable de la gestión de incidencias:**

Nombramiento	código: 5

Responsable de atención a los afectados
Nombre y Apellidos: ALBERTO RODRIGUEZ PALOMINO
Dni: 51126442H
Cargo/función en la empresa:
Fecha de Alta: 06/11/2017
Fecha de Baja:
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS

Fdo. Responsable del fichero: **Fdo. Responsable de atención a los afectados:**

ANEXO E Autorizaciones con acceso

Lista de usuarios o trabajadores de la empresa con acceso a los datos.

Usuario con acceso	código: 1

Nombre y Apellidos: ALBERTO RODRIGUEZ PALOMINO **Dni:**
Funciones o tipo de usuario: ADMINISTRADOR
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS
Locales donde se ubica: OFICINA
Fecha de alta: 06/11/2017 **Fecha de baja:**

Usuario con acceso	código: 2

Nombre y Apellidos: MATILDE PALOMINO PAZ **Dni:**
Funciones o tipo de usuario: COMERCIAL
Ficheros o Tratamientos que utiliza: CLIENTES/PROVEEDORES
Locales donde se ubica: OFICINA
Fecha de alta: 06/11/2017 **Fecha de baja:**

ANEXO E **No existen datos para este anexo o documento.**

Lista de usuarios o trabajadores de la empresa sin acceso a los datos.

ANEXO F Notificación y gestión de incidencias

Cuando se produzca una incidencia, el usuario o el administrador deberán comunicarla al Responsable de seguridad o al Responsable del fichero o superior inmediato. Para ello emplearán el formulario aquí detallado. Una vez recibida la notificación el responsable correspondiente procederá a su registro y análisis, debiendo tomar las medidas correctoras necesarias. En ficheros de nivel medio y alto el responsable del fichero debe autorizar previamente las posibles recuperaciones de datos.

Se mantendrán las incidencias registradas de los 12 últimos meses.

ANEXO F Registro automatizado de Incidencias

No existen datos para este documento.

ANEXO F Notificación y gestión manual de incidencias

Incidencia Nº: (Este número será rellenado por el Responsable de seguridad)
Fecha de notificación:
Tipo de incidencia:
Descripción detallada de la incidencia:
Fecha y hora en que se produjo la incidencia:

Efectos que puede producir:
Medidas correctoras aplicadas:
Recuperación de Datos : (A rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente:
Nombre del Responsable: Persona que ejecutó el proceso: Firma:

El responsable autoriza las recuperaciones de datos mediante la firma de este formulario.

Nombre de la persona que realiza la notificación: Firma:	Persona a quién se comunica:

ANEXO G.1 Procedimiento de respaldo y recuperación

Este anexo contiene la descripción del sistema de copias de seguridad y recuperación, así como la frecuencia.

Respaldo y recuperación	código: 1

Descripción del sistema de copias: PROGRAMA DE COPIAS DE WINDOWS
Descripción del sistema de recuperación:
Frecuencia de las copias: Mensual
Ficheros o Tratamientos: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS
Observaciones:

ANEXO G.2 Relación de los soportes utilizados por la empresa que contienen ficheros.

Inventario de soportes utilizados por la empresa que contienen ficheros de datos personales.

Soporte	código: 1

Referencia del soporte: B01
Tipo del soporte: Disco duro externo
Fecha de alta: 06/11/2017
Lugar de acceso restringido donde se deposita el soporte: EN LA OFICINA
Ficheros o Tratamientos que contiene: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS
Locales donde se encuentra: OFICINA,

Ref:
B01
Soporte:
Disco duro externo

ANEXO G.2 Registro de copias realizadas

En este apartado se archivan los registros de las copias de seguridad realizadas.

En el caso de reutilización o eliminación de soportes grabados con datos del fichero se utilizará una aplicación informática para el borrado y formateo físico de los datos.

Para ficheros de nivel Medio y nivel Alto:

Los sistemas de etiquetado permitirán la identificación de soportes a los usuarios, pero dificultará la identificación de los mismos, al resto de las personas.

ANEXO G.2 Formulario para el registro manual de las copias realizadas

Ref. Soporte	Fecha copia	Ficheros o Tratamientos contenidos	Responsable	Resultado de la copia

ANEXO G.3 Procedimiento de gestión de salida de soportes

Este apartado es obligatorio a partir de ficheros de nivel medio, pero igualmente se puede utilizar en nivel básico para obtener una implantación LOPD de mayor calidad.

Cualquier salida de soportes fuera de los locales donde está ubicado el fichero deberá ser autorizada por el responsable del fichero de acuerdo al documento adjunto.

El responsable del fichero mantendrá un Libro en el que registrará las salidas de soportes, cuyos asientos estarán constituidos por los documentos de autorización de salida debidamente cumplimentados. La persona responsable de la entrega de soportes estará debidamente autorizada por el responsable del fichero.

ANEXO G3 Registros automatizados de salidas de soportes

No existen datos para este documento.

ANEXO G.3 Gestión manual de salida de soportes

Fecha y Hora de Salida:	**Referencia del soporte:**
Tipo de información que contiene:	**Tipo de soporte (documento, disco, etc..):**
Datos del destinatario:	**Cantidad de soportes incluidos en el envío:**
Medio de transporte utilizado:	**Medidas de seguridad adoptadas para su transporte:**
Responsable que autoriza la persona que realiza la entrega. **Nombre:** **Firma:**	**Persona que realiza la entrega del soporte.** **Nombre:** **Firma:**

ANEXO G.4 Procedimiento de gestión de entrada de soportes

Este apartado es obligatorio a partir de ficheros de nivel medio, pero igualmente se puede utilizar en nivel básico para obtener una implantación LOPD de mayor calidad.

El responsable del fichero mantendrá un Libro en el que registrará las entradas de soportes cuyos asientos estarán constituidos por los datos recogidos en el formulario que se adjunta.

La persona responsable de la recepción de soportes estará debidamente autorizada por el responsable del fichero.

ANEXO G.4 Registros automatizados de entradas de soportes

No existen datos para este documento.

ANEXO G.4 Gestión manual de entrada de soportes

Fecha y Hora de Entrada:	**Referencia del soporte:**
Ficheros que contiene:	**Tipo de soporte(documento, disco, etc..):**
Datos del emisor:	**Cantidad de soportes incluidos en el envío:**
Medio de transporte utilizado:	**Medidas de seguridad adoptadas para su transporte:**
Responsable que autoriza la persona que realiza la recepción. **Nombre:** **Firma:**	**Persona que realiza la recepción del soporte.** **Nombre:** **Firma:**

ANEXO G.5 Autorización para el uso de PC portátiles

El Reglamento establece que no se realizará trabajo fuera de los locales sin la debida autorización del responsable del fichero. Para ello no se deberá copiar ni transportar información de los sistemas centrales en portátiles o estaciones de trabajo que se encuentren fuera de las oficinas sin la correspondiente autorización del Responsable del fichero.

El tratamiento, acceso y transporte de los datos del fichero en ordenadores portátiles, estará sujeto en todo caso a una autorización expresa del responsable del fichero o persona delegada, y sujeta a las mismas normas de seguridad que las de un puesto de trabajo fijo.

Se deberán adjuntar en este apartado las autorizaciones explícitas por parte del responsable del fichero o persona autorizada, para el trabajo en ordenadores portátiles fuera del local habitual, indicando la identificación de la persona autorizada, la identificación del equipo, el fichero o los datos que contiene, y las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o, pérdida del equipo.

En ficheros de Nivel Alto:

Se cifrarán los datos que contengan los ordenadores portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control del responsable, si esto no es posible se hará constar las medidas alternativas que se adopten.

Utilizar el siguiente formulario para ello.

ANEXO G.5 Autorización para el uso de PC portátiles

Nombre y firma persona autorizada: **Nombre y firma del responsable que autoriza:**	**Identificación del equipo:**
Fichero o Tratamiento que contiene:	**Fecha autorización:** **Periodo de validez:**

Detallar las medidas extraordinarias para evitar la pérdida de confidencialidad de los datos en caso de robo o pérdida del equipo:
SOLO NIVEL ALTO: **Se cifrarán los datos que contengan los ordenadores portátiles cuando estos se encuentren fuera de las instalaciones que están bajo el control del responsable, si esto no es posible se hará constar las medidas alternativas que se adopten.** **Medidas alternativas:**

Se debe garantizar como mínimo el nivel de seguridad (básico, medio, alto) correspondiente al fichero.

Anexo G.6 Política de accesos.

En esta pantalla se muestra la descripción de la política de acceso a datos automatizados utilizada por la empresa.

Acceso	código: 1

Método de control: Contraseña
Ficheros implicados: CLIENTES/PROVEEDORES, USUARIOS WEB, LISTAS DE CORREO, EMPLEADOS,
Descripción del método: CONTRASEÑA EN EQUIPO
Observaciones:

5)

Solicitudes ARCO.
Modificaciones del Documento de Seguridad.
Auditorías y controles periódicos realizados.
Registro de accesos (si existe).
Relación de cesionarios.
Recomendaciones del consultor.

REGISTRO DE MODIFICACIONES DEL DOCUMENTO DE SEGURIDAD Y ANEXOS

El responsable de seguridad será el encargado de actualizar el documento de seguridad, los anexos y también de divulgar los cambios realizados. Cada vez que se actualice el documento de seguridad se anotará en el siguiente formulario.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

MODIFICACIONES Registro automatizado de Modificaciones

Lista de las modificaciones o actualizaciones realizadas en el documento de seguridad, anexos u otros documentos.

Modificación	código: 1
Fecha: 06/11/2017 **Versión:** 1 **Documento o apartado:** Primera versión del doc. de seg. sin modificaciones	

MODIFICACIONES Registro manual de Modificaciones

Lista de las modificaciones o actualizaciones realizadas en el documento de seguridad, anexos u otros documentos.

Código	Fecha	Versión	Documento o apartado modificado	Descripción de la modificación

REGISTRO DE AUDITORÍAS Y CONTROLES PERIÓDICOS

Este apartado contendrá los resultados de los controles periódicos y de las auditorías realizadas en la empresa.

CONTROLES

Registro automatizado de Auditorías y Controles periódicos realizados en la empresa

No existen datos para este documento.

Registro manual de auditorías y controles periódicos

Tipo de Control	Fecha	Documento/s Revisado/s	Resultado del Control	Persona/s o Departamentos que han intervenido

REGISTRO DE ACCESOS

El registro de accesos es una medida de control que solo es necesaria en el caso de que los ficheros dados de alta tengan un nivel de seguridad Alto, en ficheros de nivel Básico y Medio no es necesaria. Consiste en un control y registro de los accesos a los datos por parte de los usuarios. El responsable de seguridad debe realizar una revisión e informe mensual del mencionado registro y debe conservarse durante 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario que accede al fichero, se hará constar en el documento de seguridad. Se recomienda utilizar una aplicación informática para implantar esta medida, pues genera una gran cantidad de datos.

ACCESOS Registro automatizado de accesos.

No existen datos para este documento.

Documento para el Registro manual de los accesos a los Ficheros o Documentos no automatizados.

Usuario: Fecha y Hora: Fichero o Documento: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Fichero o Documento: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Fichero o Documento: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Fichero o Documento: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:
Usuario: Fecha y Hora: Fichero o Documento: Tipo de acceso: Autorizado o Denegado: Registro accedido: Cambios realizados: Finalidad:

El responsable de seguridad debe realizar una revisión mensual del registro y debe conservarse 2 años.
Solo para ficheros de nivel ALTO

Hoja Nº:

Listado de cesionarios

No existen datos para este anexo o documento.

MODELO DE EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO:
Nombre: **ALBERTO RODRIGUEZ PALOMINO**
Dirección de la Oficina de acceso: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
Nº..... C.P ..... Localidad ..... Provincia .....
con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 15 de la Ley Orgánica 15/1999 y los artículos 27 y 28 del Real Decreto 1720/2007.

SOLICITA:

1.- Que se le facilite gratuitamente el acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin que de forma expresa se conteste a la mencionada petición de acceso se entenderá denegada.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información comprenda de modo legible e inteligible los datos de base que sobre mi persona están incluidos en sus ficheros, y los resultados de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:

1. Es necesario aportar fotocopia del D.N.I. o cualquier otro medio de identificación personal válido en derecho, para que el responsable del fichero pueda realizar la comprobación oportuna. En caso de que se actúe a través de representación legal (menor de edad o incapacitado) deberá aportarse, además de la fotocopia del DNI, la documentación que acredite la representación legal.

2. Es necesario igualmente el domicilio para notificaciones, fecha y firma del interesado.

3. El derecho de acceso no podrá llevarse a cabo en intervalos inferiores a 12 meses, salvo interés legítimo debidamente justificado.

MODELO DE EJERCICIO DEL DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO:
Nombre: **ALBERTO RODRIGUEZ PALOMINO**
Dirección de la Oficina de acceso: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
Nº..... C.P ..... Localidad ..... Provincia .....
con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999 y los artículos 31 y 32 del Real Decreto 1720/2007.

SOLICITA:

1.- Que se proceda gratuitamente a la efectiva corrección, en el plazo de diez días desde la recepción de la solicitud, de los datos inexactos relativos a mi persona que se encuentren en sus ficheros.

2.- Los datos que se deben rectificar se enumeran en la hoja anexa que se acompaña a la presente solicitud, junto con los documentos que acreditan, en caso de ser necesario, la veracidad de los nuevos datos.

3.- Que me comuniquen de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada.

4.- Que si los datos rectificados hubieran sido comunicados previamente, se notifique al encargado del tratamiento la rectificación practicada, con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

5.- Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:

1. Para probar el carácter inexacto o incompleto de los datos que figuran en los ficheros resulta necesaria la aportación de la documentación que lo acredite al responsable del fichero. Si por el contrario la rectificación solicitada depende exclusivamente del consentimiento del afectado, no será necesario aportar documentación.

2. Debido al carácter personalísimo de los datos de carácter personal es necesario aportar fotocopia del D.N.I. o documento equivalente que pruebe la identidad del afectado y sea considerado válido en derecho de modo que el responsable del fichero pueda constatarla. También puede ejercitarse a través de representante legal, debiéndose aportar en este caso, además de la fotocopia del D.N.I., documento acreditativo de la representación del representante.

3. Es necesario igualmente el domicilio para notificaciones, fecha y firma del interesado.

MODELO DE EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO:

Nombre: **ALBERTO RODRIGUEZ PALOMINO**
Dirección de la Oficina de acceso: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
Nº..... C.P ..... Localidad ..... Provincia .....
con D.N.I ....., del que acompaña fotocopia.

EXPONE:

1.- Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de oposición, de conformidad con los artículos 6.4, 17 y 30.4 de la Ley Orgánica 15/1999 y en los artículos 34 y 35 del Real Decreto 1720/2007.

2.- Que (describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo):

3.- Que para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

SOLICITA:

1.- Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:

1. Debido al carácter personalísimo de los datos de carácter personal es necesario aportar fotocopia del D.N.I. o documento equivalente que pruebe la identidad del afectado y sea considerado válido en derecho de modo que el responsable del fichero pueda constatarla. También puede ejercitarse a través de representante legal, debiéndose aportar en este caso, además de la fotocopia del D.N.I., la documentación que acredite la representación legal.

2. Es necesario igualmente el domicilio para notificaciones, fecha y firma del interesado.

MODELO DE EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DEL RESPONSABLE DEL FICHERO O TRATAMIENTO:
Nombre: **ALBERTO RODRIGUEZ PALOMINO**
Dirección de la Oficina de acceso: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**

DATOS DEL SOLICITANTE:

D./Dª ....., mayor de edad, con domicilio en la C/ .....
Nº..... C.P ..... Localidad ..... Provincia .....
con D.N.I ....., del que acompaña fotocopia.

EXPONE:

Que por medio del presente escrito manifiesta su deseo de ejercer su derecho de cancelación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999 y los artículos 31 y 32 del Real Decreto 1720/2007.

SOLICITA:

1.- Que en el plazo de diez días a contar desde la recepción de la solicitud, se proceda a la efectiva cancelación de cualesquiera datos relativos a mi persona que se encuentren en sus ficheros, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y me lo comuniquen de forma descrita a la dirección arriba indicada.

2.- Que si los datos cancelados hubieran sido comunicados previamente se notifique al encargado del tratamiento la cancelación practicada con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 4 de la mencionada Ley Orgánica 15/1999.

3.- Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del plazo de diez días señalado.

En _____ a _____ de _____de 20__

Firmado:

INSTRUCCIONES:

1. Debido al carácter personalísimo de los datos de carácter personal es necesario aportar fotocopia del D.N.I. o documento equivalente que pruebe la identidad del afectado y sea considerado válido en derecho de modo que el responsable del fichero pueda constatarla. También puede ejercitarse a través de representante legal, debiéndose aportar en este caso, además de la fotocopia del D.N.I., la documentación que acredite la representación legal.

2. Es necesario igualmente el domicilio para notificaciones, fecha y firma del interesado.

3. En el caso de que se trate de datos erróneos es necesaria la aportación de copias de documentos que lo acrediten al responsable del fichero. Si por el contrario la rectificación solicitada depende exclusivamente del consentimiento del afectado, no será necesario aportar documentación.

4. Sin perjuicio del ejercicio del derecho de cancelación, a tenor del art. 16,5 de La Ley Orgánica15/1999, los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

7) CLAUSULAS

Descripción de las cláusulas jurídicas.

CLÁUSULAS

ADAPTACIÓN DE LOS FORMULARIOS DE RECOGIDA DE INFORMACIÓN DE LOS INTERESADOS

El artículo 5 de la LOPD, dispone, en relación con el **derecho de información** en la recogida de datos los siguientes aspectos:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Asimismo, **el artículo 6 LOPD** dispone, respecto del **consentimiento** del afectado, lo siguiente:

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

Por último, **el artículo 11 LOPD** dispone respecto de la **comunicación de datos** que:

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

En cumplimiento de tales obligaciones se ha preparado diversa documentación a fin de informar a los interesados –titulares de la información- de la finalidad de recogida y tratamiento de sus datos realizado por la organización.

Habiendo examinado la documentación entregada hasta la fecha por la organización, se presenta la siguiente propuesta.

En Cualquier caso, **el artículo 13 del RDLOPD**, establece la obligación de recabar el consentimiento de los menores de 14 años, así como que la información que vaya dirigida a estos, debe expresarse en un lenguaje fácilmente comprensible por estos.

MUY IMPORTANTE:

1. Una vez aprobadas deberán incorporarse en los diferentes documentos, impresos, etc. de recogida de la información.

2. Téngase especialmente en cuenta también que si hay algún cambio en relación con el tratamiento de los datos a los que estas cláusulas se refieren, las mismas pueden tener que sufrir cambios.

Cláusula para documentos que contengan datos personales de trabajadores

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que sus datos están incorporados en un fichero del que es titular **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de gestionar la relación laboral.

Los datos han podido ser comunicados a terceras empresas que realiza servicios de Prevención de riesgos laborales, asesoría laboral, auditoria y/o consultorías de otras índoles con la finalidad de llevar a cabo el cumplimiento de obligaciones con la seguridad social, tributarias, fiscales y el correcto funcionamiento de los Recursos Humanos de empresa.

Asimismo, le informamos de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos en el domicilio fiscal de **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID -**

Cláusula acciones comerciales y publicitarias

De conformidad con el artículo 5.5 de la Ley Orgánica 15/99 de Protección de datos, le informamos que sus datos han sido obtenidos de una fuente de acceso público, pasando a formar parte de un fichero automatizado titularidad de **ALBERTO RODRIGUEZ PALOMINO** y serán tratados, únicamente, para finalidades de publicidad, promociones y marketing que pudieran ser de su interés. En todo momento, podrá Ud. ejercitar sus derechos de acceso, rectificación y cancelación mediante escrito dirigido a:
C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
O bien a la dirección de correo electrónico:

De acuerdo con la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico, Vd. podrá oponerse en cualquier momento al tratamiento de sus datos con fines promocionales notificándonoslo por escrito dirigido a:
C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
O bien a la dirección de correo electrónico: indicando **BAJA** en el asunto.

Cláusula para recabar datos de trabajadores

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que los datos aportados serán incorporados a un fichero del que es titular **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de gestionar la relación laboral.

Los datos incluidos podrán ser comunicados a terceras empresas que realizan servicios de Prevención de riesgos laborales, asesoría laboral, auditoria y/o consultorías de otras índoles con la finalidad de llevar acabo el cumplimiento de obligaciones con la seguridad social, tributarias, fiscales y el correcto funcionamiento de la empresa.

Asimismo, declaro haber sido informado de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de mis datos en el domicilio fiscal de **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID -**

Cláusula para recabar datos de clientes

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que los datos aportados serán incorporados a un fichero del que es titular **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de realizar la gestión administrativa, contable y fiscal, así como enviarle comunicaciones comerciales sobre nuestros productos y servicios.

Asimismo, declaro haber sido informado de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de mis datos en el domicilio fiscal de **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID** -

Cláusula obtención de consentimiento al recabar datos de clientes

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), consiento que mis datos sean incorporados a un fichero del que es titular **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de realizar la gestión administrativa, contable y fiscal, así como enviarle comunicaciones comerciales sobre nuestros productos y/o servicios.

Asimismo, declaro haber sido informado de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de mis datos en el domicilio fiscal de **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID -**

Cláusula informativa para el e-mail

Este mensaje y sus archivos adjuntos van dirigidos exclusivamente a su destinatario, pudiendo contener información confidencial sometida a secreto profesional. No está permitida su reproducción o distribución sin la autorización expresa de **ALBERTO RODRIGUEZ PALOMINO**. Si usted no es el destinatario final por favor elimínelo e infórmenos por esta vía.

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que sus datos están incorporados en un fichero del que es titular **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de realizar la gestión administrativa, contable y fiscal, así como enviarle comunicaciones comerciales sobre nuestros productos y/o servicios.

Asimismo, le informamos de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos en el domicilio fiscal de **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.**

Si usted no desea recibir nuestra información, póngase en contacto con nosotros enviando un correo electrónico a la siguiente dirección:

Cláusula para documentos que contengan datos personales de clientes

De acuerdo con lo establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), le informamos que sus datos están incorporados en un fichero del que es titular **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de realizar la gestión administrativa, contable y fiscal, así como enviarle comunicaciones comerciales sobre nuestros productos y/o servicios que puedan ser de su interés.

Asimismo, le informamos de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos en el domicilio fiscal de **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID** -

Circular informativa implantación lopd

Estimado cliente,

La presente circular tiene por objeto poner en su conocimiento que hemos implantado las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal que almacenamos, de acuerdo con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Es nuestro deber informarle que como consecuencia de la relación comercial que nos une, sus datos están incluidos en un fichero debidamente inscrito en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos con la finalidad de realizar la gestión administrativa, contable y fiscal y realizar el envío de información comercial sobre nuestros productos y servicios.

ALBERTO RODRIGUEZ PALOMINO se compromete a cumplir con lo dispuesto por la normativa sobre protección de datos anteriormente mencionada, así como a hacer cumplir las medidas de seguridad técnicas y organizativas implantadas al personal a su servicio que trate datos de carácter personal, evitando de esta forma, la pérdida alteración y acceso no autorizado a los mismos. Dicho personal se halla sujeto al deber de secreto y confidencialidad respecto a los datos que trata en los mismos términos que **ALBERTO RODRIGUEZ PALOMINO**.

Le informamos también que puede ejercer sus derechos de acceso, rectificación, cancelación y oposición de sus datos dirigiéndose a **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID -**

Circular Currículum vitae

Estimado Sr./Sra.:

Acusamos recibo del escrito en que nos remite su Currículum Vitae.

Le comunicamos que, con fecha de hoy, vamos a proceder a incluir sus datos en un fichero debidamente inscrito en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Los datos que nos ha proporcionado serán tratados únicamente para los procesos de selección de personal realizados por la Organización.

Si no estuviese conforme con alguno de los extremos señalados, rogamos nos lo haga saber dentro del plazo de treinta días a contar desde la recepción de esta comunicación. De otro modo, entendemos que muestra su total conformidad al respecto.

Le informamos también que puede ejercer sus derechos de acceso, rectificación, cancelación y oposición de sus datos dirigiéndose a **ALBERTO RODRIGUEZ PALOMINO** sito en **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID** -

PROTECCIÓN DE DATOS - DERECHO DE INFORMACIÓN

De conformidad con la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal:

Le informamos que los datos personales facilitados por el afectado o interesado serán incluidos en un fichero titularidad de **ALBERTO RODRIGUEZ PALOMINO** con la finalidad de prestarle los servicios solicitados o contratados, y enviarle información comercial de nuestros productos o servicios. Dicho fichero se encuentra debidamente inscrito en la Agencia Española de Protección de Datos.

Los datos obtenidos serán únicamente tratados para el fin por el cual se obtienen, respetando los principios de confidencialidad, calidad y proporcionalidad. Dichos datos serán siempre pertinentes, adecuados y no excesivos.

Los destinatarios de la información son la propia entidad y sus departamentos. Para cualquier posible cesión de datos, se solicitará el consentimiento del afectado por escrito, excepto las autorizadas legalmente.

En cualquier momento, Ud. podrá ejercitar los derechos de acceso, rectificación, oposición y, en su caso, cancelación, comunicándolo por escrito dirigido a: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**, o al e-mail:

Fecha: **12-11-2017**

Firma y sello:

8) USOS Y RECOMENDACIONES

Manual de usos y recomendaciones. (Para todos los usuarios con acceso)

USOS Y RECOMENDACIONES

Todas las personas que tengan acceso a los ficheros protegidos, a través del sistema informático o a través de cualquier otro medio automatizado de acceso, están obligadas por ley a cumplir lo establecido en el Documento de Seguridad que dispone la empresa, y por lo tanto, sujetas a las consecuencias que puedan derivar en caso de incumplimiento. El incumplimiento de las políticas, prácticas y procedimientos de seguridad estará sujeto a una acción disciplinaria, pudiendo conllevar una acción civil y/o penal.

Esta normativa debe difundirse a todos los empleados para que todos los usuarios sepan a qué medidas de seguridad están sujetos en materia de Protección de Datos, asimismo, se recomienda hacer la entrega de algún modo que permita registrar el acuse de recibo por parte de los usuarios.

FUNCIONES RDLOPD ASIGNADAS AL RESPONSABLE DEL FICHERO

1. Elaborar e implantar la normativa de seguridad que deben adoptar los ficheros detallados en el correspondiente ANEXO A del documento de seguridad así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

2. Aprobar la notificación a la Agencia de Protección de Datos los ficheros de datos personales que se creen así como sus modificaciones relevantes o su eliminación. Cuando se trate de Administraciones Públicas se promoverá la publicación de la oportuna Disposición de Creación del Fichero.

3. Comprobar el cumplimiento del deber de información, con anterioridad a la recogida de datos de acuerdo con los medios que se utilicen para ello.

4. Recabar el consentimiento de los interesados, siempre que éste sea necesario para el tratamiento de sus datos.

5. Aprobar la designación y autorización de usuarios que emplean la aplicación en su labor cotidiana, asignando los accesos permitidos a cada usuario.

6. Aprobar una política que tenga por objetivo la formación adecuada del personal con los siguientes fines:
- conocimiento de las medidas de seguridad que afecten a las funciones de cada usuario.
- conocimiento de los procedimientos a seguir por el afectado para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

7. Autorizar la puesta en marcha de la explotación de los datos de carácter personal mediante una nueva aplicación informática, o la realización de mejoras sustanciales sobre la existente.

8. Autorizar la aprobación de una política para la salida de soportes informáticos que contengan datos de carácter personal fuera de los locales en los que esté ubicado el tratamiento.

9. Aprobar la corrección de los procedimientos establecidos para la asignación de contraseñas a fin de garantizar la confidencialidad de las mismas.

10. Aprobar los procedimientos de realización de copias de seguridad y de recuperación de los datos.

11. Aprobar las medidas correctoras que se deriven de la correspondiente auditoría.

12. Y, en general, cualquier obligación que se derive de la normativa que resulte de aplicación.

FUNCIONES RDLOPD ASIGNADAS AL RESPONSABLE DE SEGURIDAD

88.7 RDLOPD Implantar (o, en su caso, modificar) controles periódicos para verificar el cumplimiento de lo establecido en el documento de seguridad.

88.7 RDLOPD Revisar los controles periódicos para verificar el cumplimiento de lo establecido en el documento de seguridad.

89.1 RDLOPD Documentar las funciones y obligaciones del personal.

89.1 RDLOPD Definir las funciones y obligaciones del personal.

89.2 RDLOPD Adoptar las medidas necesarias para que los usuarios de su organización conozcan las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

95 RDLOPD Nombrar a los responsables de seguridad oportunos y adoptar las medidas necesarias para que los Responsables de Seguridad conozcan las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

91.2 RDLOPD Disponer de una relación actualizada de usuarios con acceso autorizado al sistema de información, con procedimientos de identificación y autenticación para dicho acceso.

93.1 RDLOPD Establecer 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.

93.2 RDLOPD En caso de autenticación con contraseñas, definir e implantar un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

93.3 RDLOPD Controlar que las contraseñas se cambien periódicamente y su almacenamiento sea de forma ininteligible mientras estén vigentes.

98 RDLOPD Establecer un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

91.1 RDLOPD Establecer controles de acceso para los usuarios de tal forma que sólo tengan acceso autorizado a datos y recursos necesarios para sus funciones.

91.3 RDLOPD Establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

91.4 RDLOPD Disponer lo necesario para que sólo el personal autorizado pueda conceder, alterar o anular el acceso autorizado, según los criterios establecidos por el responsable del fichero.

99 RDLOPD Establecer lo oportuno para que exclusivamente el personal autorizado en el documento de seguridad pueda tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

100.1 RDLOPD Cuidar que dicho registro consigne 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.

100.2 RDLOPD Recabar la autorización por escrito del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

90 RDLOPD Fijar un procedimiento de notificación y gestión de incidencias con indicación de: tipo, fecha-hora, persona que notifica, a quién se comunica y efectos que produzca.

92.1 RDLOPD Encargarse de que los soportes informáticos se inventaríen y almacenen en un lugar con acceso restringido al personal autorizado en el documento de seguridad. (NOTA: Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad).s

92.2 RDLOPD Autorizar la salida de soportes fuera de los locales.

92.4 RDLOPD Proceder a la destrucción o borrado de cualquier documento o soporte que contenga datos de carácter personal que vaya a desecharse, adoptando las medidas para impedir cualquier recuperación posterior de la información.

97.1 RDLOPD Crear y mantener un registro de entrada de soportes informáticos con indicación de: tipo de soporte, fecha y hora, emisor, número de soportes, tipo de información que contienen, forma de envío y responsable de la recepción (que deberá estar debidamente autorizado).

97.2 RDLOPD Crear y mantener un registro de salida de soportes informáticos con indicación de: tipo de soporte, fecha y hora, destinatario, número de soportes, tipo de información que contienen, forma de envío y responsable de la entrega (que deberá estar debidamente autorizado).

93.4 RDLOPD 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.

94.1 RDLOPD Realizar copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

94.2 RDLOPD Verificar la definición y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos. (Dichos procedimientos de copias de respaldo y recuperación de los datos deberán garantizar su reconstrucción en el estado en el que se encontraban al producirse la pérdida o destrucción. Art. 94.2.).

96.1 RDLOPD Someter los sistemas de información, al menos cada 2 años, a una auditoría interna o externa que verifique el cumplimiento del Reglamento, procedimientos e instrucciones. (El informe de auditoría dictaminará sobre la adecuación de las medidas y controles, identificará deficiencias y propondrá medidas correctoras o complementarias. Deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas. ART. 96.2.).

96.3 RDLOPD Analizar el informe de auditoría y elevar las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia de Protección de Datos.

94.4 RDLOPD Realizar una copia de seguridad con carácter previo a la realización de pruebas con datos reales.

94.4 RDLOPD Encargarse de que, anteriormente a la implantación o modificación de los sistemas de información, las pruebas no se realicen con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

4.1 LOPD Revisar que los datos que se traten sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

4.2 LOPD Revisar que los datos de carácter personal objeto de tratamiento no se usen para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4.3 LOPD Revisar que los datos de carácter personal sean exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4.4 LOPD Ordenar lo oportuno para que los datos de carácter personal sean cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados o cuando resultaran ser inexactos, en todo o en parte, o incompletos y revisar la correcta ejecución de esta obligación.

11 LOPD Comprobar que, salvo en los supuestos en que la Ley exceptúa esta obligación, se cuenta con el consentimiento, previo, libre e informado del titular de los datos para la cesión de sus datos.

6 LOPD Comprobar que, salvo en los supuestos en que la Ley exceptúa esta obligación, se cuenta con el consentimiento, previo, libre e informado del titular de los datos para el tratamiento de sus datos.

5 LOPD Comprobar el cumplimiento del deber de información.

12 LOPD Detectar los supuestos de encargados del tratamiento y comprobar la suscripción de los contratos de encargado/s del tratamiento.

20 26 LOPD Detectar y - en su caso- notificar a la Agencia de Protección de Datos la inscripción de nuevos ficheros.

20 26 LOPD Detectar y - en su caso- notificar a la Agencia de Protección de Datos la modificación de ficheros de su organización.

20 26 LOPD Detectar y - en su caso- notificar a la Agencia de Protección de Datos la supresión de ficheros de su organización.

15 16 LOPD Atender las peticiones de ejercicio de los derechos de acceso rectificación, cancelación y oposición.

15 16 LOPD Implantar (y en su caso revisar y/o modificar) el procedimiento para la atención al titular de los datos en el ejercicio de los derechos de acceso rectificación, cancelación y oposición.

33 34 LOPD Comprobar si se producen transferencias internacionales y, -en el caso en que se produzcan- que, salvo en los supuestos en que la Ley exceptúa esta obligación, se cuenta con la autorización del Director de la Agencia Española de Protección de Datos para proceder a la realización de transferencias internacionales de datos.

FUNCIONES RDLOPD ASIGNADAS A LOS USUARIOS

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Guardar todos los soportes físicos y/o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

3. Queda prohibido el traslado de cualquier soporte, listado o documento con datos de carácter personal en los que se almacene información titularidad de la organización fuera de los locales de la misma, sin autorización previa del Responsable de Seguridad. En el supuesto de existir traslado o distribución de soportes y documentos se realizará cifrando dichos datos, o mediante otro mecanismo que imposibilite el acceso o manipulación de la información por terceros.

4. Ficheros de carácter temporal o copias de documentos son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada o trabajos temporales y auxiliares, siempre y cuando su existencia no sea superior a un mes. Estos ficheros de carácter temporal o copias de documentos deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán cumplir con los niveles de seguridad asignados por el Responsable de Seguridad. Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.

5.Únicamente las personas autorizadas en un listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad correspondiente.

6. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

7. Cambiar las contraseñas a petición del sistema.

8. Cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

9. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al ordenador personal, disquetes, portátil o a cualquier otro soporte sin autorización expresa del Responsable de Seguridad correspondiente.

10. Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad correspondiente, a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.

11. Los usuarios tiene prohibido el envío de información de carácter personal de nivel alto, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

12. Los usuarios no podrán, salvo autorización expresa del Responsable de Seguridad que tenga asignada esta tarea, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador empleado en el puesto de trabajo.

13. Queda prohibido:

a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad competente.

c. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.

d. Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.

g. Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

14. Mantener debidamente custodiadas las llaves de acceso a la organización, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de carácter personal, debiendo poner en conocimiento del Responsable de Seguridad competente cualquier hecho que pueda haber comprometido esa custodia.

15. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

16. Asegurarse de que no quedan documentos impresos que contengan datos de carácter personal impresos en la bandeja de salida de la impresora o fax.

17. Establecerse procedimientos en el copiado o reproducción de documentos, a fin que solo puedan acceder a las copias las personas habilitadas por el Responsable de Seguridad correspondiente.

FUNCIONES RDLOPD ASIGNADAS A LOS USUARIOS DE FICHEROS NO AUTOMATIZADOS

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.

2. Mantener debidamente custodiadas las llaves de acceso a la residencia, a sus despachos y a los armarios, archivadores u otros elementos que contenga ficheros no automatizados con datos de carácter personal, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido esa custodia.

3. Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

4. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

5. Queda prohibido el traslado de cualquier listado o documento análogo con datos de carácter personal en los que se almacene información titularidad de la entidad fuera de los locales de la misma.

6. Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

7. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.

8. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad.

9. Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de carácter temporal deben ser destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán contemplarse las medidas de seguridad contenidas en este documento.

FUNCIONES RDLOPD ASIGNADAS A LOS USUARIOS ADMINISTRADORES INFORMÁTICOS

El usuario que tiene privilegios para la administración de equipos informáticos, debe conocer las obligaciones que le corresponden como personal informático. Debido al especial acceso que tiene el persona informático se le atribuyen unas responsabilidades complementarias:

1. Guardar secreto de toda la información de carácter personal, o que afecte a ésta, de la que tenga conocimiento en el desarrollo de su de trabajo, aún después de acabada la relación con la organización.

2. Aunque debido a sus funciones disponga de un acceso privilegiado a ciertos recursos, se compromete a acceder únicamente a los datos necesarios para desarrollar sus funciones.

3. En el caso que detecten, deficiencias de seguridad en el sistema de información, lo deberán comunicar al Responsable de Seguridad correspondiente.

4. Colaborar con el Responsable/s de Seguridad en la resolución de las incidencias que se le encarguen.

5. Desempeñar sus funciones con estricta observancia de las obligaciones dispuestas por la legislación sobre protección de datos.

FUNCIONES RDLOPD ASIGNADAS A LOS USUARIOS DE ATENCIÓN AL PÚBLICO

1. Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

2. Mantener en secreto sus claves de acceso al sistema, debiendo poner en conocimiento del Responsable de Seguridad cualquier hecho que pueda haber comprometido el secreto.

3. Las contraseñas de acceso al sistema son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.

4. Cambiar las contraseñas a petición del sistema.

5. Cerrar o bloquear todas las sesiones al término de la jornada laboral.

6. Bloquear las sesiones en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

7. Comunicar al Responsable de Seguridad, conforme al procedimiento de notificación, las incidencias de seguridad de las que tenga conocimiento.

8. No copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal al propio ordenador, disquetes o a cualquier otro soporte sin autorización expresa del Responsable de Seguridad. Queda igualmente prohibido el traslado de cualquier soporte en los que se almacene información titularidad de la compañía fuera de los locales de la misma.

9. Guardar todos los ficheros con datos de carácter personal en la carpeta indicada por el Responsable de Seguridad a fin de facilitar la aplicación de las medidas de seguridad que les correspondan.

10. Guardar todos los soportes físicos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

11. Asegurarse de que no quedan documentos impresos que contengan datos protegidos impresos en la bandeja de salida de la impresora.

12. Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular los datos contenidos en los ficheros objeto de protección. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Responsable de Seguridad.

13. Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a un mes. Los ficheros de carácter temporal deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación y, mientras estén vigentes, deberán ser almacenados en la carpeta designada por el Responsable de Seguridad. Si, transcurrido el mes, el usuario necesita continuar utilizando la información almacenada en el fichero, deberá comunicarlo al Responsable de Seguridad, para adoptar las medidas oportunas sobre el mismo.

14. El correo electrónico es considerado por la entidad como elemento fundamental para las comunicaciones entre la organización y el resto de agentes, públicos o privados, que intervienen en las relaciones propias de la actividad desarrollada. Por ello, el correo electrónico sea cual sea la dirección asignada, se configura como una herramienta de trabajo no exclusiva, colectiva y de libre acceso, asignadas a áreas o puestos de trabajo y no a personas. Queda prohibido el uso del mismo para fines no relacionados con las funciones laborales encomendadas. El empleo del nombre o apellidos de los trabajadores o funcionarios junto al dominio de la organización en las direcciones de correo no significa la asignación por la organización de un correo personal, esto se realiza únicamente por motivos organizativos internos de asignación de áreas y puestos de trabajo. Los usuarios tienen prohibido el envío de Información de carácter personal de nivel alto, salvo autorización expresa del Responsable de Seguridad. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

15. Los usuarios no podrán, salvo autorización expresa del Responsable de Seguridad, instalar cualquier tipo de programas informáticos o dispositivos ni en los servidores centrales ni en el ordenador personal empleado para el desarrollo de su trabajo.

16. Conocer la existencia de derechos de los interesados (derecho acceso, rectificación, cancelación y, en su caso, oposición), así como su procedimiento de respuesta ante el ejercicio de uno de ellos.

17. Queda prohibido:

a. Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

b. Intentar modificar o acceder al registro de accesos habilitado por el Responsable de Seguridad.

c. Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros o programas cuyo acceso no le haya sido permitido.

d. Utilizar Internet para tareas que no estén relacionadas directamente con las funciones asignadas al usuario. La organización regulará las modalidades de acceso y las restricciones o limitaciones del mismo. Queda prohibida la descarga de software o ficheros de cualquier tipo desde Internet, sin consentimiento expreso de la organización, y ello aunque resulte de un acceso consentido por motivos de trabajo.

e. Introducir contenidos en la red corporativa y/o ordenador personal que no guarden relación con la actividad y objetivos de la entidad.

f. Enviar correos masivos (spam) empleando la dirección de correo electrónico corporativa.

g. Y en general, el empleo de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

9) MEDIDAS DE SEGURIDAD

1. Manual de medidas de seguridad y organizativas.
2. Medidas de destrucción. (Desechos informáticos)

MEDIDAS DE SEGURIDAD Y ORGANIZATIVAS

Se recomienda adoptar todas estas medidas en la empresa, es posible que algunas requieran la intervención de un técnico informático.

-Activar contraseñas a nivel de Windows o programas de gestión.

-Limitación de acceso a información innecesaria para el usuario.

-Salva pantallas activado por contraseña.

-Copias de seguridad una vez por semana mínimo, si se han modificado datos.

-Incluir textos informativos sobre la LOPD en la documentación de la empresa (presupuestos, facturas, cartas informativas, formularios de recogida de datos, correos electrónicos, Currículums, etc..).

-Utilizar una destructora de papel.

-Guardar las copias de seguridad en lugar seguro bajo llave o de acceso restringido.

-Inventariar y etiquetar los soportes (pendrives, etc..) utilizados en las copias de seguridad según indica el programa.

-Guardar la aplicación con la que se hacen las copias de seguridad en lugar seguro por si hay que hacer una recuperación.

-Charla informativa con el personal de la empresa sobre programas nocivos para el sistema informático, buen uso de las contraseñas, informar y entregar a los usuarios de la empresa los formularios habilitados por el programa para atender posibles peticiones sobre los derechos ARCO (acceso, rectificación, cancelación y oposición) de los clientes.

PROCEDIMIENTO PARA LA DESTRUCCIÓN DE DESECHOS INFORMÁTICOS

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados. En este apartado se describirá el método empleado para la destrucción o borrado de los mismos. Como mínimo se deberá seguir el siguiente procedimiento.

Todos los desechos informáticos de cualquier tipo que puedan contener información del Fichero, como CDs, cintas, discos removibles, listados, memorias removibles de cualquier tipo, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo con el siguiente Procedimiento para la Destrucción de Desechos Informáticos.

1. Como norma general ningún desecho informático, ya sea listado u otro tipo de soporte, debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

2. Aquellos informes en papel o CDs que contengan datos de carácter personal más sensible y no sean voluminosos, deberán ser destruidos en una destructora de papel si es que existe en la organización.

3. En caso de no existir máquina destructora de papel y CDs o en el caso de que los listados e informes sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una compañía de reciclaje que garantice mediante contrato la destrucción de los mismos.

4. Todos los disquetes y otros soportes removibles desechados deberán ser formateados y entregados para su reutilización al Responsable de Seguridad o al Responsable del Fichero. En el caso de que no se vayan a reutilizar deberán ser formateados si se puede, y depositados en los contenedores confidenciales de la organización para ser entregados a la empresa encargada de la destrucción de los datos.

5. Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras instituciones, deberá comunicarse al Responsable de Seguridad para que se formatee el disco duro o se pase un programa especial que elimine de forma segura todos los datos de los discos duros. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y depositarlos en el contenedor de la empresa de reciclaje para su destrucción.

6. El responsable del fichero deberá exigir a la empresa de reciclaje un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

10) CONTRATOS

Prestación de servicios con acceso a datos:
1. Contratos de Encargados de tratamiento (si existieran).
2. Contratos de tratamientos (si existieran).

Prestación de servicios sin acceso a datos:
1. Contrato de prestación de servicios sin acceso a datos de carácter personal,(si existieran).

Acuerdo de cesiones:
1. Contrato de acuerdo de cesión de datos (si existieran).

ANEXO CONTRATOS

En este anexo puede encontrar:

- Contratos de Encargados de tratamiento
- Contratos de prestación de servicios sin acceso a datos personales
- Acuerdos de cesión de datos

PRESTACIONES DE SERVICIO CON ACCESO A DATOS:

No se considerará comunicación de datos el acceso de un tercero a los datos cuando sea necesario para la prestación de un servicio.

En este caso cuando un tercero presta servicio a ALBERTO RODRIGUEZ PALOMINO y para ello necesita realizar un acceso a datos que están bajo la responsabilidad de ALBERTO RODRIGUEZ PALOMINO (en adelante el Responsable del fichero), a este tercero con acceso a datos se le denominará como ENCARGADO DE TRATAMIENTO y se seguirá las siguientes directrices:

El Responsable del fichero y el Encargado de tratamiento deberán firmar un contrato basado en el art. 12 de la LOPD para legalizar esta situación.

Estos son los contratos de Encargados de tratamiento que encontrará en este anexo con su asesoría laboral, asesoría fiscal, prevención d riesgos laborales, mantenimiento informático, etc…

PRESTACIONES DE SERVICIO SIN ACCESO A DATOS:

El Responsable del fichero adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer de forma accidental con motivo de la prestación del servicio.

En este anexo encontrará los contratos para legitimar esta situación con su empresa de limpieza, mantenimiento de extintores, etc...

COMUNICACIÓN / CESIÓN DE DATOS:

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Para realizar una cesión de datos, deberá firmar el/los acuerdos de cesión de datos que encuentre en este anexo, así como obtener el consentimiento expreso (mediante el aviso legal que encontrará en el apartado correspondiente) del titular de los datos que vayan a ser contenido de la cesión.

No será necesario ni el acuerdo de cesión de datos, ni el consentimiento del titular, siempre y cuando la cesión de datos sea obligatoria y/o esta autorizada por Ley (cesiones a: bancos y cajas de ahorro, administración tributaria, seguridad social, entidades aseguradoras, etc…).

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

_____ de _____ de _____

REUNIDOS

De una parte, ALBERTO RODRIGUEZ PALOMINO con NIF/CIF 51126442H, y domicilio social en C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
Representada por el Sr./a ALBERTO RODRIGUEZ PALOMINO con NIF 51126442H.

(En adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, AGENCIA SERVICIOS MENSAJERIA, S.A. con NIF/CIF A61441523, y domicilio social en Avda. Fuentemar, 18 - 28823 - Coslada - MADRID.
Representada por el Sr./a con NIF .

(En adelante, el ENCARGADO DEL TRATAMIENTO).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla en la actualidad, prestando determinados servicios de: Empresa de mensajería. Empresa de mensajería
II. Que el RESPONSABLE DEL FICHERO ha contratado los servicios del ENCARGADO DEL TRATAMIENTO, consistentes en: Empresa de mensajería. Empresa de mensajería
III.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal del Responsable del fichero.
IV.- Que de conformidad con el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD), ambas partes convienen en suscribir el presente CONTRATO, el cual aceptan expresamente y de acuerdo a las siguientes:

ESTIPULACIONES

PRIMERA.- Definiciones.
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes.
Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física o en el caso de representantes de una persona jurídica o Administración serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento.
Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa manifestada por escrito del Responsable. Se prohíbe asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto.
El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.
Se adoptarán las medidas de nivel básico, medio o alto según corresponda (tal y como se indica en el anexo), de acuerdo con lo dispuesto en el RD 1720/2007, así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

Se atenderá a las siguientes reglas:
En caso de ser realizados los servicios que impliquen tratamiento de datos personales, objeto del presente contrato, en las propias instalaciones del Responsable, en equipos de hardware y software de ésta, así como cuando este sea remoto (Art. 82.1 RDLOPD). El Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales en las propias instalaciones del encargado del tratamiento, el mismo adoptará las medidas de seguridad correspondientes, elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RDLOPD).

SEXTA.- Ejercicio de derechos por los interesados.
Los derechos de acceso, rectificación, cancelación y, en su caso, oposición, se ejercerán por los interesados ante el Responsable del tratamiento. Si el encargado recibiese una petición de ejercicio de derechos deberá informar al interesado de la identidad del responsable para que se dirija al mismo.

SÉPTIMA.- Deber de devolución y no conservación.
Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
Aquellos datos que no se devuelvan, deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el encargado del tratamiento conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

OCTAVA.- Responsabilidad.
Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA.- Subcontratación.
El Responsable apodera al Encargado para que subcontrate, en nombre y por cuenta del responsable, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. A estos efectos, el Encargado informa al Responsable de la identidad de la sociedad a la cual pretende él subcontratar los servicios objeto de este contrato así como de los servicios que serían objeto de esta subcontratación. La validez del apoderamiento que el responsable en su caso otorgue (y que en tal caso deberá constar por escrito) quedará sujeta a la firma de un contrato escrito entre el Encargado y la empresa subcontratada, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el encargado en su propio nombre y el subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por el subcontratista.

DÉCIMA.- Fuero.
Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales más cercanos al domicilio del responsable del fichero, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

ANEXO. I

FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO.

1. INTRODUCCIÓN.

El presente anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros que trata el encargado, los datos concretos que trata, el nivel de seguridad a adoptar por el encargado y las finalidades que justifican el tratamiento.

2. ACCESO POR PARTE DEL ENCARGADO.

Nombre del fichero/s que trata el encargado, nivel de seguridad y datos identificativos que contiene:

Finalidad que justifica el tratamiento por parte del encargado:
Empresa de mensajería. Empresa de mensajería

Información adicional sobre el tratamiento:

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

_____ de _____ de _____

REUNIDOS

De una parte, ALBERTO RODRIGUEZ PALOMINO con NIF/CIF 51126442H, y domicilio social en C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
Representada por el Sr./a ALBERTO RODRIGUEZ PALOMINO con NIF 51126442H.

(En adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, AMERICAN M Y D, S.L. con NIF/CIF B60260452, y domicilio social en Plaza de Francesc Macià, 8 - 08029 - Barcelona - BARCELONA.
Representada por el Sr./a con NIF .

(En adelante, el ENCARGADO DEL TRATAMIENTO).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla en la actualidad, prestando determinados servicios de: Proveedor productos medicos y dentales. Proveedor productos medicos y dentales
II. Que el RESPONSABLE DEL FICHERO ha contratado los servicios del ENCARGADO DEL TRATAMIENTO, consistentes en: Proveedor productos medicos y dentales. Proveedor productos medicos y dentales
III.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal del Responsable del fichero.
IV.- Que de conformidad con el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD), ambas partes convienen en suscribir el presente CONTRATO, el cual aceptan expresamente y de acuerdo a las siguientes:

ESTIPULACIONES

PRIMERA.- Definiciones.
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes.
Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física o en el caso de representantes de una persona jurídica o Administración serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento.
Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa manifestada por escrito del Responsable. Se prohíbe asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto.
El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.
Se adoptarán las medidas de nivel básico, medio o alto según corresponda (tal y como se indica en el anexo), de acuerdo con lo dispuesto en el RD 1720/2007, así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

Se atenderá a las siguientes reglas:
En caso de ser realizados los servicios que impliquen tratamiento de datos personales, objeto del presente contrato, en las propias instalaciones del Responsable, en equipos de hardware y software de ésta, así como cuando este sea remoto (Art. 82.1 RDLOPD). El Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales en las propias instalaciones del encargado del tratamiento, el mismo adoptará las medidas de seguridad correspondientes, elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RDLOPD).

SEXTA.- Ejercicio de derechos por los interesados.
Los derechos de acceso, rectificación, cancelación y, en su caso, oposición, se ejercerán por los interesados ante el Responsable del tratamiento. Si el encargado recibiese una petición de ejercicio de derechos deberá informar al interesado de la identidad del responsable para que se dirija al mismo.

SÉPTIMA.- Deber de devolución y no conservación.
Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
Aquellos datos que no se devuelvan, deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el encargado del tratamiento conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

OCTAVA.- Responsabilidad.
Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA.- Subcontratación.
El Responsable apodera al Encargado para que subcontrate, en nombre y por cuenta del responsable, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. A estos efectos, el Encargado informa al Responsable de la identidad de la sociedad a la cual pretende él subcontratar los servicios objeto de este contrato así como de los servicios que serían objeto de esta subcontratación. La validez del apoderamiento que el responsable en su caso otorgue (y que en tal caso deberá constar por escrito) quedará sujeta a la firma de un contrato escrito entre el Encargado y la empresa subcontratada, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el encargado en su propio nombre y el subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por el subcontratista.

DÉCIMA.- Fuero.
Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales más cercanos al domicilio del responsable del fichero, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

ANEXO. I

FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO.

1. INTRODUCCIÓN.

El presente anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros que trata el encargado, los datos concretos que trata, el nivel de seguridad a adoptar por el encargado y las finalidades que justifican el tratamiento.

2. ACCESO POR PARTE DEL ENCARGADO.

Nombre del fichero/s que trata el encargado, nivel de seguridad y datos identificativos que contiene:

Finalidad que justifica el tratamiento por parte del encargado:
Proveedor productos medicos y dentales. Proveedor productos medicos y dentales

Información adicional sobre el tratamiento:

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

_____ de _____ de _____

REUNIDOS

De una parte, ALBERTO RODRIGUEZ PALOMINO con NIF/CIF 51126442H, y domicilio social en C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
Representada por el Sr./a ALBERTO RODRIGUEZ PALOMINO con NIF 51126442H.

(En adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, ASESORIA DE CONSUMO Y SANIDAD, S.L. con NIF/CIF B91985978, y domicilio social en Calle Imagen 7 - 5º derecha - 41003 - Sevilla - SEVILLA.
Representada por el Sr./a con NIF .

(En adelante, el ENCARGADO DEL TRATAMIENTO).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla en la actualidad, prestando determinados servicios de: Tecnico garante. Tecnico garante
II. Que el RESPONSABLE DEL FICHERO ha contratado los servicios del ENCARGADO DEL TRATAMIENTO, consistentes en: Tecnico garante. Tecnico garante
III.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal del Responsable del fichero.
IV.- Que de conformidad con el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD), ambas partes convienen en suscribir el presente CONTRATO, el cual aceptan expresamente y de acuerdo a las siguientes:

ESTIPULACIONES

PRIMERA.- Definiciones.
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes.
Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física o en el caso de representantes de una persona jurídica o Administración serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento.
Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa manifestada por escrito del Responsable. Se prohíbe asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto.
El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.
Se adoptarán las medidas de nivel básico, medio o alto según corresponda (tal y como se indica en el anexo), de acuerdo con lo dispuesto en el RD 1720/2007, así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

Se atenderá a las siguientes reglas:
En caso de ser realizados los servicios que impliquen tratamiento de datos personales, objeto del presente contrato, en las propias instalaciones del Responsable, en equipos de hardware y software de ésta, así como cuando este sea remoto (Art. 82.1 RDLOPD). El Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales en las propias instalaciones del encargado del tratamiento, el mismo adoptará las medidas de seguridad correspondientes, elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RDLOPD).

SEXTA.- Ejercicio de derechos por los interesados.
Los derechos de acceso, rectificación, cancelación y, en su caso, oposición, se ejercerán por los interesados ante el Responsable del tratamiento. Si el encargado recibiese una petición de ejercicio de derechos deberá informar al interesado de la identidad del responsable para que se dirija al mismo.

SÉPTIMA.- Deber de devolución y no conservación.
Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
Aquellos datos que no se devuelvan, deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el encargado del tratamiento conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

OCTAVA.- Responsabilidad.
Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA.- Subcontratación.
El Responsable apodera al Encargado para que subcontrate, en nombre y por cuenta del responsable, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. A estos efectos, el Encargado informa al Responsable de la identidad de la sociedad a la cual pretende él subcontratar los servicios objeto de este contrato así como de los servicios que serían objeto de esta subcontratación. La validez del apoderamiento que el responsable en su caso otorgue (y que en tal caso deberá constar por escrito) quedará sujeta a la firma de un contrato escrito entre el Encargado y la empresa subcontratada, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el encargado en su propio nombre y el subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por el subcontratista.

DÉCIMA.- Fuero.
Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales más cercanos al domicilio del responsable del fichero, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

ANEXO. I

FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO.

1. INTRODUCCIÓN.

El presente anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros que trata el encargado, los datos concretos que trata, el nivel de seguridad a adoptar por el encargado y las finalidades que justifican el tratamiento.

2. ACCESO POR PARTE DEL ENCARGADO.

Nombre del fichero/s que trata el encargado, nivel de seguridad y datos identificativos que contiene:

Finalidad que justifica el tratamiento por parte del encargado:
Tecnico garante. Tecnico garante

Información adicional sobre el tratamiento:

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

_____ de _____ de _____

REUNIDOS

De una parte, ALBERTO RODRIGUEZ PALOMINO con NIF/CIF 51126442H, y domicilio social en C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
Representada por el Sr./a ALBERTO RODRIGUEZ PALOMINO con NIF 51126442H.

(En adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, INTERNACIONAL VENTUR, S.A. con NIF/CIF A12093357, y domicilio social en Calle Luxemburgo, 75 - 12006 - Castellón de la Plana - CASTELLON DE LA PLANA.
Representada por el Sr./a con NIF .

(En adelante, el ENCARGADO DEL TRATAMIENTO).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla en la actualidad, prestando determinados servicios de: Proveedor productos dentales. Proveedor productos dentales
II. Que el RESPONSABLE DEL FICHERO ha contratado los servicios del ENCARGADO DEL TRATAMIENTO, consistentes en: Proveedor productos dentales. Proveedor productos dentales
III.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal del Responsable del fichero.
IV.- Que de conformidad con el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD), ambas partes convienen en suscribir el presente CONTRATO, el cual aceptan expresamente y de acuerdo a las siguientes:

ESTIPULACIONES

PRIMERA.- Definiciones.
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes.
Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física o en el caso de representantes de una persona jurídica o Administración serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento.
Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa manifestada por escrito del Responsable. Se prohíbe asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto.
El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.
Se adoptarán las medidas de nivel básico, medio o alto según corresponda (tal y como se indica en el anexo), de acuerdo con lo dispuesto en el RD 1720/2007, así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

Se atenderá a las siguientes reglas:
En caso de ser realizados los servicios que impliquen tratamiento de datos personales, objeto del presente contrato, en las propias instalaciones del Responsable, en equipos de hardware y software de ésta, así como cuando este sea remoto (Art. 82.1 RDLOPD). El Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales en las propias instalaciones del encargado del tratamiento, el mismo adoptará las medidas de seguridad correspondientes, elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RDLOPD).

SEXTA.- Ejercicio de derechos por los interesados.
Los derechos de acceso, rectificación, cancelación y, en su caso, oposición, se ejercerán por los interesados ante el Responsable del tratamiento. Si el encargado recibiese una petición de ejercicio de derechos deberá informar al interesado de la identidad del responsable para que se dirija al mismo.

SÉPTIMA.- Deber de devolución y no conservación.
Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
Aquellos datos que no se devuelvan, deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el encargado del tratamiento conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

OCTAVA.- Responsabilidad.
Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA.- Subcontratación.
El Responsable apodera al Encargado para que subcontrate, en nombre y por cuenta del responsable, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. A estos efectos, el Encargado informa al Responsable de la identidad de la sociedad a la cual pretende él subcontratar los servicios objeto de este contrato así como de los servicios que serían objeto de esta subcontratación. La validez del apoderamiento que el responsable en su caso otorgue (y que en tal caso deberá constar por escrito) quedará sujeta a la firma de un contrato escrito entre el Encargado y la empresa subcontratada, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el encargado en su propio nombre y el subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por el subcontratista.

DÉCIMA.- Fuero.
Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales más cercanos al domicilio del responsable del fichero, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

ANEXO. I

FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO.

1. INTRODUCCIÓN.

El presente anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros que trata el encargado, los datos concretos que trata, el nivel de seguridad a adoptar por el encargado y las finalidades que justifican el tratamiento.

2. ACCESO POR PARTE DEL ENCARGADO.

Nombre del fichero/s que trata el encargado, nivel de seguridad y datos identificativos que contiene:

Finalidad que justifica el tratamiento por parte del encargado:
Proveedor productos dentales. Proveedor productos dentales

Información adicional sobre el tratamiento:

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

_____ de _____ de _____

REUNIDOS

De una parte, ALBERTO RODRIGUEZ PALOMINO con NIF/CIF 51126442H, y domicilio social en C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
Representada por el Sr./a ALBERTO RODRIGUEZ PALOMINO con NIF 51126442H.

(En adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, JAVIER RODRIGUEZ SANTOS con NIF/CIF 50804718H, y domicilio social en Av. de América, 56 - 28028 - Madrid - MADRID.
Representada por el Sr./a con NIF .

(En adelante, el ENCARGADO DEL TRATAMIENTO).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla en la actualidad, prestando determinados servicios de: Asesor fiscal y contable. Asesor fiscal y contable
II. Que el RESPONSABLE DEL FICHERO ha contratado los servicios del ENCARGADO DEL TRATAMIENTO, consistentes en: Asesor fiscal y contable. Asesor fiscal y contable
III.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal del Responsable del fichero.
IV.- Que de conformidad con el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD), ambas partes convienen en suscribir el presente CONTRATO, el cual aceptan expresamente y de acuerdo a las siguientes:

ESTIPULACIONES

PRIMERA.- Definiciones.
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes.
Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física o en el caso de representantes de una persona jurídica o Administración serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento.
Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa manifestada por escrito del Responsable. Se prohíbe asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto.
El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.
Se adoptarán las medidas de nivel básico, medio o alto según corresponda (tal y como se indica en el anexo), de acuerdo con lo dispuesto en el RD 1720/2007, así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

Se atenderá a las siguientes reglas:
En caso de ser realizados los servicios que impliquen tratamiento de datos personales, objeto del presente contrato, en las propias instalaciones del Responsable, en equipos de hardware y software de ésta, así como cuando este sea remoto (Art. 82.1 RDLOPD). El Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales en las propias instalaciones del encargado del tratamiento, el mismo adoptará las medidas de seguridad correspondientes, elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RDLOPD).

SEXTA.- Ejercicio de derechos por los interesados.
Los derechos de acceso, rectificación, cancelación y, en su caso, oposición, se ejercerán por los interesados ante el Responsable del tratamiento. Si el encargado recibiese una petición de ejercicio de derechos deberá informar al interesado de la identidad del responsable para que se dirija al mismo.

SÉPTIMA.- Deber de devolución y no conservación.
Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
Aquellos datos que no se devuelvan, deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el encargado del tratamiento conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

OCTAVA.- Responsabilidad.
Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA.- Subcontratación.
El Responsable apodera al Encargado para que subcontrate, en nombre y por cuenta del responsable, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. A estos efectos, el Encargado informa al Responsable de la identidad de la sociedad a la cual pretende él subcontratar los servicios objeto de este contrato así como de los servicios que serían objeto de esta subcontratación. La validez del apoderamiento que el responsable en su caso otorgue (y que en tal caso deberá constar por escrito) quedará sujeta a la firma de un contrato escrito entre el Encargado y la empresa subcontratada, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el encargado en su propio nombre y el subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por el subcontratista.

DÉCIMA.- Fuero.
Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales más cercanos al domicilio del responsable del fichero, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

ANEXO. I

FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO.

1. INTRODUCCIÓN.

El presente anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros que trata el encargado, los datos concretos que trata, el nivel de seguridad a adoptar por el encargado y las finalidades que justifican el tratamiento.

2. ACCESO POR PARTE DEL ENCARGADO.

Nombre del fichero/s que trata el encargado, nivel de seguridad y datos identificativos que contiene:

Finalidad que justifica el tratamiento por parte del encargado:
Asesor fiscal y contable. Asesor fiscal y contable

Información adicional sobre el tratamiento:

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

_____ de _____ de _____

REUNIDOS

De una parte, ALBERTO RODRIGUEZ PALOMINO con NIF/CIF 51126442H, y domicilio social en C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID.
Representada por el Sr./a ALBERTO RODRIGUEZ PALOMINO con NIF 51126442H.

(En adelante, el RESPONSABLE DEL FICHERO).

Y de otra parte, SOFTWARE DEL SOL, S.A. con NIF/CIF B60260452, y domicilio social en Geolit Parque Científico y Tecnológico - 23620 - Mengíbar - JAEN.
Representada por el Sr./a con NIF .

(En adelante, el ENCARGADO DEL TRATAMIENTO).

Ambas partes se declaran, según intervienen, con capacidad suficiente para suscribir el presente CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS, y puestas previamente de acuerdo,

MANIFIESTAN

I.- Que el Encargado del tratamiento se halla en la actualidad, prestando determinados servicios de: Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servic. Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servicios en la Nube)
II. Que el RESPONSABLE DEL FICHERO ha contratado los servicios del ENCARGADO DEL TRATAMIENTO, consistentes en: Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servic. Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servicios en la Nube)
III.- Para el correcto cumplimiento de estos servicios, el Encargado trata datos de carácter personal del Responsable del fichero.
IV.- Que de conformidad con el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, RLOPD), ambas partes convienen en suscribir el presente CONTRATO, el cual aceptan expresamente y de acuerdo a las siguientes:

ESTIPULACIONES

PRIMERA.- Definiciones.
De conformidad con las definiciones recogidas en la LOPD, a los efectos de lo dispuesto en este Contrato, se entenderá por:

Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento y accede a los datos de carácter personal del responsable del fichero mediante contrato.

SEGUNDA.- De los datos facilitados por las partes.
Los datos personales facilitados por las partes del presente contrato, para los casos en que éstos sean una persona física o en el caso de representantes de una persona jurídica o Administración serán incorporados a un fichero cuya titularidad corresponde a cada una de las partes respectivamente. La finalidad de la recogida y tratamiento de la información es la gestión y mantenimiento de las relaciones comerciales o profesionales establecidas, así como la de mantenerle informado de nuevos servicios y ofertas. Asimismo ambas partes se dan por informadas de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, respecto de sus datos personales, pudiendo ejercitar estos derechos por escrito mediante carta dirigida al domicilio de la parte que corresponda.

TERCERA.- Finalidad que justifica el Tratamiento.
Las finalidades que justifican el acceso por parte del encargado a los datos del Responsable son exclusivamente las que se detallan en los anexos correspondientes.

Queda terminantemente prohibida la aplicación o utilización de los datos contenidos en estos ficheros con fines distintos a los aquí previstos, salvo autorización expresa manifestada por escrito del Responsable. Se prohíbe asimismo, la comunicación de los datos objeto de tratamiento, ni siquiera para su conservación a otras personas, salvo las cesiones legalmente establecidas y las que resulten necesarias para el cumplimiento de las finalidades de la relación contractual.

En el caso de que el Encargado destine los datos a finalidad distinta de las señaladas, los comunique o utilice incumpliendo las estipulaciones del presente contrato, será considerado a todos los efectos, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

CUARTA.- Deber de secreto.
El personal del Encargado del tratamiento tendrá la obligación de mantener el deber de secreto respecto a la información contenida en las bases de datos a las que, en su caso, hubieren tenido acceso, aun después de haber cesado su relación laboral con el Encargado.

Es obligación de este último comunicar este deber a su personal, así como cuidar de su cumplimiento.

QUINTA.- Seguridad de los datos.
Se adoptarán las medidas de nivel básico, medio o alto según corresponda (tal y como se indica en el anexo), de acuerdo con lo dispuesto en el RD 1720/2007, así como cuantas medidas de seguridad sean exigidas por las leyes y reglamentos destinadas a preservar el secreto, confidencialidad e integridad en el tratamiento de datos personales, con objeto de garantizar la seguridad de los datos de carácter personal y evitar su alteración, tratamiento o acceso no autorizado, así como a adoptar en el futuro.

Se atenderá a las siguientes reglas:
En caso de ser realizados los servicios que impliquen tratamiento de datos personales, objeto del presente contrato, en las propias instalaciones del Responsable, en equipos de hardware y software de ésta, así como cuando este sea remoto (Art. 82.1 RDLOPD). El Encargado deberá cumplir con las medidas de seguridad adoptadas por el Responsable para la protección de los datos personales, y que esta previamente le comunique.

En caso de ser realizado el servicio que implique tratamiento de datos personales en las propias instalaciones del encargado del tratamiento, el mismo adoptará las medidas de seguridad correspondientes, elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento (art. 82.2. RDLOPD).

SEXTA.- Ejercicio de derechos por los interesados.
Los derechos de acceso, rectificación, cancelación y, en su caso, oposición, se ejercerán por los interesados ante el Responsable del tratamiento. Si el encargado recibiese una petición de ejercicio de derechos deberá informar al interesado de la identidad del responsable para que se dirija al mismo.

SÉPTIMA.- Deber de devolución y no conservación.
Una vez finalizada la prestación contractual, los datos de carácter personal deben ser devueltos al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento, excepto cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
Aquellos datos que no se devuelvan, deberán destruirse adoptando las medidas de seguridad para evitar el acceso por parte de terceros. También podrá el encargado del tratamiento conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

OCTAVA.- Responsabilidad.
Ambas partes se comprometen a respetar, en el cumplimiento de las obligaciones que se derivan de este documento, toda la legislación y normativa que resulte aplicable, muy en particular, las obligaciones impuestas y determinadas por la Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal. Cada parte deberá hacer frente a la responsabilidad que se derive de su propio incumplimiento de dicha legislación y normativa.

NOVENA.- Subcontratación.
El Responsable apodera al Encargado para que subcontrate, en nombre y por cuenta del responsable, el tratamiento de los datos necesarios para la prestación de los servicios objeto de subcontratación. A estos efectos, el Encargado informa al Responsable de la identidad de la sociedad a la cual pretende él subcontratar los servicios objeto de este contrato así como de los servicios que serían objeto de esta subcontratación. La validez del apoderamiento que el responsable en su caso otorgue (y que en tal caso deberá constar por escrito) quedará sujeta a la firma de un contrato escrito entre el Encargado y la empresa subcontratada, que recoja términos análogos a los previstos en este contrato con el contenido íntegro establecido en el artículo 12 de la LOPD y a la asunción expresa por el encargado en su propio nombre y el subcontratista de una responsabilidad solidaria por cualquier incumplimiento de los términos del tratamiento por el subcontratista.

DÉCIMA.- Fuero.
Las partes, para la resolución de cualquier conflicto que pudiera surgir en la interpretación y aplicación del presente contrato, se someten a la jurisdicción de los Juzgados y Tribunales más cercanos al domicilio del responsable del fichero, con renuncia expresa al fuero que por Ley pudiera corresponderles.

Y en prueba de conformidad, las partes suscriben el presente contrato, en duplicado ejemplar y a un solo efecto, en la ciudad y fecha al inicio indicados.

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

ANEXO. I

FINALIDADES QUE JUSTIFICAN EL ACCESO POR PARTE DEL ENCARGADO.

1. INTRODUCCIÓN.

El presente anexo forma parte del contrato de acceso a datos suscrito entre las partes y detalla los ficheros que trata el encargado, los datos concretos que trata, el nivel de seguridad a adoptar por el encargado y las finalidades que justifican el tratamiento.

2. ACCESO POR PARTE DEL ENCARGADO.

Nombre del fichero/s que trata el encargado, nivel de seguridad y datos identificativos que contiene:

Finalidad que justifica el tratamiento por parte del encargado:
Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servic. Alojamiento de la web y del correo electrónico, y Servicios informáticos (software contabilidad, tienda virtual y servicios en la Nube)

Información adicional sobre el tratamiento:

Fdo. por el **RESPONSABLE DEL FICHERO** Fdo. por el **ENCARGADO DEL TRATAMIENTO**

11) PERSONAL

Documentos, impresos y recibos cumplimentados:
1. Impresos para trabajadores (si existieran).
2. Recibos del manual de usos y recomendaciones (si existieran).

Impreso para trabajadores

Nombre y Apellidos: **ALBERTO RODRIGUEZ PALOMINO**

D.N.I. / N.I.F.:

De conformidad con la Ley Orgánica 15/99 de Protección de datos, le informamos que los datos obtenidos para la formalización de su relación laboral con **ALBERTO RODRIGUEZ PALOMINO**, así como durante el desarrollo de la misma, forman parte del fichero de Personal, Nóminas y RRHH, titularidad de **ALBERTO RODRIGUEZ PALOMINO**. Estos datos son imprescindibles para formalizar su condición de empleado, así como para llevar a cabo las tareas internas de gestión de Recursos Humanos, Prevención de Riesgos, etc.

Mediante la firma del presente documento, y en virtud de lo establecido en el artículo 7 de la L.O.P.D., Vd. otorga consentimiento expreso para que proceda, en cumplimiento de los fines mencionados en el apartado anterior, al tratamiento de los datos personales facilitados.

En cualquier momento, Ud. podrá ejercitar los derechos de acceso, rectificación, oposición y, en su caso, cancelación, comunicándolo por escrito con indicación de sus datos a la dirección: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**
o al email:

Y para que así conste firmo la presente en ....., a.....de ..... de 20.....

Firmado: **ALBERTO RODRIGUEZ PALOMINO**

Impreso para trabajadores

Nombre y Apellidos: **MATILDE PALOMINO PAZ**

D.N.I. / N.I.F.:

De conformidad con la Ley Orgánica 15/99 de Protección de datos, le informamos que los datos obtenidos para la formalización de su relación laboral con **ALBERTO RODRIGUEZ PALOMINO**, así como durante el desarrollo de la misma, forman parte del fichero de Personal, Nóminas y RRHH, titularidad de **ALBERTO RODRIGUEZ PALOMINO**. Estos datos son imprescindibles para formalizar su condición de empleado, así como para llevar a cabo las tareas internas de gestión de Recursos Humanos, Prevención de Riesgos, etc.

Mediante la firma del presente documento, y en virtud de lo establecido en el artículo 7 de la L.O.P.D., Vd. otorga consentimiento expreso para que proceda, en cumplimiento de los fines mencionados en el apartado anterior, al tratamiento de los datos personales facilitados.

En cualquier momento, Ud. podrá ejercitar los derechos de acceso, rectificación, oposición y, en su caso, cancelación, comunicándolo por escrito con indicación de sus datos a la dirección: **C/ CEA BERMUDEZ 14, 5º-5 - 28003 - MADRID - MADRID**
o al email:

Y para que así conste firmo la presente en ....., a.....de ..... de 20.....

Firmado: **MATILDE PALOMINO PAZ**

Acuse de recibo

ALBERTO RODRIGUEZ PALOMINO

Acuse de Recibo de la documentación entregada al personal con acceso a los datos.

ALBERTO RODRIGUEZ PALOMINO, con NIF , en mi calidad de trabajador usuario con acceso a los datos de la empresa, por medio de la presente declaro haber recibido el manual de usos y recomendaciones, y me comprometo a cumplir con todas las obligaciones que de él se desprenden en relación a la normativa aplicable en materia de protección de datos de carácter personal.

Y para que así conste firmo la presente en ....., a.....de ..... de 20.....

Firmado: **ALBERTO RODRIGUEZ PALOMINO**

Acuse de recibo

ALBERTO RODRIGUEZ PALOMINO

Acuse de Recibo de la documentación entregada al personal con acceso a los datos.

MATILDE PALOMINO PAZ, con NIF , en mi calidad de trabajador usuario con acceso a los datos de la empresa, por medio de la presente declaro haber recibido el manual de usos y recomendaciones, y me comprometo a cumplir con todas las obligaciones que de él se desprenden en relación a la normativa aplicable en materia de protección de datos de carácter personal.

Y para que así conste firmo la presente en ....., a.....de ..... de 20.....

Firmado: **MATILDE PALOMINO PAZ**

12) AEPD

Apartado para archivar las cartas de Inscripción (Ficheros), modificación o supresión del fichero/s que remitirá la AEPD con el número identificativo de los fichero/s.