Annexos: Implantació de legislació internacional en matèria de protecció de dades

Javier Padilla Vázquez
Grau d'enginyeria informàtica
Administració de xarxes i sistemes operatius

Joan Ramon Esteban Grifoll
Pierre Bourdin

03/01/2018

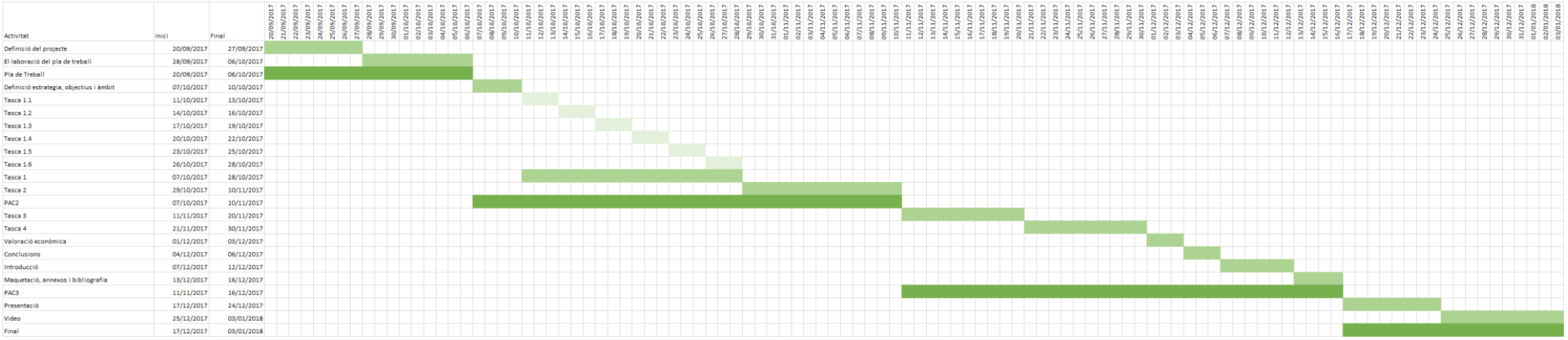
Índex

Annexos

Annex I. Cronograma

Tasca	Subtasca	Inici	Final	Activitat	Duració
Definició del projecte		20/09/2017	27/09/2017	Definir el tema del TFG	7 dies
El·laboració del pla de treball		28/09/2017	05/10/2017	El·laborar el pla de treball del TFG	10 dies
Pla de Treball		20/09/2017	06/10/2017	Entrega del Pla de Treball	17 dies
Definició estrategia, objectius i àmbit		07/10/2017	10/10/2017	Definir la estratègia, els objectius i l'àmbit del TFG	4 dies
	Tasca 1.1	11/10/2017	13/10/2017	Recopilar i analitzar legislació Espanya	3 dies
	Tasca 1.2	14/10/2017	16/10/2017	Recopilar i analitzar legislació Portugal	3 dies
	Tasca 1.3	17/10/2017	19/10/2017	Recopilar i analitzar legislació França	3 dies
	Tasca 1.4	20/10/2017	22/10/2017	Recopilar i analitzar legislació Regne Unit	3 dies
	Tasca 1.5	23/10/2017	25/10/2017	Recopilar i analitzar legislació Mèxic	3 dies
	Tasca 1.6	26/10/2017	28/10/2017	Recopilar i analitzar legislació EUA	3 dies
Tasca 1		07/10/2017	28/10/2017	Recopilar i analitzar les diferents legislacions	18 dies
Tasca 2		29/10/2017	10/11/2017	Identificar bases de dades	13 dies
PAC2		07/10/2017	10/11/2017	Entrega de la PAC2	35 dies
Tasca 3		11/11/2017	20/11/2017	Revisar nivell de compliment	10 dies
Tasca 4		21/11/2017	30/11/2017	Documentar proposta de compliment.	10 dies
Valoració econòmica		01/12/2017	03/12/2017	Realitzar valoració econòmica	3 dies
Conclusions		04/12/2017	06/12/2017	Analitzar les conclusions del projecte	3 dies
Introducció		07/12/2017	12/12/2017	Realitzar la introducció del TFG	6 dies
Maquetació, annexos i bibliografia		13/12/2017	16/12/2017	Maquetar, corregir i afegir annexos i bibliografia	4 dies
PAC3		11/11/2017	16/12/2017	Entrega de la PAC3	36 dies
Presentació		17/12/2017	24/12/2017	Realitzar diapositives de presentació	8 dies
Video		25/12/2017	03/01/2018	Realitzar el vídeo del TFG	10 dies
Final		17/12/2017	03/01/2018	Entrega Final	18 dies

Annex II. Diagrama de Gantt



Activitat	Inici	Final
Definició del projecte	20/09/2017	27/09/2017
El·laboració del pla de treball	28/09/2017	06/10/2017
Pla de Treball	20/09/2017	06/10/2017
Definició estrategia, objectius i àmbit	07/10/2017	10/10/2017
Tasca 1.1	11/10/2017	13/10/2017
Tasca 1.2	14/10/2017	16/10/2017
Tasca 1.3	17/10/2017	19/10/2017
Tasca 1.4	20/10/2017	22/10/2017
Tasca 1.5	23/10/2017	25/10/2017
Tasca 1.6	26/10/2017	28/10/2017
Tasca 1	07/10/2017	28/10/2017
Tasca 2	29/10/2017	10/11/2017
PAC2	07/10/2017	10/11/2017
Tasca 3	11/11/2017	20/11/2017
Tasca 4	21/11/2017	30/11/2017
Valoració econòmica	01/12/2017	03/12/2017
Conclusions	04/12/2017	06/12/2017
Introducció	07/12/2017	12/12/2017
Maquetació, annexos i bibliografia	13/12/2017	16/12/2017
PAC3	11/11/2017	16/12/2017
Presentació	17/12/2017	24/12/2017
Video	25/12/2017	03/01/2018
Final	17/12/2017	03/01/2018

Annex III. Document de seguretat de JPV Inversiones S.L.

[Protección de Datos de Carácter Personal]

DOCUMENTO DE SEGURIDAD

JPV INVERSIONES, S.L.

Versión 2.0

Diciembre 2015

ÍNDICE

1. OBJETO DEL DOCUMENTO.

El presente documento responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en el que se regulan entre otras, las medidas de seguridad para los ficheros y Tç ratamientos automatizados que contengan datos de carácter personal.

Los ficheros de datos a los que se refiere este documento se encuentran legalmente clasificados como nivel de seguridad **BÁSICO,** atendiendo a las condiciones descritas en el artículo 81.1 del Real Decreto citado, siendo por tanto aplicables todas las medidas de seguridad de nivel **BÁSICO** que se establecen en el Capítulo III del Título VIII, del citado Reglamento.

2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO.

JPV INVERSIONES, S.L., como consecuencia de las actividades desarrolladas dentro de su objeto social, trata información en ficheros que contienen datos de carácter personal que se hallan bajo su propia responsabilidad, incluyendo los sistemas de información soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en la normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

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

FICHERO	**TIPO DE SISTEMA**	**NIVEL DE SEGURIDAD**
CLIENTES Y/O PROVEEDORES (SAP R/3)	AUTOMATIZADO	BÁSICO
NÓMINAS Y RECURSOS HUMANOS (Dominio GrupoJPV)	AUTOMATIZADO	BÁSICO
SELECCIÓN DE PERSONAL (Dominio GrupoJPV)	AUTOMATIZADO	BÁSICO

VIDEOVIGILANCIA (Struxuware Data Center)	AUTOMATIZADO	BÁSICO
CONTRATOS Y ESCRITURAS (OpenKM)	AUTOMATIZADO	BÁSICO

En el **ANEXO I** (*"FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS")* se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los ficheros, aplicaciones y herramientas de actualización y consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos, gestionados por JPV INVERSIONES, S.L., o por cualquier otra empresa con la que haya suscrito un contrato de prestación de servicios que conlleve el tratamiento de los datos de carácter personal. 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 así como las aplicaciones y sistemas que los tratan, los equipos informáticos que las soportan y los locales donde se ubican.

En la actualidad JPV INVERSIONES, S.L., ha suscrito diversos contratos de prestación de servicios con terceras entidades actuando en calidad de prestatarias, que conllevan el tratamiento de datos de carácter personal de los ficheros de JPV INVERSIONES, S.L., por estas entidades.

3. RESPONSABLE DE SEGURIDAD.

JPV INVERSIONES, S.L., ha designado como Responsable de Seguridad en materia de protección de datos, en adelante, el Responsable de Seguridad, a CALPURNIA CONSULTING, S.L., quien se ocupará de la coordinación de todos los asuntos relacionados con esta materia dentro de la organización.

4. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO.

4.1. Identificación y autenticación.

Medidas y normas relativas a la identificación y autentificación del personal autorizado para acceder a los datos personales.

El Responsable del Fichero elabora una relación actualizada de usuarios que tengan acceso autorizado al sistema de información.

El Responsable de Seguridad custodia y actualiza la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información. Es competencia del Responsable de Seguridad que la atribución y asignación de contraseñas así como la custodia de la relación de usuarios se realice de forma que se garantice su confidencialidad e integridad.

El procedimiento seguido en JPV INVERSIONES, S.L., para la identificación y autenticación de los usuarios cuando intentan acceder al sistema o las aplicaciones, está basada en la combinación de un código de identificación de usuario y una contraseña, en red. A cada usuario le ha sido asignado un identificador único tanto para el acceso al sistema, como para el acceso a las aplicaciones, no existe un procedimiento para la asignación de contraseñas.

El control de acceso al sistema se limitará a tres (3) intentos. En caso de agotar los intentos, se procederá a la revocación del usuario que, para volver a acceder al sistema, deberá solicitarlo.

Los números de identificación y claves de acceso asignadas a cada usuario de la red corporativa del Responsable del Fichero son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de las mismas.

Las contraseñas de los usuarios autorizados son alfanuméricas, tienen una longitud mínima de ocho caracteres, se modifican con una periodicidad de 45 días y no es posible la repetición de las cinco últimas contraseñas introducidas. El administrador del sistema informático indica la obligatoriedad de cambio de contraseña en la cuenta del usuario y éste debe cambiarla en el plazo establecido. Durante el tiempo que estén vigentes, las contraseñas se almacenan de forma ininteligible.

Las contraseñas serán modificadas de acuerdo con el procedimiento técnico y de organización establecido por el Responsable de Seguridad Técnico en cada caso y que dependerá de cada sistema y de cada aplicación en concreto. Solamente el Responsable de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos o recursos.

Este proceso de caducidad de contraseñas lo realiza el Responsable de Seguridad, por medio de los profesionales designados al efecto que tienen las potestades para el acceso a los datos estrictamente necesarios para el desempeño de su trabajo y están sometidos a las mismas obligaciones que el personal de la empresa en materia de protección de datos, especialmente a la de secreto respecto de los datos personales que hubiese podido conocer con motivo de la prestación del servicio. Las contraseñas se almacenan de forma ininteligible y cifrada. En el entorno de red se utiliza un mecanismo "desafío-respuesta" HMAC-MD5, de forma que las contraseñas nunca viajan por la red para la transmisión de la información.

Las operaciones susceptibles de seguimiento que se realicen en la red corporativa del Responsable del Fichero quedan registradas en los archivos de registro del servidor (que proporcionan constancia de los accesos a los ficheros de la empresa mediante identificación del usuario que accede, la fecha y la hora del acceso y si éste ha sido autorizado o denegado). El uso del usuario y la contraseña asignados a cada persona implica la aceptación, como documento probatorio de la operación efectuada, de los registros generados en dichos archivos *LOG* y almacenados en el sistema informático de la empresa. Salvo prueba en contrario, se presume que los actos que se lleven a cabo con el usuario y la contraseña asignados han sido realizados en realidad por la persona titular de los mismos.

El Responsable del Fichero posee los mecanismos necesarios para obtener una relación actualizada de los usuarios que tienen acceso autorizado a los sistemas de información de la compañía y establece los procedimientos de identificación y autenticación necesarios para garantizar la seguridad de dicho acceso.

El mecanismo de identificación se basa en la asignación de usuarios a cada una de las personas que acceden a los sistemas de información y el mecanismo de autenticación se basa en la existencia de contraseñas.

Cuando el tratamiento se realiza por el encargado del tratamiento mediante acceso remoto a los sistemas del Responsable del Tratamiento, se ha establecido una limitación, cuyo procedimiento es la incorporación de datos a los sistemas o soportes distintos de los del responsable.

4.2. Gestión de soportes.

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en los locales bajo el control tanto del encargado del tratamiento como del responsable del tratamiento, lugares de acceso restringido al que solo tendrán acceso las personas con autorización.

4.3. Ficheros temporales o copias de trabajo de documentos.

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo

a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

4.4. Copias de respaldo y recuperación.

Se realizarán copias de respaldo y recuperación, salvo que no se hubiese producido ninguna actualización de los datos, este procedimiento se realizará con una periodicidad diaria.

La copia de respaldo se realiza en un soporte extraíble que es depositado en una caja de seguridad ignífuga. Con esta medida se evita la necesidad de traslado de los mismos a otra ubicación fuera de las instalaciones.

En caso de traslado de los soportes físicos, éstos deberán cifrarse para evitar el acceso a la información que contienen.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizan su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, así como se realizan cifradas para que en caso de sustracción o pérdida sea totalmente imposible descifrarlas. El sistema de copia de seguridad identifica los soportes mediante un sistema de etiquetado.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

4.5. Control de acceso.

Los usuarios tanto en la red como en los puestos individuales, deben identificarse y autenticar el acceso a sistemas y aplicaciones, mediante clave de usuario y contraseña, para poder acceder de forma autorizada.

La introducción de una clave distinta a la autorizada impide el acceso a la red, ofreciendo la posibilidad de subsanar errores de teclado, con un límite de tres (3) accesos no autorizados.

El Responsable de Seguridad es el encargado del mantenimiento de los usuarios del sistema y aplicaciones en base a los criterios establecidos por la Dirección. Todo usuario estará obligado a bloquear su equipo en el momento en que se va a ausentar de su puesto de trabajo, es decir el equipo deberá estar configurado para que se bloquee automáticamente tras un cierto tiempo de inactividad.

Con el alta de la contraseña de cada usuario se identifica qué grupo de acceso debe ser asignado, tanto para datos como para el acceso a determinadas aplicaciones.

5. GESTIÓN DE INCIDENCIAS.

5.1. Objeto.

Al no existir en JPV INVERSIONES, S.L. un protocolo destinado a atender cualquier eventualidad que afecte a la seguridad de los datos, el procedimiento será acudir a los asesores informáticos. No obstante, JPV INVERSIONES, S.L. recogerá cuantas incidencias de seguridad se produzcan sobre los datos que trata, tales como:

- ✓ Incidencias que afecten a la identificación y autentificación de los usuarios.
- ✓ Incidencias que afecten a los derechos de acceso a los datos.
- ✓ Incidencias que afecten a la gestión de soportes.
- ✓ Incidencias que afecten a los procedimientos de copias de seguridad y recuperación.
- ✓ 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.

En este Documento de Seguridad se establecen los mecanismos de actuación por parte de los usuarios de los sistemas de información de JPV INVERSIONES, S.L., para la comunicación de las incidencias.

5.2. Ámbito de aplicación.

Al igual que en caso de los ficheros temporales, el Reglamento de Medidas de Seguridad tampoco define el concepto de incidencia. Únicamente se indica como incidencia de seguridad de manera explícita, los procesos de recuperación de datos. JPV INVERSIONES, S.L. intentará contemplar en el sentido más amplio del concepto de incidencia, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de las medidas físicas y lógicas que puedan afectar a su disponibilidad y 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 afectan a la identificación y autentificación 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 afectan a la revisión de soportes:

  - ✓ Comunicación de pérdida de soportes.
  - ✓ Comunicación de localización de soportes en lugares inadecuados.
  - ✓ Errores de contenido en los soportes recibidos.

- Incidencias que afectan a los procedimientos de copias de salvaguardia y recuperación:

  - ✓ Errores en los procesos de realización de copias de salvaguardia.
  - ✓ 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 todos los usuarios de los sistemas de información de JPV INVERSIONES, S.L., empleados y colaboradores externos.

5.3. Responsabilidades.

- El Responsable de Seguridad es responsable de la redacción y mantenimiento de este procedimiento, así como de su custodia y archivo.
- Todos los usuarios de JPV INVERSIONES, S.L., deben informar de cualquier incidencia producida en materia de seguridad.
- El Responsable de Seguridad debe ocuparse del seguimiento de las incidencias en materia de protección de datos de carácter personal.

5.4. Comunicación de incidencias.

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. La difusión de la Circular adjunta a este Documento de Seguridad en el **ANEXO IV** implica que todos los usuarios de JPV INVERSIONES, S.L., deben ser conocedores de su obligación de comunicar las incidencias en materia de seguridad al Responsable de Seguridad. Todas las comunicaciones deberán efectuarse al Responsable de Seguridad indicando el momento en que se detectaron y utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente. Para que quede constancia de la comunicación, el usuario, además, lo comunicará por correo electrónico.

5.5. Registros.

El Responsable de Seguridad procederá a incluir las incidencias en el registro y, si afectan a la seguridad de los datos de carácter personal, las marcará como tales. 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 contará con los siguientes campos:

- Tipo de incidencia.
- Momento en que se ha producido o se ha detectado la incidencia.
- Persona que la notifica.
- Persona a la que se le notifica.
- Efectos causados por la misma

También se llevará un registro de resolución de incidencias, que recoja la información sobre las medidas adoptadas. En el caso en que la incidencia implique la ejecución de un proceso de recuperación de datos, el registro de resolución de incidencias contendrá además, la siguiente información:

- Persona que ejecutó el proceso.
- Datos restaurados.
- En su caso, datos que fue necesario grabar manualmente para su recuperación.

En el **ANEXO II** se recogen los modelos para proceder al registro de incidencias y de su resolución.

6. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL.

Con el objeto de dar el debido cumplimiento a la normativa de protección de datos de carácter personal, el Responsable del Fichero impone a su personal el cumplimiento de las siguientes obligaciones, las cuales deberán ser conocidas, aceptadas y respetadas por todo el personal.

6.1. Obligaciones del personal.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como a las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

- JPV INVERSIONES, S.L. emitirá una circular donde se recogerán las principales obligaciones en materia de seguridad sobre datos de carácter personal, incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de los recursos informáticos para otras finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral, así como la obligación de mantener el deber de secreto sobre todos los datos tratados con motivo del desempeño de su puesto de trabajo y de no comunicar los referidos datos a ninguna otra persona o entidad sin la autorización pertinente.

Las normas aplicables al personal con acceso a datos de carácter personal se recogen en el **ANEXO III,** cuyo contenido y detalle se actualiza periódicamente en función de las decisiones empresariales al respecto y de los cambios normativos o jurisprudenciales que, en su caso, se produzcan.

6.2. Información al personal.

El Reglamento 1720/2007, dispone la obligación de adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

El Responsable de Seguridad ha sido personalmente informado de las funciones que le han sido asignadas y que figuran en el apartado siguiente del presente Documento de seguridad.

6.3. Obligaciones del Responsable del Fichero o responsable del tratamiento.

Además de las que a continuación se detallan, cualesquiera otras obligaciones que le sean atribuidas por la normativa o por el presente Documento:

- ✓ Notificar a la Agencia Española de Protección de Datos los ficheros de datos personales del Responsable del Fichero.
- ✓ Velar por el cumplimiento de todos los requisitos establecidos en la LOPD y en su Reglamento de desarrollo.
- ✓ Redactar, establecer, actualizar y comprobar la aplicación y el cumplimiento del Documento de Seguridad.
- ✓ Adaptar el documento de seguridad a la normativa vigente.

- ✓ Describir los sistemas de información que realizan el tratamiento de los datos personales del Responsable del Fichero.
- ✓ Establecer los criterios que el Responsable de Seguridad debe seguir al realizar la función de conceder, alterar o anular el acceso autorizado a los datos y recursos.
- ✓ Establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- ✓ Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.
- ✓ Autorizar la salida de soportes que contengan datos de carácter personal fuera de los locales en los que esté ubicado el soporte.
- ✓ 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 se ha autorizado.
- ✓ Establecer los criterios para la definición de los derechos de acceso de los usuarios.

6.4. Obligaciones del Responsable de Seguridad.

Además de las que a continuación se detallan, cualesquiera otras obligaciones que le sean atribuidas por la normativa o por el presente Documento:

- ✓ Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.
- ✓ Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por el Responsable del Fichero.
- ✓ Determinar el ámbito del Documento de Seguridad.
- ✓ Determinar y describir los recursos informáticos a los que se aplicará el Documento de Seguridad.
- ✓ Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
- ✓ Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos.
- ✓ Comprobar el cumplimiento de la periodicidad establecida para la realización de copias de respaldo.
- ✓ Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al sistema informático del Responsable del Fichero con especificación del nivel de acceso que tiene cada usuario.
- ✓ Establecer y comprobar la aplicación del procedimiento de identificación y autentificación de usuarios.
- ✓ Establecer y comprobar la aplicación del procedimiento de asignación distribución y almacenamiento de contraseñas.
- ✓ Comprobar el mantenimiento de la confidencialidad de las contraseñas de los usuarios.
- ✓ Establecer y comprobar la aplicación de un procedimiento de cambio periódico de las contraseñas de los usuarios.

- ✓ Establecer y comprobar la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma inteligible.
- ✓ Conceder, alterar o anular el acceso autorizado a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.
- ✓ Establecer y comprobar la aplicación de un sistema que permita identificar, inventariar y almacenar en un lugar seguro de los soportes informáticos que contienen datos de carácter personal.
- ✓ Autorizar la entrada y salida de soportes informáticos que contienen datos de carácter personal.
- ✓ Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas, para el establecimiento de las correspondientes sanciones.
- ✓ Coordinar y controlar las medidas definidas en el Documento de Seguridad.
  Traslado de documentación.

7. CONTRATOS DE PRESTACIÓN DE SERVICIOS.

En este apartado aparece una relación exhaustiva de los datos tratados por terceros, como consecuencia de un contrato de prestación de servicios. A continuación se presenta un modelo de tabla para recoger esta información:

PRESTADOR DEL SERVICIO	FINALIDADES	DATOS FACILITADOS	LUGAR DE TRABAJO	SISTEMA DE TRATAMIENTO
CALPURNIA CONSULTIG, S.L.	CLIENTES Y PROVEEDORES	CLIENTES Y PROVEEDORES	JPV INVERSIONES, S.L. (Avenida del Percebe, s/n, 08, 08080, Barcelona)	MIXTO

8. FLUJO INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL

JPV INVERSIONES, S.L.U. es la sociedad matriz de un grupo de sociedades de carácter inmobiliario titulares, directa e indirectamente, de inmuebles y/o participaciones sociales ubicadas en estados diferentes a España, tanto dentro como fuera del Espacio Común Europeo.

La actividad de JPV INVERSIONES, S.L.U. y sus sociedades filiales se centra de forma exclusiva en datos de personas jurídicas no efectuando en ningún caso flujo internacional de datos de carácter personal, salvo a los meros efectos analíticos de inversión y decisión de inversión.

9. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a la normativa vigente en cada momento sobre protección de datos de carácter personal.

ANEXO I FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS	DOC. DE SEGURIDAD VERSIÓN 2.0

En el presente Anexo se recoge información relativa a los ficheros responsabilidad de JPV INVERSIONES, S.L. que se hallan inscritos en el Registro General de Protección de Datos, indicando el entorno donde se encuentran ubicados y las aplicaciones que los gestionan.

NOMBRE DEL FICHERO	DATOS TRATADOS	FECHA DE INSCRIPCIÓN	CÓDIGO DE INSCRIPCIÓN	UBICACIÓN Y MODO DE TRATAMIENTO	NIVEL DE SEGURIDAD
CLIENTES Y/O PROVEEDORES (SAP R/3)	Datos de clientes y suministradores de la sociedad			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	BÁSICO
NÓMINAS Y RECURSOS HUMANOS (Dominio GrupoJPV)	Datos del personal de la sociedad			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	BÁSICO
SELECCIÓN DE PERSONAL (Dominio GrupoJPV)	Datos de empleados y aspirantes a puestos de trabajo			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	BÁSICO
VIDEOVIGILANCIA (Struxuware Data Center)	Imágenes registradas en las instalaciones			**Ubicación:** Responsable del fichero **Modo de tratamiento: Mixto**	BÁSICO
CONTRATOS Y ESCRITURAS (OpenKM)	Contratos y escrituras de la sociedad			**Ubicación:** Responsable del fichero **Modo de tratamiento: Mixto**	BÁSICO

ANEXO II REGISTRO DE INCIDENCIAS	DOC. DE SEGURIDAD VERSIÓN 2.0

NOTIFICACIÓN Y REGISTRO DE INCIDENCIAS		
Numero de incidencia:		
Fecha de notificación:	Hora:	
Usuario que realiza la notificación:		
Personas a las que se le comunica la incidencia:		
DESCRIPCION DE LA INCIDENCIA		
Fecha de la incidencia:	Hora:	
Tipo de incidencia (intrusión, pérdida de datos, etc.):		
Descripción detallada de la incidencia:		
Posibles efectos de la incidencia		
Firma del notificante:	Firma receptor:	
REGISTRO DE RESOLUCION DE INCIDENCIAS		
Numero de incidencia:		
Medidas adoptadas y pasos realizados:		
Resultado de las medidas:		
Fecha de resolución:		
RECUPERACION DE DATOS:		
Procedimiento realizado:		
Fecha de realización:		
Datos restaurados:		Datos grabados manualmente:
Persona que realiza el procedimiento:		
Fecha y lugar:	Firma del Responsable del Fichero:	

ANEXO III NORMAS APLICABLES A PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL	DOC. DE SEGURIDAD VERSIÓN 2.0

El Documento de Seguridad de JPV INVERSIONES, S.L. enumera detalladamente las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal con arreglo a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y al Real Decreto 1720/2007, por el que se aprobó el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El personal sobre el que recaen dichas obligaciones y funciones podrá acceder al contenido del Documento de Seguridad, siempre previa solicitud al Responsable de Seguridad. No obstante, y a efectos aclaratorios, en el presente Anexo se recogen las principales obligaciones en materia de protección de datos de carácter personal para conocimiento directo de los trabajadores, quienes deberán dar íntegro cumplimiento a las mismas:

OBLIGACIONES DEL PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL

CONTRASEÑAS:

1) Las contraseñas de los usuarios serán personales e intransferibles.
2) Las contraseñas deberán ser alfanuméricas y tener una longitud máxima de ocho caracteres.
3) Las contraseñas caducarán cada 45 días, momento en el cual el usuario deberá designar una nueva contraseña que no podrá coincidir con las últimas cinco contraseñas introducidas.

EQUIPOS INFORMÁTICOS:

4) Se prohíbe al personal la instalación de cualquier tipo de aplicación en los equipos informáticos sin autorización previa.
5) Se prohíbe la utilización de los equipos y soportes informáticos para finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral.
6) Los usuarios estarán obligados a bloquear su equipo en el momento de ausentarse de su puesto de trabajo, requiriendo la introducción de usuario y contraseña para volver a acceder al equipo.

SECRETO Y CONFIDENCIALIDAD:

7) Los usuarios deberán mantener el secreto sobre todos los datos tratados con motivo del desempeño de su puesto de trabajo.
8) No podrán, asimismo, comunicar los referidos datos a ninguna otra persona o entidad, salvo autorización pertinente.

INCIDENCIAS:

9) Los usuarios deberán informar al Responsable de Seguridad sobre cualquier incidencia producida en materia de seguridad de acuerdo con el procedimiento establecido en el punto 4.4 del Documento de Seguridad.
10) Los usuarios deberán participar en la implantación y seguimiento de la política de seguridad mediante la firma de la Circular que les será entregada a cada uno.

OTROS:

11) Todas las obligaciones anteriores deberán mantenerse, incluso tras la extinción de la relación laboral con JPV INVERSIONES, S.L.
12) El trabajador será responsable tanto frente a JPV INVERSIONES, S.L., como frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores, pudiendo JPV INVERSIONES, S.L. reclamar las indemnizaciones pertinentes.

Para cualquier aclaración al respecto se puede contactar con la Responsable de Seguridad, CALPURNIA CONSULTING.

ANEXO IV CIRCULAR A LOS TRABAJADORES	DOC. DE SEGURIDAD VERSIÓN 2.0

Nombre: _____ NIF: _____

En mi capacidad de empleado (ya sea fijo, o temporal) y en consideración de la relación laboral que mantengo con JPV INVERSIONES, S.L., así como del acceso que se me permite a sus Bases de Información, constato que:

- Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja JPV INVERSIONES, S.L. En concreto he leído, entiendo y me comprometo a cumplir los Procedimientos de Seguridad de los Sistemas de Información que corresponden a mi función en la empresa (Descritos en el Documento de Seguridad).

- Entiendo que el incumplimiento de cualesquiera de las normas aplicables al personal con acceso a datos de carácter personal incluidas todas ellas en el Documento de Seguridad de JPV INVERSIONES, S.L., intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empres y la posible reclamación por parte de la misma de los daños causados.

En_____, a __ de_____ de 20__.

Firma,

El empleado/a

ANEXO V ACUERDO DE CONFIDENCIALIDAD (TRABAJADORES Y ENCARGADOS DEL TRATAMIENTO)	DOC. DE SEGURIDAD VERSIÓN 2.0

ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO:

En _____, a___ de _____ de 20__.

ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO

REUNIDOS

De una parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

De otra parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

INTERVIENEN

La primera lo hace en nombre y representación de JPV INVERSIONES, S.L., con domicilio social en Avda. del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº B-00000001, en su calidad de _____ de la sociedad.

La segunda lo hace en nombre y representación de _____, con domicilio social en _____, y CIF nº _____, en su calidad de _____ de la sociedad (en adelante, el "**Encargado del Tratamiento**").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que las Partes se hallan vinculadas por un contrato de prestación de servicios de fecha ___ de _____ de _____, en virtud del cual el Encargado del Tratamiento se obligaba al tratamiento de datos por cuenta del responsable de los ficheros, esto es JPV INVERSIONES, S.L.

II.- Que, el artículo 10 de La Ley Orgánica de Protección de Datos de Carácter Personal (en adelante, "LOPD"), en su artículo 10 refiriéndose al Deber de Secreto, establece la obligación al

secreto profesional y al deber de guardar los datos, por parte de todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal.

III.- Que, en cumplimiento de lo establecido en la LOPD, las Partes suscriben el presente Acuerdo de Confidencialidad, de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- INFORMACIÓN CONFIDENCIAL.

Se considerará información confidencial a toda aquella a la que el Responsable del Tratamiento acceda con motivo de la realización de sus funciones y obligaciones, independientemente del soporte en el que esté contenida.

SEGUNDA.- OBLIGACIÓN DE SECRETO.

El Encargado del Tratamiento no podrá revelar a persona alguna ajena a JPV INVERSIONES, S.L., cualesquiera datos confidenciales, protegidos por la LOPD, a los que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

TERCERA.- USO DE LA INFORMACIÓN.

El Encargado del Tratamiento se limitará a utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en relación al contrato de prestación de servicios suscrito con JPV INVERSIONES, S.L.. No pudiendo disponer de tal información de ninguna otra forma o con otra finalidad.

CUARTA.- DURACIÓN.

Las obligaciones contenidas en el presente Acuerdo seguirán rigiendo de manera indefinida en el tiempo, aun tras la finalización de la relación contractual entre las Partes.

QUINTA.- INCUMPLIMIENTOS.

En caso de incumplimiento, el Responsable del Tratamiento se hace responsable ante cualquier daño que pueda ocasionar tanto a JPV INVERSIONES, S.L., como a terceros, debiendo resarcir a JPV INVERSIONES, S.L., de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y en prueba de conformidad, ambas partes firman el presente documento por duplicado, a un solo efecto y en lugar y fecha ut supra.

_____	_____
Fdo. D./Dña. _____	Fdo. D./Dña._____
EL RESPONSABLE DEL TRATAMIENTO	**JPV INVERSIONES, S.L.**

ACUERDO DE CONFIDENCIALIDAD CON TRABAJADORES:

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD. 15/99), en su artículo 10 refiriéndose al Deber de Secreto, establece que:

> "*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*

Como consecuencia de lo anterior, el abajo firmante, D/Dña _____, con DNI _____, y domicilio en _____ en el marco de la **relación laboral** que le une con JPV INVERSIONES, S.L., se compromete a:

PRIMERA.- Teniendo en cuenta que los datos de carácter personal, tanto automatizados como en soporte papel, a los cuales va a tener acceso, en muchos casos son considerados por la legislación vigente en materia de protección de datos, como especialmente protegidos, se establece en la presente cláusula la obligatoriedad de no revelar a persona alguna ajena a JPV INVERSIONES, S.L., la información referente a la que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones del abajo firmante o a las impuestas por las leyes o normas que resulten de aplicación; o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

SEGUNDA.- Utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en JPV INVERSIONES, S.L., y no disponer de ella de ninguna otra forma o con otra finalidad.

TERCERA.- No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado, y que no sea necesaria para el desempeño de sus funciones en JPV INVERSIONES, S.L.

CUARTA.- Cumplir, en el desempeño de sus funciones en JPV INVERSIONES, S.L., la normativa vigente relativa a la Protección de Datos de Carácter Personal y, en particular la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y disposiciones complementarias o cualquier otra norma que la sustituya en el futuro.

QUINTA.- Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral que le une con JPV INVERSIONES, S.L.

SEXTA.- El trabajador transmite a JPV INVERSIONES, S.L. que adquiere, todos los derechos que pudieran corresponderle sobre los programas de ordenador, aplicaciones informáticas y bases de datos desarrolladas por aquel en el marco de su relación laboral, trabajos, informes, estando estos realizados utilizando medios y recursos a los que haya tenido acceso con ocasión de su vinculación con JPV INVERSIONES, S.L.

SÉPTIMA.- El trabajador, se compromete a guardar deber de secreto, en concordancia con lo estipulado en el artículo 10 de la LOPD, de la información a la que tenga acceso en el desempeño de sus funciones en JPV INVERSIONES, S.L.

OCTAVA.- El abajo firmante se hace responsable frente a JPV INVERSIONES, S.L., y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a JPV INVERSIONES, S.L., de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y para que surta plenos efectos, firmo la presente declaración,

En _____, a___ de _____ de 20__.

Firma del trabajador

Fdo.: D/Dña:

ANEXO VI INVENTARIO DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

En el presente Anexo se inventariarán los soportes que contengan datos de carácter personal de manera detallada, de acuerdo con el siguiente cuadro de información:

NOMBRE DE LA ETIQUETA	CONTENIDO DEL SOPORTE	TIPO DE SOPORTE	UBICACIÓN	FRECUENCIA DE UTILIZACIÓN	PROCEDIMIENTO DE DESTRUCCIÓN DEL SOPORTE	FECHA DE ALTA Y DE BAJA	CIFRADO
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □

En caso de soportes cuya especial naturaleza impida su correcto registro según lo establecido más arriba, se procederá a dejar constancia de tal situación, indicando los aspectos que se puedan especificar.

ANEXO VII REGISTRO DE ENTRADA Y SALIDA DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

REGISTRO DE ENTRADA

Nº DE SOPORTES	FECHA	HORA	TIPO DE SOPORTE	REMITENTE	MODO DE ENVÍO	CONTENIDO	RECEPTOR	DEPARTAMENTO	ESTADO

REGISTRO DE SALIDA

Nº DE SOPORTES	FECHA	HORA	TIPO DE SOPORTE	DESTINATARIO	MODO DE ENVÍO	CONTENIDO	EMISOR	DEPARTAMENTO

ANEXO VIII SALIDAS AUTORIZADAS DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

La dirección de JPV INVERSIONES, S.L., ha aprobado la relación de salidas periódicas de soportes que contienen datos de carácter personal que han sido autorizados por la entidad.

A continuación se presenta la relación que será actualizada cada vez que se produzcan modificaciones al respecto.

DATOS ENVIADOS	DESTINATARIO	PERIODICIDAD

ANEXO IX CONTROL DE ENTRADA / SALIDA DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

CONTROL DE ENTRADA / SALIDA DE SOPORTES

Referencia Nº _____ **Fecha y hora de la operación** _____

ENTRADA ☐ **SALIDA** ☐ **DEVOLUCIÓN** ☐

TIPO DE SOPORTES _____ **NÚMERO DE SOPORTES** _____

NÚMERO DE IDENTIFICACIÓN DEL SOPORTE _____

CONTENIDO _____

FINALIDAD _____

FICHERO DEL QUE PROCEDEN LOS DATOS _____

IDENTIFICACIÓN DE LA DELEGACIÓN / ENTIDAD (ORIGEN / DESTINO)

NOMBRE DELEGACIÓN / ENTIDAD _____

DESTINATARIO _____

DIRECCIÓN _____

TELEFONO DE CONTACTO _____

DATOS DEL RESPONSABLE DE LA ENTREGA / RECEPCIÓN (AUTORIZADO)

NOMBRE Y APELLIDOS _____

CARGO / PUESTO _____

PERSONA QUE AUTORIZA _____

FECHA DE ENTRADA _____ /_____ / _____

FECHA DE SALIDA _____ / _____ /_____

FECHA DE DEVOLUCIÓN _____ /_____ /_____

FORMA Y PRECAUCIONES DE ENVÍO _____

OBSERVACIONES _____

_____

_____

Fdo. _____

ANEXO X MODELO DE CONTRATO DE ENCARGADO DEL TRATAMIENTO DE LOS DATOS POR CUENTA DE TERCEROS.	DOC. DE SEGURIDAD VERSIÓN 2.0

En _____, a __ de _____ de 20__.

CONTRATO DE ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

REUNIDOS

De una parte, D./Dña._____, con D.N.I_____, que actúa en nombre y representación de JPV INVERSIONES, S.L., con domicilio social en Avda. del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº B-00000001, en su calidad de _____, (en adelante, "EL RESPONSABLE DEL FICHERO").

Y de otra parte, D./Dña._____, con D.N.I_____, que actúa en nombre y representación de (SOCIEDAD), con domicilio social en_____, Y con C.I.F. nº _____, en su calidad de _____, (en adelante, "EL ENCARGADO DEL TRATAMIENTO").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que ambas Partes se hallan vinculadas por un contrato de prestación de servicios, en virtud del cual la (SOCIEDAD) tiene acceso a datos de carácter personal protegidos por la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (en adelante, "LOPD").

II.- Que, las Partes han acordado la suscripción del presente contrato de Acceso a los Datos por Cuenta de Terceros en cumplimiento con lo dispuesto en el artículo 12 de la LOPD, para el tratamiento de dichos datos de carácter personal, cumpliendo con los requisitos legales correspondientes y de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- DEFINICIONES.

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.

SEGUNDA.- OBJETO.

El objeto del presente contrato es el tratamiento por parte de EL ENCARGADO DEL TRATAMIENTO de los datos personales relativos a: _____ con la finalidad de poder realizar los servicios contratados, para lo cual previamente deberá ésta poner a disposición del encargado del tratamiento dichos datos personales.

Dicho tratamiento se realizará de conformidad con lo establecido en la LOPD y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante "RLOPD"), o normativa que los sustituya.

TERCERA.- DATOS A LOS QUE SE DA ACCESO Y NIVEL DE SEGURIDAD.

Los datos personales que forman parte de los ficheros del RESPONSABLE DEL FICHERO, a los que tendrá acceso el encargado del tratamiento son los siguientes:

- Fichero: _____.
    - Datos afectados por el tratamiento: _____.
    - Nivel de seguridad: _____.
- Fichero: _____.
    - Datos afectados por el tratamiento: _____.
    - Nivel de seguridad: _____.

CUARTA.- OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO.

4.1 EL ENCARGADO DEL TRATAMIENTO solamente tratará los datos que se le han encomendado conforme a las instrucciones del responsable del fichero.

4.2 Los datos facilitados no se aplicarán ni utilizarán con una finalidad diferente a la que figura en este documento, ni EL ENCARGADO DEL TRATAMIENTO los comunicará, ni siquiera a efectos de su conservación, a terceros.

4.3 EL ENCARGADO DEL TRATAMIENTO y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de los datos que les han sido confiados para su tratamiento.

4.4 EL ENCARGADO DEL TRATAMIENTO deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Las medidas de seguridad que deberán ser observadas dependerán del nivel de seguridad de los datos objeto de tratamiento, por ello, dichas medidas podrán ser de nivel básico, medio o alto, según lo estipulado en la LOPD y el RLOPD.

4.5 En caso de resolución del presente contrato, los datos serán destruidos en su totalidad o devueltos al RESPONSABLE DEL FICHERO, teniendo en cuenta los distintos soportes o documentos donde estos puedan constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc.

4.6 Una vez se haya realizado la operación mencionada en el punto anterior, EL ENCARGADO DEL TRATAMIENTO se compromete a entregar una declaración por escrito al RESPONSABLE DEL FICHERO donde conste que así se ha realizado.

4.7 Será de aplicación en todo caso, en lo no previsto en este contrato, la normativa vigente en materia de protección de datos personales.

4.8 En el caso de que EL ENCARGADO DEL TRATAMIENTO incumpla con las obligaciones antes establecidas, pasará a tener la consideración de responsable del tratamiento o fichero, respondiendo de las infracciones en que hubiera incurrido personalmente.

QUINTA.- DURACIÓN Y RESOLUCIÓN DEL CONTRATO.

El presente contrato se considera accesorio del contrato de prestación de servicios de existente entre las partes, por lo que su duración y extinción queda supeditada al mismo.

SEXTA.- LEY APLICABLE Y FORO.

El presente contrato se regirá e interpretará conforme a la legislación española vigente, en aquello que no esté expresamente regulado, sometiéndose las partes, para todas las controversias que pudieran surgir en relación con el mismo, a la competencia de los Juzgados y Tribunales de la ciudad de A “ “, con renuncia a cualquier otro foro que les pudiera corresponder.

Y en prueba de su conformidad, firman las partes el presente contrato en duplicado ejemplar y a un sólo efecto, en lugar y fecha señalados en el encabezamiento.

JPV INVERSIONES, S.L. **(_____)**

EL RESPONSABLE DEL FICHERO **EL ENCARGADO DEL TRATAMIENTO**

ANEXO XI CLÁUSULA LOPD PARA E-MAILS/FAX	DOC. DE SEGURIDAD VERSIÓN 2.0

La información contenida en este mensaje y en cualquier archivo o documento que se adjunte al mismo es confidencial y privilegiada.

Esta dirigida exclusivamente para el uso privado del destinatario y no debe ser diseminada o utilizada por otra personal.

JPV INVERSIONES, S.L. no garantiza la transmisión de mensajes electrónicos en forma segura y libre de errores debido a que la información puede ser interceptada, dañada, perdida, destruida, pueda llegar tarde, incompleta, o conteniendo virus.

JPV INVERSIONES, S.L. no acepta responsabilidad por cualquier error u omisión en el contenido de este mensaje, que puede surgir como resultado de la transmisión de este mensaje electrónico.

Los empleados y usuarios del sistema de correo electrónico/fax están expresamente advertidos de no crear o enviar enunciados difamatorios y de no cometer ninguna violación a los derechos de autor u otras disposiciones legales, a través de comunicaciones por mensaje electrónico/fax. Cualquier comunicado de esta naturaleza es contrario a la política de JPV INVERSIONES, S.L., esta no acepta ninguna responsabilidad.

ANEXO XII CLÁUSULA LOPD PARA FACTURAS	DOC. DE SEGURIDAD VERSIÓN 2.0

En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le comunicamos que los datos que usted nos facilite quedarán incorporados y serán tratados en los ficheros titularidad de JPV INVERSIONES, S.L. con el fin de poderle prestar nuestros servicios, así como para mantenerle informado sobre cuestiones relativas a la actividad de la Empresa. JPV INVERSIONES, S.L. se compromete a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros.

Asimismo, le informamos de la posibilidad que tiene de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal de forma presencial en las oficinas de JPV INVERSIONES, S.L., acompañando copia de DNI, o bien mediante correo postal dirigido a: Av. Del Percebe, s/n, 08080, Barcelona.

ANEXO XIII FORMULARIO PARA EL EJERCICIO DE LOS DERECHOS ARCO	DOC. DE SEGURIDAD VERSIÓN 2.0

DATOS DEL RESPONSABLE DEL TRATAMIENTO

JPV INVERSIONES, S.L. C.I.F.: B-00000001

Domicilio: Avda. Del Percebe, s/n.

Localidad: Barcelona. Provincia: Barcelona C.P.: 08080

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

☐ Hombre ☐ Mujer

Nombre y apellidos: _____ D.N.I.: _____

Domicilio: _____

Localidad: _____ Provincia: _____ C.P.: _____

Telf. de contacto: _____

Que, mediante la presente solicito ejercitar el siguiente derecho de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal:

☐ Derecho de **acceso**, para ser informado de mis datos de carácter personal sometidos a tratamiento por parte de JPV INVERSIONES, S.L.

☐ Derecho de **rectificación**, de los datos de carácter personal que señalo a continuación:

_____
_____
_____
_____

☐ Derecho de **cancelación**, de los datos de carácter personal que señalo a continuación:

_____
_____
_____
_____

☐ Derecho de **oposición**, de manera que no se lleve a cabo tratamiento alguno de mis datos de carácter personal por los siguientes motivos y en relación con:

_____
_____
_____
_____

En relación con la solicitud expuesta, adjunto los siguientes documentos:
_____
_____

SOLICITO, que sea atendido mi ejercicio del derecho mencionado en los términos anteriormente expuestos.

Fecha: ___ de _____ de _____

Fdo.: _____

Annex IV. Document de seguretat de la Fundació JPV

DOCUMENTO DE SEGURIDAD

Fundación JPV

Versión 2.0

Diciembre 2015

ÍNDICE

1. OBJETO DEL DOCUMENTO

El presente documento responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en el que se regulan entre otras, las medidas de seguridad para los ficheros y tratamientos automatizados que contengan datos de carácter personal.

Los ficheros de datos a los que se refiere este documento se encuentran legalmente clasificados como nivel de seguridad **MEDIO,** atendiendo a las condiciones descritas en el artículo 81.1 del Real Decreto citado, siendo por tanto aplicables todas las medidas de seguridad de nivel **MEDIO** que se establecen en el Capítulo III del Título VIII, del citado Reglamento.

2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

FUNDACIÓN JPV como consecuencia de las actividades desarrolladas dentro de su objeto social, trata información en ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de FUNDACIÓN JPV incluyendo los sistemas de información soportes y equipos empleados para el tratamiento de datos de carácter personal, las personas que intervienen en el tratamiento y los locales en los que se ubican, todo ello que debe ser protegido de acuerdo a lo dispuesto en la normativa vigente,.

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

FICHERO	**TIPO DE SISTEMA**	**NIVEL DE SEGURIDAD**
CLIENTES Y/O PROVEEDORES (SAP R/3)	AUTOMATIZADO	BÁSICO
RECURSOS HUMANOS (Dominio GrupoJPV)	AUTOMATIZADO	MEDIO

En el **ANEXO I** ("*FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS")* se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los ficheros, aplicaciones y herramientas de actualización y consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos, gestionados por FUNDACIÓN JPV, o por cualquier otra empresa con la que haya suscrito un contrato de prestación de servicios que conlleve el tratamiento de los datos de carácter personal. 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 así como las aplicaciones y sistemas que los tratan, los equipos informáticos que las soportan y los locales donde se ubican.

En la actualidad la FUNDACIÓN JPV, ha suscrito diversos contratos de prestación de servicios con terceras entidades actuando en calidad de prestatario, que conllevan el tratamiento de datos de carácter personal de los ficheros de FUNDACIÓN JPV por estas entidades.

3. RESPONSABLE DE SEGURIDAD

FUNDACIÓN JPV, ha designado como responsable de seguridad en materia de protección de datos, en adelante, el "Responsable de Seguridad", a CALPURNIA CONSULTING, S.L. de todos los asuntos relacionados con esta materia dentro de la organización.

4. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

4.1. Identificación y autenticación.

Medidas y normas relativas a la identificación y autentificación del personal autorizado para acceder a los datos personales.

El Responsable del Fichero elabora una relación actualizada de usuarios que tengan acceso autorizado al sistema de información.

El Responsable de Seguridad custodia y actualiza la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información. Es competencia del Responsable de

Seguridad que la atribución y asignación de contraseñas así como la custodia de la relación de usuarios se realice de forma que se garantice su confidencialidad e integridad.

El procedimiento seguido en FUNDACIÓN JPV para la identificación y autenticación de los usuarios cuando intentan acceder al sistema o las aplicaciones, está basada en la combinación de un código de identificación de usuario y una contraseña, en red. A cada usuario le ha sido asignado un identificador único tanto para el acceso al sistema, como para el acceso a las aplicaciones, no existe un procedimiento para la asignación de contraseñas.

El control de acceso al sistema se limitará a tres (3) intentos. En caso de agotar los intentos, se procederá a la revocación del usuario que, para volver a acceder al sistema, deberá solicitarlo.

Los números de identificación y claves de acceso asignadas a cada usuario de la red del Responsable del Fichero son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de las mismas.

Las contraseñas de los usuarios autorizados son alfanuméricas, tienen una longitud mínima de ocho caracteres, se modifican con una periodicidad de 45 días y no es posible la repetición de las cinco últimas contraseñas introducidas. El administrador del sistema informático indica la obligatoriedad de cambio de contraseña en la cuenta del usuario y éste debe cambiarla en el plazo establecido. Durante el tiempo que estén vigentes, las contraseñas se almacenan de forma ininteligible.

Las contraseñas serán modificadas de acuerdo con el procedimiento técnico y de organización establecido por el Responsable de Seguridad Técnico en cada caso y que dependerá de cada sistema y de cada aplicación en concreto. Solamente el Responsable de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos o recursos.

Este proceso de caducidad de contraseñas lo realiza el Responsable de Seguridad, por medio de los profesionales designados al efecto que tienen las potestades para el acceso a los datos estrictamente necesarios para el desempeño de su trabajo y están sometidos a las mismas obligaciones que el personal de la empresa en materia de protección de datos, especialmente a la de secreto respecto de los datos personales que hubiese podido conocer con motivo de la prestación del servicio. Las contraseñas se almacenan de forma ininteligible y cifrada. En el entorno de red se utiliza un mecanismo “desafío-respuesta” HMAC-MD5, de forma que las contraseñas nunca viajan por la red para la transmisión de la información.

Las operaciones susceptibles de seguimiento que se realicen en la red del Responsable del Fichero quedan registradas en los archivos de registro del servidor (que proporcionan constancia de los accesos a los ficheros de la empresa mediante identificación del usuario que accede, la fecha y la hora del acceso y si éste ha sido autorizado o denegado). El uso del usuario y la contraseña asignados a cada persona implica la aceptación, como documento probatorio de la operación efectuada, de los registros generados en dichos archivos LOG y almacenados en el sistema informático de la empresa. Salvo prueba en contrario, se presume que los actos que se

lleven a cabo con el usuario y la contraseña asignados han sido realizados en realidad por la persona titular de los mismos.

El Responsable del Fichero posee los mecanismos necesarios para obtener una relación actualizada de los usuarios que tienen acceso autorizado a los sistemas de información de la compañía y establece los procedimientos de identificación y autenticación necesarios para garantizar la seguridad de dicho acceso.

El mecanismo de identificación se basa en la asignación de usuarios a cada una de las personas que acceden a los sistemas de información y el mecanismo de autenticación se basa en la existencia de contraseñas.

Cuando el tratamiento se realiza por el encargado del tratamiento mediante acceso remoto a los sistemas del Responsable del Tratamiento, se ha establecido una limitación, cuyo procedimiento es la incorporación de datos a los sistemas o soportes distintos de los del responsable.

4.2. Gestión de soportes

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en los locales bajo el control tanto del encargado del tratamiento como del responsable del tratamiento, lugares de acceso restringido al que solo tendrán acceso las personas con autorización.

4.2.1. Inventario de soportes

Los soportes no automatizados con datos personales (papel) deberán poder identificar su contenido y se registrarán en el anexo Inventario de Soportes.

4.2.2. Destrucción de documentos

Cuando vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal, deberá procederse a su destrucción, de manera que se impida la reconstrucción posterior del documento; por ejemplo mediante el uso de destructora de papel.

4.3. Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

4.4. Copias de respaldo y recuperación

Se realizarán copias de respaldo y recuperación, salvo que no se hubiese producido ninguna actualización de los datos, este procedimiento se realizará con una periodicidad diaria.

La copia de respaldo se realiza en un soporte extraíble que es depositado en una caja de seguridad ignífuga. Con esta medida se evita la necesidad de traslado de los mismos a otra ubicación fuera de las instalaciones.

En caso de traslado de los soportes físicos estos deberán cifrarse para evitar el acceso a la información que contienen.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizan su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción, así como se realizan cifradas para que en caso de sustracción o pérdida sea totalmente imposible descifrarlas. El sistema de copia de seguridad identifica los soportes mediante un sistema de etiquetado.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

4.5. Control de acceso

Los usuarios tanto en la red como en los puestos individuales, deben identificarse y autenticar el acceso a sistemas y aplicaciones, mediante clave de usuario y contraseña, para poder acceder de forma autorizada.

La introducción de una clave distinta a la autorizada impide el acceso a la red, ofreciendo la posibilidad de subsanar errores de teclado, con un límite de tres (3) accesos no autorizados.

El Responsable de Seguridad es el encargado del mantenimiento de los usuarios del sistema y aplicaciones en base a los criterios establecidos por la Dirección. Todo usuario estará obligado a bloquear su equipo en el momento en que se va a ausentar de su puesto de trabajo, es decir el equipo deberá estar configurado para que se bloquee automáticamente tras un cierto tiempo de inactividad.

Con el alta de la contraseña de cada usuario se identifica qué grupo de acceso debe ser asignado, tanto para datos como para el acceso a determinadas aplicaciones.

4.6. Auditoría

Los sistemas de tratamiento no automatizados se someterán a auditoría, al menos cada dos años, de manera análoga a los sistemas automatizados.

5. GESTIÓN DE INCIDENCIAS

5.1. Objeto.

Al no existir en FUNDACIÓN JPV un protocolo destinado a atender cualquier eventualidad que afecte a la seguridad de los datos, el procedimiento será acudir a los asesores informáticos.

No obstante, FUNDACIÓN JPV recogerá cuantas incidencias de seguridad se produzcan sobre los datos que trata, tales como:

- ✓ Incidencias que afecten a la identificación y autentificación de los usuarios.
- ✓ Incidencias que afecten a los derechos de acceso a los datos.
- ✓ Incidencias que afecten a la gestión de soportes.
- ✓ Incidencias que afecten a los procedimientos de copias de seguridad y recuperación.
- ✓ 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.

En este apartado se establecen los mecanismos de actuación por parte de los usuarios de los sistemas de información de FUNDACIÓN JPV, para la comunicación de las incidencias.

5.2. Ámbito de aplicación

Al igual que en caso de los ficheros temporales, el Reglamento de Medidas de Seguridad tampoco define el concepto de incidencia. Únicamente se indica como incidencia de seguridad de manera explícita, los procesos de recuperación de datos. FUNDACIÓN JPV intentará contemplar en el sentido más amplio del concepto de incidencia, entendiendo por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal funcionamiento de las medidas físicas y lógicas que puedan afectar a su disponibilidad y 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 afectan a la identificación y autentificación 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 afectan a la revisión de soportes:

  - ✓ Comunicación de pérdida de soportes.
  - ✓ Comunicación de localización de soportes en lugares inadecuados.
  - ✓ Errores de contenido en los soportes recibidos.

- Incidencias que afectan a los procedimientos de copias de salvaguardia y recuperación:

  - ✓ Errores en los procesos de realización de copias de salvaguardia.
  - ✓ 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 todos los usuarios de los sistemas de información de FUNDACIÓN JPV, empleados y colaboradores externos.

5.3. Responsabilidades

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

- Todos los usuarios de la FUNDACIÓN JPV, deben informar de cualquier incidencia producida en materia de seguridad.
- El Responsable de Seguridad debe ocuparse del seguimiento de las incidencias en materia de protección de datos de carácter personal.

5.4. Comunicación de incidencias

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. La difusión de la Circular que se adjunta a este documento de seguridad como **ANEXO IV** implica que todos los usuarios de la FUNDACIÓN JPV, deben ser conocedores de su obligación de comunicar las incidencias en materia de seguridad al Responsable de Seguridad. Todas las comunicaciones deberán efectuarse al Responsable de Seguridad indicando el momento en que se detectaron y utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente. Para que quede constancia de la comunicación, el usuario, además, lo comunicará por correo electrónico.

5.5. Registros

El Responsable de Seguridad procederá a incluir las incidencias en el registro y, si afectan a la seguridad de los datos de carácter personal, las marcará como tales. 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 contará con los siguientes campos:

- Tipo de incidencia.
- Momento en que se ha producido o se ha detectado la incidencia.
- Persona que la notifica.
- Persona a la que se le notifica.
- Efectos causados por la misma.

También se llevará un registro de resolución de incidencias, que recoja la información sobre las medidas adoptadas. En el caso en que la incidencia implique la ejecución de un proceso de recuperación de datos, el registro de resolución de incidencias contendrá, además, la siguiente información:

- Persona que ejecutó el proceso.
- Datos restaurados.
- En su caso, datos que fue necesario grabar manualmente para su recuperación.

En el **ANEXO II** se recogen los modelos para proceder al registro de incidencias y de su resolución.

6. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

Con el objeto de respetar lo establecido en la normativa de protección de datos de carácter personal, el Responsable del Fichero impone a su personal el cumplimiento de las siguientes obligaciones, las cuales deberán ser conocidas, aceptadas y respetadas por todo el personal.

6.1. Obligaciones del personal

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, se establece que serán informadas de acuerdo con el siguiente procedimiento:

- FUNDACIÓN JPV emitirá una circular donde se recogerán las principales obligaciones en materia de seguridad sobre datos de carácter personal, incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de los recursos informáticos para otras finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral, así como la obligación de mantener el deber de secreto sobre todos los datos tratados con motivos del desempeño de su puesto de trabajo y de no comunicar los referidos datos a ninguna otra persona o entidad sin la autorización pertinente.

Las normas aplicables al personal con acceso a datos de carácter personal se recogen en el **ANEXO III**, cuyo contenido y detalle se actualiza periódicamente en función de las decisiones empresariales al respecto y de los cambios normativos o jurisprudenciales que, en su caso, se produzcan.

6.2. Información al personal

El Reglamento 1720/2007, dispone la obligación de adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

El Responsable de Seguridad ha sido personalmente informado de las funciones que le han sido asignadas y que figuran en el apartado siguiente del presente Documento de seguridad.

6.3. Obligaciones del Responsable del Fichero o responsable del tratamiento

Además de las obligaciones que a continuación se detallan, cualesquiera otras obligaciones que le sean atribuidas por la normativa o por el presente Documento:

- ✓ Notificar a la Agencia Española de Protección de Datos los ficheros de datos personales del Responsable del Fichero.
- ✓ Velar por el cumplimiento de todos los requisitos establecidos en la LOPD y en su Reglamento de desarrollo.
- ✓ Redactar, establecer, actualizar y comprobar la aplicación y el cumplimiento del Documento de Seguridad.
- ✓ Adaptar el documento de seguridad a la normativa vigente.
- ✓ Describir los sistemas de información que realizan el tratamiento de los datos personales del Responsable del Fichero.
- ✓ Establecer los criterios que el Responsable de Seguridad debe seguir al realizar la función de conceder, alterar o anular el acceso autorizado a los datos y recursos.
- ✓ Establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- ✓ Verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.
- ✓ Autorizar la salida de soportes que contengan datos de carácter personal fuera de los locales en los que esté ubicado el soporte.
- ✓ 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 se ha autorizado.
- ✓ Establecer los criterios para la definición de los derechos de acceso de los usuarios.

6.4. Obligaciones del Responsable de Seguridad

Además de las obligaciones que a continuación se detallan, cualesquiera otras obligaciones que le sean atribuidas por la normativa o por el presente Documento:

- ✓ Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.
- ✓ Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por el Responsable del Fichero.
- ✓ Determinar el ámbito del Documento de Seguridad.
- ✓ Determinar y describir los recursos informáticos a los que se aplicará el Documento de Seguridad.
- ✓ Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.

- ✓ Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos.
- ✓ Comprobar el cumplimiento de la periodicidad establecida para la realización de copias de respaldo.
- ✓ Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al sistema informático del Responsable del Fichero con especificación del nivel de acceso que tiene cada usuario.
- ✓ Establecer y comprobar la aplicación del procedimiento de identificación y autentificación de usuarios.
- ✓ Establecer y comprobar la aplicación del procedimiento de asignación distribución y almacenamiento de contraseñas.
- ✓ Comprobar el mantenimiento de la confidencialidad de las contraseñas de los usuarios.
- ✓ Establecer y comprobar la aplicación de un procedimiento de cambio periódico de las contraseñas de los usuarios.
- ✓ Establecer y comprobar la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma inteligible.
- ✓ Conceder, alterar o anular el acceso autorizado a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.
- ✓ Establecer y comprobar la aplicación de un sistema que permita identificar, inventariar y almacenar en un lugar seguro de los soportes informáticos que contienen datos de carácter personal.
- ✓ Autorizar la entrada y salida de soportes informáticos que contienen datos de carácter personal.
- ✓ Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas, para el establecimiento de las correspondientes sanciones.
- ✓ Coordinar y controlar las medidas definidas en el Documento de Seguridad.
  Traslado de documentación.

7. CONTRATOS DE PRESTACIÓN DE SERVICIOS

En este apartado aparece una relación exhaustiva de los datos tratados por terceros, como consecuencia de un contrato de prestación de servicios. A continuación se presenta un modelo de tabla para recoger esta información:

PRESTADOR DEL SERVICIO	FINALIDADES	DATOS FACILITADOS	LUGAR DE TRABAJO	SISTEMA DE TRATAMIENTO

JPV INVERSIONES, S.L.	CLIENTES Y PROVEEDORES	CLIENTES Y PROVEEDORES	JPV INVERSIONES, S.L. (Avenida del Percebe, s/n, 08080, Barcelona)	MIXTO

8. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a la normativa vigente en cada momento sobre protección de datos de carácter personal.

ANEXO I FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS	DOC. DE SEGURIDAD VERSIÓN 2.0

En el presente Anexo se recoge la información relativa a los ficheros responsabilidad de FUNDACIÓN JPV que se hallan inscritos en el Registro General de Protección de Datos, indicando el entorno donde se encuentran ubicados y las aplicaciones que los gestionan.

NOMBRE DEL FICHERO	DATOS TRATADOS	FECHA DE INSCRIPCIÓN	CÓDIGO DE INSCRIPCIÓN	UBICACIÓN Y MODO DE TRATAMIENTO	NIVEL DE SEGURIDAD
CLIENTES Y/O PROVEEDORES	Datos de clientes y suministradores de la fundación			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	BÁSICO
RECURSOS HUMANOS	Datos del personal de la fundación			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	MEDIO

ANEXO II REGISTRO DE INCIDENCIAS	DOC. DE SEGURIDAD VERSIÓN 2.0

NOTIFICACIÓN Y REGISTRO DE INCIDENCIAS	
Numero de incidencia:	
Fecha de notificación: Hora:	
Usuario que realiza la notificación:	
Personas a las que se le comunica la incidencia:	
DESCRIPCION DE LA INCIDENCIA	
Fecha de la incidencia: Hora:	
Tipo de incidencia (intrusión, pérdida de datos, etc.):	
Descripción detallada de la incidencia:	
Posibles efectos de la incidencia	
Firma del notificante:	Firma receptor:

REGISTRO DE RESOLUCION DE INCIDENCIAS		
Numero de incidencia:		
Medidas adoptadas y pasos realizados:		
Resultado de las medidas:		
Fecha de resolución:		
RECUPERACION DE DATOS:		
Procedimiento realizado:		
Fecha de realización:		
Datos restaurados:		Datos grabados manualmente:
Persona que realiza el procedimiento:		

Fecha y lugar:	Firma del Responsable del Fichero:

ANEXO III NORMAS APLICABLES A PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL	DOC. DE SEGURIDAD VERSIÓN 2.0

El Documento de Seguridad de FUNDACIÓN JPV enumera detalladamente las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal con arreglo a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y al Real Decreto 1720/2007, por el que se aprobó el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El personal sobre el que recaen dichas obligaciones y funciones podrá acceder al contenido del Documento de Seguridad, siempre previa solicitud al Responsable de Seguridad. No obstante, y a efectos aclaratorios, en el presente Anexo se recogen las principales obligaciones en materia de protección de datos de carácter personal para conocimiento directo de los trabajadores, quienes deberán dar íntegro cumplimiento a las mismas:

OBLIGACIONES DEL PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL

CONTRASEÑAS:

1) Las contraseñas de los usuarios serán personales e intransferibles.
2) Las contraseñas deberán ser alfanuméricas y tener una longitud máxima de ocho caracteres.
3) Las contraseñas caducarán cada 45 días, momento en el cual el usuario deberá designar una nueva contraseña que no podrá coincidir con las últimas cinco contraseñas introducidas.

EQUIPOS INFORMÁTICOS:

4) Se prohíbe al personal la instalación de cualquier tipo de aplicación en los equipos informáticos sin autorización previa.
5) Se prohíbe la utilización de los equipos y soportes informáticos para finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral.
6) Los usuarios estarán obligados a bloquear su equipo en el momento de ausentarse de su puesto de trabajo, requiriendo la introducción de usuario y contraseña para volver a acceder al equipo.

SECRETO Y CONFIDENCIALIDAD:

7) Los usuarios deberán mantener el secreto sobre todos los datos tratados con motivo del desempeño de su puesto de trabajo.
8) No podrán, asimismo, comunicar los referidos datos a ninguna otra persona o entidad, salvo autorización pertinente.

INCIDENCIAS:

9) Los usuarios deberán informar al Responsable de Seguridad sobre cualquier incidencia producida en materia de seguridad de acuerdo con el procedimiento establecido en el punto 4.4 del Documento de Seguridad.
10) Los usuarios deberán participar en la implantación y seguimiento de la política de seguridad mediante la firma de la Circular que les será entregada a cada uno.

OTROS:

11) Todas las obligaciones anteriores deberán mantenerse, incluso tras la extinción de la relación laboral con FUNDACIÓN JPV.
12) El trabajador será responsable tanto frente a FUNDACIÓN JPV, como frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores, pudiendo FUNDACIÓN JPV reclamar las indemnizaciones pertinentes.

Para cualquier aclaración al respecto se puede contactar con la Responsable de Seguridad, INNOTO GESTIÓN PARA EL DESARROLLO, S.L.

ANEXO IV CIRCULAR A LOS TRABAJADORES	DOC. DE SEGURIDAD VERSIÓN 2.0

Nombre: _____ NIF: _____

En mi capacidad de empleado (ya sea fijo, o temporal) y en consideración de la relación laboral que mantengo con FUNDACIÓN JPV, así como del acceso que se me permite a sus Bases de Información, constato que:

- Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja FUNDACIÓN JPV. En concreto he leído, entiendo y me comprometo a cumplir los Procedimientos de Seguridad de los Sistemas de Información que corresponden a mi función en la empresa (Descritos en el Documento de Seguridad).

- Entiendo que el incumplimiento de cualesquiera de las normas aplicables al personal con acceso a datos de carácter personal incluidas todas ellas en el Documento de Seguridad de FUNDACIÓN JPV, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empres y la posible reclamación por parte de la misma de los daños causados.

En_____, a __ de_____ de 20__.

Firma,

El empleado/a

ANEXO V ACUERDO DE CONFIDENCIALIDAD (TRABAJADORES Y ENCARGADOS DEL TRATAMIENTO)	DOC. DE SEGURIDAD VERSIÓN 2.0

ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO:

En _____, a___ de _____ de 20__.

ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO

REUNIDOS

De una parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

De otra parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

INTERVIENEN

La primera lo hace en nombre y representación de FUNDACIÓN JPV, con domicilio en Avda. del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº G-0000002, en su calidad de _____ de la fundación.

La segunda lo hace en nombre y representación de _____, con domicilio social en _____, y CIF nº _____, en su calidad de _____ de la sociedad (en adelante, el "**Encargado del Tratamiento**").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que las Partes se hallan vinculadas por un contrato de prestación de servicios de fecha ___ de _____ de _____, en virtud del cual el Encargado del Tratamiento se obligaba al tratamiento de datos por cuenta del responsable de los ficheros, esto es FUNDACIÓN JPV.

II.- Que, el artículo 10 de La Ley Orgánica de Protección de Datos de Carácter Personal (en adelante, "LOPD"), en su artículo 10 refiriéndose al deber de secreto, establece la obligación al

secreto profesional y al deber de guardar los datos, por parte de todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal.

III.- Que, en cumplimiento de lo establecido en LOPD, las Partes suscriben el presente Acuerdo de Confidencialidad, de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- INFORMACIÓN CONFIDENCIAL.

Se considerará información confidencial a toda aquella a la que el Responsable del Tratamiento acceda con motivo de la realización de sus funciones y obligaciones, independientemente del soporte en el que esté contenida.

SEGUNDA.- OBLIGACIÓN DE SECRETO.

El Encargado del Tratamiento no podrá revelar a persona alguna ajena a FUNDACIÓN JPV, cualesquiera datos confidenciales, protegidos por la LOPD, a los que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

TERCERA.- USO DE LA INFORMACIÓN.

El Encargado del Tratamiento se limitará a utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en relación al contrato de prestación de servicios suscrito con FUNDACIÓN JPV. No pudiendo disponer de tal información de ninguna otra forma o con otra finalidad.

CUARTA.- DURACIÓN.

Las obligaciones contenidas en el presente Acuerdo seguirán rigiendo de manera indefinida en el tiempo, aun tras la finalización de la relación contractual entre las Partes.

QUINTA.- INCUMPLIMIENTOS.

En caso de incumplimiento, el Responsable del Tratamiento se hace responsable ante cualquier daño que pueda ocasionar tanto a FUNDACIÓN JPV, como a terceros, debiendo resarcir a FUNDACIÓN JPV, de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y en prueba de conformidad, ambas partes firman el presente documento por duplicado, a un solo efecto y en lugar y fecha ut supra.

_____ _____

Fdo. D./Dña. _____ Fdo. D./Dña._____
EL RESPONSABLE DEL TRATAMIENTO **FUNDACIÓN JPV**

ACUERDO DE CONFIDENCIALIDAD CON TRABAJADORES:

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD. 15/99), en su artículo 10 refiriéndose al Deber de Secreto, establece que:

> "*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*"

Como consecuencia de lo anterior, el abajo firmante, D/Dña _____, con DNI _____, y domicilio en _____ en el marco de la **relación laboral** que le une con FUNDACIÓN JPV, se compromete a:

PRIMERA.- Teniendo en cuenta que los datos de carácter personal, tanto automatizados como en soporte papel, a los cuales va a tener acceso, en muchos casos son considerados por la legislación vigente en materia de protección de datos, como especialmente protegidos, se establece en la presente cláusula la obligatoriedad de no revelar a persona alguna ajena a FUNDACIÓN JPV, la información referente a la que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones del abajo firmante o a las impuestas por las leyes o normas que resulten de aplicación; o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

SEGUNDA.- Utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en FUNDACIÓN JPV, y no disponer de ella de ninguna otra forma o con otra finalidad.

TERCERA.- No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado, y que no sea necesaria para el desempeño de sus funciones en FUNDACIÓN JPV.

CUARTA.- Cumplir, en el desempeño de sus funciones en FUNDACIÓN JPV, la normativa vigente relativa a la Protección de Datos de Carácter Personal y, en particular la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y disposiciones complementarias o cualquier otra norma que la sustituya en el futuro.

QUINTA.- Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral que le une con FUNDACIÓN JPV.

SEXTA.- El trabajador transmite a FUNDACIÓN JPV que adquiere, todos los derechos que pudieran corresponderle sobre los programas de ordenador, aplicaciones informáticas y bases de datos desarrolladas por aquel en el marco de su relación laboral, trabajos, informes, estando estos realizados utilizando medios y recursos a los que haya tenido acceso con ocasión de su vinculación con FUNDACIÓN JPV.

SÉPTIMA.- El trabajador, se compromete a guardar Deber de Secreto, en concordancia con lo estipulado en el artículo 10 de la LOPD, de la información a la que tenga acceso en el desempeño de sus funciones en FUNDACIÓN JPV.

OCTAVA.- El abajo firmante se hace responsable frente a FUNDACIÓN JPV, y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a FUNDACIÓN JPV, de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y para que surta plenos efectos, firmo la presente declaración,

En _____, a___ de _____ de 20__.

Firma del trabajador

Fdo.: D/Dña:

ANEXO VI INVENTARIO DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

En el presente Anexo se inventariarán los soportes que contengan datos de carácter personal de manera detallada, de acuerdo con el siguiente cuadro de información:

NOMBRE DE LA ETIQUETA	**CONTENIDO DEL SOPORTE**	**TIPO DE SOPORTE**	**UBICACIÓN**	**FRECUENCIA DE UTILIZACIÓN**	**PROCEDIMIENTO DE DESTRUCCIÓN DEL SOPORTE**	**FECHA DE ALTA Y DE BAJA**	**CIFRADO**
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □

En caso de soportes cuya especial naturaleza impida su correcto registro según lo establecido más arriba, se procederá a dejar constancia de tal situación, indicando los aspectos que se puedan especificar.

ANEXO VII REGISTRO DE ENTRADA Y SALIDA DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

REGISTRO DE ENTRADA

Nº DE SOPORTES	**FECHA**	**HORA**	**TIPO DE SOPORTE**	**REMITENTE**	**MODO DE ENVÍO**	**CONTENIDO**	**RECEPTOR**	**DEPARTAMENTO**	**ESTADO**

REGISTRO DE SALIDA

Nº DE SOPORTES	FECHA	HORA	TIPO DE SOPORTE	DESTINATARIO	MODO DE ENVÍO	CONTENIDO	EMISOR	DEPARTAMENTO

ANEXO VIII SALIDAS AUTORIZADAS DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

La dirección de FUNDACIÓN JPV, ha aprobado la relación de salidas periódicas de soportes que contienen datos de carácter personal que han sido autorizados por la entidad.

A continuación se presenta la relación que será actualizada cada vez que se produzcan modificaciones al respecto.

ANEXO IX CONTROL DE ENTRADA / SALIDA DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

CONTROL DE ENTRADA / SALIDA DE SOPORTES

Referencia Nº _____ **Fecha y hora de la operación** _____

ENTRADA ☐ **SALIDA** ☐ **DEVOLUCIÓN** ☐

TIPO DE SOPORTES _____ **NÚMERO DE SOPORTES** _____

NÚMERO DE IDENTIFICACIÓN DEL SOPORTE _____

CONTENIDO _____

FINALIDAD _____

FICHERO DEL QUE PROCEDEN LOS DATOS _____

IDENTIFICACIÓN DE LA DELEGACIÓN / ENTIDAD (ORIGEN / DESTINO)

NOMBRE DELEGACIÓN / ENTIDAD _____

DESTINATARIO _____

DIRECCIÓN _____

TELEFONO DE CONTACTO _____

DATOS DEL RESPONSABLE DE LA ENTREGA / RECEPCIÓN (AUTORIZADO)

NOMBRE Y APELLIDOS _____

CARGO / PUESTO _____

PERSONA QUE AUTORIZA _____

FECHA DE ENTRADA _____ / _____ / _____

FECHA DE SALIDA _____ / _____ / _____

FECHA DE DEVOLUCIÓN _____ / _____ /_____

FORMA Y PRECAUCIONES DE ENVÍO _____

OBSERVACIONES _____

_____

_____

Fdo. _____

ANEXO X MODELO DE CONTRATO DE ENCARGADO DEL TRATAMIENTO DE LOS DATOS POR CUENTA DE TERCEROS.	DOC. DE SEGURIDAD VERSIÓN 2.0

En _____, a __ de _____ de 20__.

CONTRATO DE ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

REUNIDOS

De una parte, D./Dña._____, con D.N.I_____, que actúa en nombre y representación de FUNDACIÓN JPV, con domicilio en Avda. del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº G-00000002, en su calidad de _____, (en adelante, "EL RESPONSABLE DEL FICHERO").

Y de otra parte, D./Dña._____, con D.N.I_____, que actúa en nombre y representación de (SOCIEDAD), con domicilio social en_____, Y con C.I.F. nº _____, en su calidad de _____, (en adelante, "EL ENCARGADO DEL TRATAMIENTO").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que ambas Partes se hallan vinculadas por un contrato de prestación de servicios, en virtud del cual la (SOCIEDAD) tiene acceso a datos de carácter personal protegidos por la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (en adelante, "LOPD").

II.- Que, las Partes han acordado la suscripción del presente contrato de Acceso a los Datos por Cuenta de Terceros en cumplimiento con lo dispuesto en el artículo 12 de la LOPD, para el tratamiento de dichos datos de carácter personal, cumpliendo con los requisitos legales correspondientes y de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- DEFINICIONES.

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.

SEGUNDA.- OBJETO.

El objeto del presente contrato es el tratamiento por parte de EL ENCARGADO DEL TRATAMIENTO de los datos personales relativos a: _____ con la finalidad de poder realizar los servicios contratados, para lo cual previamente deberá ésta poner a disposición del encargado del tratamiento dichos datos personales.

Dicho tratamiento se realizará de conformidad con lo establecido en la LOPD y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante "RLOPD"), o normativa que los sustituya.

TERCERA.- DATOS A LOS QUE SE DA ACCESO Y NIVEL DE SEGURIDAD.

Los datos personales que forman parte de los ficheros del RESPONSABLE DEL FICHERO, a los que tendrá acceso el encargado del tratamiento son los siguientes:

- Fichero (1): _____.
    - Datos afectados por el tratamiento: _____.
    - Nivel de seguridad: _____.

CUARTA.- OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO.

4.1 EL ENCARGADO DEL TRATAMIENTO solamente tratará los datos que se le han encomendado conforme a las instrucciones del responsable del fichero.

4.2 Los datos facilitados no se aplicarán ni utilizarán con una finalidad diferente a la que figura en este documento, ni EL ENCARGADO DEL TRATAMIENTO los comunicará, ni siquiera a efectos de su conservación, a terceros.

4.3 EL ENCARGADO DEL TRATAMIENTO y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de los datos que les han sido confiados para su tratamiento.

4.4 EL ENCARGADO DEL TRATAMIENTO deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Las medidas de

seguridad que deberán ser observadas dependerán del nivel de seguridad de los datos objeto de tratamiento, por ello, dichas medidas podrán ser de nivel básico, medio o alto, según lo estipulado en la LOPD y el RLOPD.

4.5 En caso de resolución del presente contrato, los datos serán destruidos en su totalidad o devueltos al RESPONSABLE DEL FICHERO, teniendo en cuenta los distintos soportes o documentos donde estos puedan constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc.

4.6 Una vez se haya realizado la operación mencionada en el punto anterior, EL ENCARGADO DEL TRATAMIENTO se compromete a entregar una declaración por escrito al RESPONSABLE DEL FICHERO donde conste que así se ha realizado.

4.7 Será de aplicación en todo caso, en lo no previsto en este contrato, la normativa vigente en materia de protección de datos personales.

4.8 En el caso de que EL ENCARGADO DEL TRATAMIENTO incumpla con las obligaciones antes establecidas, pasará a tener la consideración de responsable del tratamiento o fichero, respondiendo de las infracciones en que hubiera incurrido personalmente.

QUINTA.- DURACIÓN Y RESOLUCIÓN DEL CONTRATO.

El presente contrato se considera accesorio del contrato de prestación de servicios de existente entre las partes, por lo que su duración y extinción queda supeditada al mismo.

SEXTA.- LEY APLICABLE Y FORO.

El presente contrato se regirá e interpretará conforme a la legislación española vigente, en aquello que no esté expresamente regulado, sometiéndose las partes, para todas las controversias que pudieran surgir en relación con el mismo, a la competencia de los Juzgados y Tribunales de la ciudad de A Coruña, con renuncia a cualquier otro foro que les pudiera corresponder.

Y en prueba de su conformidad, firman las partes el presente contrato en duplicado ejemplar y a un sólo efecto, en lugar y fecha señalados en el encabezamiento.

FUNDACIÓN JPV **(_____)**
EL RESPONSABLE DEL FICHERO **EL ENCARGADO DEL TRATAMIENTO**

ANEXO XI CLÁUSULA LOPD PARA E-MAILS/FAX	DOC. DE SEGURIDAD VERSIÓN 2.0

La información contenida en este mensaje y en cualquier archivo o documento que se adjunte al mismo es confidencial y privilegiada.

Esta dirigida exclusivamente para el uso privado del destinatario y no debe ser diseminada o utilizada por otra personal.

FUNDACIÓN JPV no garantiza la transmisión de mensajes electrónicos en forma segura y libre de errores debido a que la información puede ser interceptada, dañada, perdida, destruida, pueda llegar tarde, incompleta, o conteniendo virus.

FUNDACIÓN JPV no acepta responsabilidad por cualquier error u omisión en el contenido de este mensaje, que puede surgir como resultado de la transmisión de este mensaje electrónico.

Los empleados y usuarios del sistema de correo electrónico/fax están expresamente advertidos de no crear o enviar enunciados difamatorios y de no cometer ninguna violación a los derechos de autor u otras disposiciones legales, a través de comunicaciones por mensaje electrónico/fax. Cualquier comunicado de esta naturaleza es contrario a la política de FUNDACIÓN JPV, esta no acepta ninguna responsabilidad.

ANEXO XII CLÁUSULA LOPD PARA FACTURAS	DOC. DE SEGURIDAD VERSIÓN 2.0

En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le comunicamos que los datos que usted nos facilite quedarán incorporados y serán tratados en los ficheros titularidad de FUNDACIÓN JPV con el fin de poderle prestar nuestros servicios, así como para mantenerle informado sobre cuestiones relativas a la actividad de la Empresa. FUNDACIÓN JPV se compromete a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros.

Asimismo, le informamos de la posibilidad que tiene de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal de forma presencial en las oficinas de FUNDACIÓN JPV, acompañando copia de DNI, o bien mediante correo postal dirigido a: Av. Del Percebe, s/n, 08080, Barcelona.

ANEXO XIII TRATAMIENTO DE IMÁGENES DE MENORES DE EDAD	DOC. DE SEGURIDAD VERSIÓN 2.0

Por otra parte, FUNDACIÓN JPV informa a los interesados que, de acuerdo con la LOPD y con la Ley 1/1982 de protección civil, derecho al honor, intimidad personal y familiar y la propia imagen, durante la estancia del menor podrán realizarse fotografías y grabaciones del campamento o actividades en las que participen los menores de edad. Dichas imágenes y/o grabaciones podrán ser publicadas en los medios de comunicación de FUNDACIÓN JPV, convencionales y electrónicas (Internet) que FUNDACIÓN JPV estime convenientes, para dar publicidad a sus actividades.

FUNDACIÓN JPV advierte al padre/madre/tutor/representante legal que la publicación de las fotografías y/o grabaciones mencionadas implica la cesión de dichos datos a terceros y en particular, a las personas físicas y/o jurídicas que accedan a los mismos desde cualquier país, incluidos los sitios fuera del territorio del Espacio Económico Europeo o en Estados que no ofrecen un nivel adecuado de protección conforme a lo previsto en la normativa vigente sobre protección de datos personales.

FUNDACIÓN JPV necesita contar con la autorización expresa de los interesados para poder realizar los tratamientos descritos, por lo que se ruega al interesado que marque la casilla correspondiente:

☐ Autorizo a la realización de fotografías y grabaciones del campamento o actividad en las que participen los menores de edad. Dichas imágenes y/o grabaciones podrán ser publicadas en los medios de comunicación de FUNDACIÓN JPV electrónicos o no.

☐ No autorizo al tratamiento de imágenes arriba señalado en el correspondiente campamento o actividad.

ANEXO XIV AVISO LEGAL PÁGINA WEB	DOC. DE SEGURIDAD VERSIÓN 2.0

1. Información legal y aceptación.

Las presentes disposiciones regulan el uso del servicio de la web (en adelanta, la "Web") que FUNDACIÓN JPV, pone a disposición de los usuarios de Internet. FUNDACIÓN JPV con domicilio social en Avd. del Percebe, s/n, 08080, Barcelona y con C.I.F. número G-00000002.

La utilización de la Web atribuye la condición de usuario de la Web (en adelante, el "Usuario") e implica la aceptación de todas las condiciones incluidas en este Aviso Legal. La prestación del servicio de la Web tiene una duración limitada al momento en el que el Usuario se encuentre conectado a la Web o a alguno de los servicios que a través del mismo se facilitan. Por tanto, el Usuario debe leer atentamente el presente Aviso Legal en cada una de las ocasiones en que se proponga utilizar la Web, ya que éste y sus condiciones de uso recogidas en el presente Aviso Legal pueden sufrir modificaciones.

2. Objeto.

El objeto de las presente condiciones generales es regular el uso que puede realizar los Usuarios de la Web de FUNDACIÓN JPV que actualmente se encuentra en la URL http://www.fundacionjpv.org, sin perjuicio de que ciertos servicios o contenidos dentro de la Web se sometan a sus propias condiciones particulares, reglamentos e instrucciones que, en su caso, sustituyen, complementan y/o modifican el presente Aviso Legal y que deberán ser aceptadas por el Usuario antes de iniciarse la prestación del servicio correspondiente.

3. Acceso.

El acceso y el uso de la Web, tiene carácter gratuito para los Usuarios (salvo en lo relativo al coste de conexión a través de la red de telecomunicaciones suministrada por el proveedor de acceso contratado por los usuarios) y no exige el registro previo del usuario con carácter general. No obstante, el acceso y uso de determinadas informaciones y servicios ofrecidos a través de la Web solo pueden hacerse previo registro del usuario.

En caso del registro de usuarios a través de identificadores y contraseñas, tanto el identificador como la contraseña pertenecerán exclusivamente a la persona a la que se le conceden. El usuario deberá mantener bajo su exclusiva responsabilidad tanto el identificador como la contraseña en la más estricta y absoluta confidencialidad, asumiendo, por tanto, cuantos daños o consecuencias de todo tipo se deriven del quebrantamiento o revelación del secreto.

4. Propiedad intelectual e industrial.

Todos los contenidos de la Web, entendiendo por estos a título meramente enunciativo los textos, fotografías, software, links y demás contenidos audiovisuales o sonoros, así como su diseño gráfico, códigos fuente, estructuras de navegación y demás servicios o productos telemáticos integrados en la Web (en adelante, los "Contenidos") son propiedad exclusiva de FUNDACIÓN JPV o de terceros, sin que pueda entenderse cedidos al usuario ninguno de los derechos de explotación reconocidos por la normativa vigente en materia de propiedad intelectual sobre los mismos, salvo aquellos que resulten estrictamente necesarios para el uso del la Web, por lo que el usuario se compromete a no infringir ningún derecho derivado de la propiedad intelectual o industrial, quedando expresamente prohibida la reproducción total o parcial de los mismos, su comunicación pública, distribución o cualquier forma de explotación, salvo consentimiento expreso y por escrito por parte de FUNDACIÓN JPV El usuario se compromete a utilizar dicha información y servicios exclusivamente para sus propias necesidades y a no realizar directa o indirectamente una explotación comercial de los servicios a los que tiene acceso o de los resultados obtenidos gracias a la utilización de la Web, salvo que haya obtenido consentimiento expreso de FUNDACIÓN JPV El usuario se obliga a no utilizar las facilidades y capacidades de la Web para realizar o sugerir actividades prohibidas por la ley o para intentar atraer a los usuarios hacia otros servicios competidores.

Las marcas, nombres comerciales o signos distintivos son titularidad de FUNDACIÓN JPV o terceros, y están protegidos por la legislación vigente en materia de propiedad industrial, sin que pueda entenderse que el acceso a la Web atribuya ningún derecho sobre las citadas marcas, nombres comerciales y/o signos distintivos.

5. Condiciones generales de uso.

5.1 General

El usuario se obliga a hacer un uso correcto de la Web de conformidad con la Ley y el presente Aviso Legal. El usuario responderá frente a FUNDACIÓN JPV o frente a terceros, de cualesquiera daños o perjuicios que pudiera causarse como consecuencia del incumplimiento de dicha obligación.

FUNDACIÓN JPV se reserva el derecho de bloquear el acceso de los usuarios que hagan un uso de la Web contrario a la Ley o a las condiciones del presente Aviso Legal, pudiendo anular o bloquear, en su caso, el identificador y contraseña de los usuarios registrados.

Queda expresamente prohibido el uso de la Web con usos lesivos de bienes o intereses de FUNDACIÓN JPV o de terceros o que de cualquier otra forma sobrecarguen, dañen o inutilicen las redes, servidores y demás equipos informáticos (hardware) o productos y aplicaciones informáticas (software) de FUNDACIÓN JPV o de terceros.

5.2 Contenidos

El usuario se compromete a utilizar los contenidos de conformidad con la Ley y el presente Aviso Legal, así como con las demás condiciones, reglamentos e instrucciones que en su caso pudieran ser de aplicación de conformidad con lo dispuesto en la cláusula 2. Con carácter

meramente enunciativo, el usuario de acuerdo con la legislación vigente deberá abstenerse de:

- Reproducir, copiar, distribuir, poner a disposición, comunicar públicamente, transformar o modificar los Contenidos salvo en los casos autorizados en la ley o expresamente consentidos por FUNDACIÓN JPV o por quien ostente la titularidad de los derechos de explotación en su caso.
- Reproducir, copiar para uso privado los Contenidos que pueden ser considerados como Software o Base de Datos de conformidad con la legislación vigente en materia de propiedad intelectual, así como su comunicación pública o puesta a disposición de terceros cuando estos actos impliquen necesariamente la reproducción por parte del usuario o de un tercero.
- Extraer y/o reutilizar la totalidad o una parte sustancial de los Contenidos integrantes de la Web así como de las bases de datos que FUNDACIÓN JPV ponga a disposición de los usuarios.

5.3 Formularios de recogida de datos.

Sin perjuicio de lo dispuesto en la cláusula 7 del presente Aviso Legal, así como en las políticas de privacidad accesibles desde la Web y que pudieran resultar aplicables en cada momento, la utilización de ciertos servicios o solicitudes dirigidos a FUNDACIÓN JPV están condicionados a la previa cumplimentación del registro de usuario.

Toda la información que facilite el usuario a través de los formularios de la Web a los efectos anteriores o cualesquiera otros deberá ser veraz. A estos efectos, el usuario garantiza la autenticidad de todos aquellos datos que facilite garantiza la autenticidad de todos aquellos datos que comunique y mantendrá la información facilitada a FUNDACIÓN JPV perfectamente actualizada de forma que responda, en todo momento, a la situación real del usuario. En todo caso será el usuario el único responsable de las manifestaciones falsas o inexactas que realice y de los perjuicios que cause a FUNDACIÓN JPV o a terceros por la información que facilite.

5.4 Introducción de enlaces a la Web.

El usuario de internet que quiera introducir enlaces desde sus propias páginas web a la Web deberá cumplir con las condiciones que se detallan a continuación sin que el desconocimiento de las mismas evite las responsabilidades derivadas de la Ley:

- El enlace podrá vincular a cualquier página web- a excepción de aquellas que incorporen datos personales, bases de datos u otra información sometida a LOPD pero no podrá reproducirla de ninguna forma (inline links, copia de los textos, gráficos, etc.).
- Quedará en todo caso prohibido, de acuerdo con la legislación aplicable y vigente en cada momento, establecer frames o marcos de cualquier tipo que envuelvan a la Web o permitan la visualización de los Contenidos a través de direcciones de internet

distintas de las de la Web y, en cualquier caso, cuando se visualicen conjuntamente con contenidos ajenos a la Web de forma que: (I) produzca, o pueda producir, error, confusión o engaño en los usuarios sobre la verdadera procedencia del servicio o Contenidos; (II) suponga un acto de comparación o imitación desleal; (III) sirva para aprovechar la reputación de la marca y prestigio de FUNDACIÓN JPV ; (IV) de cualquier otra forma resulte prohibido por la legislación vigente.

- No se realizarán desde la página que introduce el enlace ningún tipo de manifestación falsa, inexacta o incorrecta sobre FUNDACIÓN JPV, sus socios, empleados o clientes sobre la calidad de los servicios que presta.
- En ningún caso, se expresará en la página donde se ubique el enlace que FUNDACIÓN JPV ha prestado su consentimiento para la inserción del enlace o que de otra forma patrocina, colabora, verifica o supervisa los servicios del remitente.
- Está prohibida la utilización de cualquier marca denominativa, gráfica o mixta o cualquier otro signo distintivo de FUNDACIÓN JPV, dentro de la página del remitente salvo en los casos permitidos por la ley o expresamente autorizados por FUNDACIÓN JPV y siempre que se permita, en estos casos, un enlace directo con la Web en la forma establecida en esta cláusula.
- La página que establezca deberá cumplir fielmente con la ley y no podrá en ningún caso disponer o enlazar con contenidos propios o de terceros que: (I) sean ilícitos, nocivos o contrarios a la moral y a las buenas costumbres (pornográficos, violentos, racistas, etc.); (II) induzcan o puedan inducir en el usuario la falsa concepción de que FUNDACIÓN JPV suscribe, respalda, se adhiere o que de cualquier manera apoya, las ideas, manifestaciones o expresiones, lícitas o ilícitas, del remitente; (III) resulten inapropiados o no pertinentes con la actividad de FUNDACIÓN JPV en atención al lugar, contenidos y temática de la página web del remitente.

6. Exclusión de responsabilidad.

6.1 De la información.

El acceso a la Web no implica la obligación por parte de FUNDACIÓN JPV de comprobar la veracidad, exactitud, adecuación, idoneidad, exhaustividad y actualidad de la información suministrada a través del mismo. Los contenidos de esta Web son de carácter general y no constituyen, en modo alguno, la prestación de ningún tipo de servicio.

FUNDACIÓN JPV no se responsabiliza de las decisiones tomadas a partir de la información suministrada en la Web ni de los daños y perjuicios producidos en el usuario o terceros con motivo de actuaciones que tengan como único fundamento la información obtenida en la Web.

6.2 De la calidad del servicio.

El acceso a la Web no implica la obligación por parte de FUNDACIÓN JPV de controlar la ausencia de virus, gusanos o cualquier otro elemento informático dañino. Corresponde al

usuario, en todo caso, la disponibilidad de herramientas adecuadas para la detección y desinfección de programas informáticos dañinos.

FUNDACIÓN JPV no se responsabiliza de los daños producidos en los equipos informáticos de los usuarios o de terceros durante la prestación del servicio de la Web.

6.3 De la disponibilidad del servicio.

El acceso a la Web requiere de servicios y suministros de terceros, incluidos el transporte a través de redes de telecomunicaciones cuya finalidad, calidad, continuidad y funcionamiento no corresponde a FUNDACIÓN JPV. Por consiguiente, los servicios proveídos a través de la Web pueden ser suspendidos, cancelados o resultar inaccesibles, con carácter previo o simultáneo a la prestación del servicio de la Web.

FUNDACIÓN JPV no se responsabiliza de los daños o perjuicios de cualquier tipo producidos en el usuario que traigan causa de fallos o desconexiones en las redes de telecomunicaciones que produzcan la suspensión, cancelación o interrupción del servicio de la Web durante la prestación del mismo o con carácter previo.

FUNDACIÓN JPV podrá realizar las modificaciones que estime convenientes en la Web, pudiendo incluir servicios y contenidos adicionales a los actuales o, en su caso, suprimirlos. FUNDACIÓN JPV podrá modificar la Web cuando considere oportuno y podrá bloquear el acceso a todos o parte de los usuarios de la misma para proceder a realizar modificaciones o las reparaciones que considere necesarias en cualquier momento. En ningún caso, FUNDACIÓN JPV será responsable del inadecuado funcionamiento del sistema si ello obedece a una defectuosa configuración de los equipos del usuario o a su insuficiente capacidad para soportar los sistemas informáticos indispensables para poder hacer uso del servicio.

6.4 De los contenidos y servicios enlazados a través de la Web.

El servicio de acceso a la Web incluye dispositivos técnicos de enlace, directorios e incluso instrumentos de búsqueda que permiten al usuario acceder a otras páginas y portales de internet (en adelante, “Sitios Enlazados”). En estos casos, FUNDACIÓN JPV actúa como prestador de servicios de intermediación de conformidad con el artículo 17 de la Ley 34/2002, de 12 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI) y solo será responsable de los contenidos y servicios suministrados en los Sitios Enlazados en la medida en que tenga conocimiento efectivo de la ilicitud y no haya desactivado el enlace con la diligencia debida. En el supuesto de que el usuario considere que existe un Sitio Enlazado con contenidos ilícitos o inadecuados podrá comunicárselo a FUNDACIÓN JPV de acuerdo con el procedimiento y los efectos establecidos en la cláusula 8, sin que en ningún caso esta comunicación conlleve la obligación de retirar el correspondiente enlace. En ningún caso, la existencia de Sitios Enlazados debe de presuponer la existencia de acuerdos con los responsables o titulares de los mismos, ni la

recomendación, promoción o identificación de FUNDACIÓN JPV con las manifestaciones, contenidos o servicios proveídos.

FUNDACIÓN JPV no conoce los contenidos y servicios de los Sitios Enlazados y por tanto no se hace responsable por los daños producidos por la ilicitud, calidad, desactualización, indisponibilidad, error o inutilidad de los contenidos y/o servicios de los Sitios Enlazados ni de cualquier otro daño que no sea directamente imputable a FUNDACIÓN JPV.

7. Protección de datos personales.

Los datos recabados a través de formularios de recogida de datos de la Web será incorporados a un fichero automatizado de datos de carácter personal del que es responsable FUNDACIÓN JPV.

De acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "la LOPD"), el abonado y/o usuario (en adelante, "el cliente") presta su consentimiento para que sus datos personales se incorporen a los ficheros, automatizados o no, propiedad de FUNDACIÓN JPV, que tienen como finalidad la gestión de los clientes, premiar su finalidad y mantenerlos informados (envíos de la información sobre nuevas actividades y celebración de campeonatos hípicos por ejemplo) por cualquier medio (electrónico o no) de todas las ofertas de productos y/o servicios, y/o promociones incluyendo el análisis y la formación de perfiles y, en general, la realización de acciones comerciales, de promoción y/o marketing relacionadas con las actividades propias del objeto social de FUNDACIÓN JPV, así como con el deporte ocio, salud, bienestar, proveedores de transporte, seguros, servicios inmobiliarios, publicidad y la prestación de servicios de valor añadido.

El cliente tiene derecho a acceder al fichero que contiene sus datos de carácter personal, de cuyo tratamiento es responsable FUNDACIÓN JPV, a fin de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, mediante correo postal ordinario dirigido a FUNDACIÓN JPV, S.L., Avda., da Diputación, s/n (Edificio Inditex)- Polígono de Sabón, 15142, Arteixo, Asunto: LOPD, aportando fotocopia del DNI, solicitud que se realiza, indicación del domicilio a efectos de notificaciones, fecha y firma. Para su mayor comodidad, podrá igualmente obtener información para el ejercicio de estos derechos telefónicamente, a través del número que se indica en el apartado 1 de este Aviso Legal.

Asimismo, FUNDACIÓN JPV cancelará, borrará y/o bloqueará los datos cuando resulten inexactos, incompletos o hayan dejado de ser necesarios o pertinentes para su finalidad, de conformidad con lo previsto en la legislación en materia de protección de datos de carácter personal. A estos efectos, le rogamos que nos comunique inmediatamente cualquier modificación de sus Datos a fin de que la información contenida en nuestros ficheros esté en todo momento actualizada y no contenga errores.

En los formularios de recogida de datos, los campos obligatorios vendrán señalados, específicamente, por lo que en caso de que el usuario no facilite los datos correspondientes, FUNDACIÓN JPV podrá a su sola discreción denegar el correspondiente servicio.

FUNDACIÓN JPV adopta los niveles de seguridad requeridos por el Reglamento de Medidas de Seguridad aprobado por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. No obstante lo anterior, la seguridad técnica en un medio como un medio como Internet no es inexpugnable y pueden existir filtraciones por actuaciones dolosas de terceros.

FUNDACIÓN JPV podrá utilizar cookies durante la prestación del servicio de la Web. Las cookies son procedimientos automáticos de recogida de información relativa a las preferencias determinadas por un usuario durante su visita a una determinada página web. Esta información se registra en pequeños archivos que son guardados en los equipos informáticos del usuario correspondiente de forma imperceptible. Cada vez que el usuario vuelve a acceder al sitio web en cuestión estos archivos se activan automáticamente de manera que se configura el sitio web con las preferencias señaladas en anteriores visitas. En definitiva, las cookies son ficheros físicos de información personal alojados en el propio terminal del usuario y asociados inequívocamente a este terminal.

Las cookies no pueden lee los archivos cookies creados por otros proveedores.

El usuario tiene la posibilidad de configurar su programa navegador de manera que se impida la creación de los archivos cookie o se advierta del momento en que eso ocurre la Web es accesible sin que estén activadas las opciones referentes a los archivos cookie, si bien pueden impedir el correcto funcionamiento de mecanismos de seguridad para servicios excluidos o determinados servicios que requieren de mayor seguridad. Por norma general, la finalidad de los archivos cookie de la Web es la de facilitar la navegación del usuario.

8. Comunicación de carácter ilícito e inadecuado.

En el caso de que el usuario o cualquier otro usuario de internet tuvieran conocimiento de que los Sitios Enlazados remiten a páginas cuyos contenidos o servicios son ilícitos, nocivos, denigrantes, violentos o contrarios a la moral podrá ponerse en contacto con FUNDACIÓN JPV indicando los siguientes extremos:

- Datos personales del comunicante: nombre, dirección, número de teléfono y dirección de correo electrónico;
- Descripción de los hechos que revelan el carácter ilícito o inadecuado del Sitio Enlazado;
- En el supuesto de violación de derechos, tales como propiedad intelectual e industrial, los datos personales del titular del derecho infringido cuando sea persona distinta del comunicante;

- Asimismo, deberá aportar el título que acredite la legitimación del titular de los derechos y, en su caso, el de representación para actuar por cuenta del titular cuando sea persona distinta del comunicante;
- Declaración expresa de que la información contenida en la reclamación es exacta.

La recepción por parte de FUNDACIÓN JPV de la comunicación prevista en esta cláusula no supondrá, según lo dispuesto en la LSSI, el conocimiento efectivo de las actividades y/o contenidos por el comunicante.

9. Legislación.

El presente Aviso Legal se rige en todos y cada uno de sus extremos por la ley española.

ANEXO XV POLÍTICA DE PRIVACIDAD PÁGINA WEB	DOC. DE SEGURIDAD VERSIÓN 2.0

DATOS PERSONALES REGISTRADOS: FUNDACIÓN JPV (Avd. da del Percebe, s/n 08080, Barcelona) y CIF número G-00000002, como responsable del fichero, en cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, comunica a los usuarios de la Página Web: http://www.fundacionjpv.org/, en adelante "la Página Web", que los datos facilitados mediante los correspondientes formularios y los e-mails recibidos solicitando información y que tienen consideración de datos de carácter personal, se incluirán en un fichero automatizado o no de carácter confidencial.

Asimismo, se informa y los usuarios de la Página Web consientes su utilización mediante sistemas automáticos de decisión, segmentación y valoración respecto de las solicitudes que se realicen con la finalidad de gestión sus usuarios, la obtención de estadísticas diversas, la realización de prospecciones de mercado y el envío por parte de la Página Web, de publicidad e información en relación con los servicios prestados, y que estén relacionados con el uso de la plataforma, atendiendo a las preferencias que cada usuario haya configurado en la Página Web incluso después de finalizada la relación. Dicho fichero se encuentra inscrito en la Agencia Española de Protección de Datos conforme a la legislación vigente y normativa de desarrollo.

Asimismo, y de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante, "la LOPD"), el usuario presta su consentimiento para que sus datos personales se incorporen a los ficheros, automatizados o no, propiedad de FUNDACIÓN JPV, que tienen como finalidad la gestión de usuarios, mantenerlos informados , por cualquier medio (electrónico o no), de todas las ofertas y servicios y/o promociones, incluyendo el análisis y formación de perfiles, y en general, la realización de acciones comerciales de promoción y/o marketing relacionadas con las actividades propias del objeto social de FUNDACIÓN JPV así como servicios inmobiliarios, proveedores de transporte, seguros, servicios inmobiliarios, publicidad y la prestación de servicios de valor añadido.

Pulsando le botón "enviar" del correspondiente formulario y a los efectos de los dispuesto en el artículo 21 de la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, el usuario autoriza expresamente a FUNDACIÓN JPV a remitirle comunicaciones comerciales, promociones publicitarias, por correo electrónico o por cualquier otro medio de comunicación electrónica o no electrónica equivalente. Asimismo, pulsando el botón "enviar" o equivalente a este del correspondiente formulario el usuario prestará también su consentimiento expreso para que sus datos personales puedan ser comunicados, con idénticos fines, a las sociedades que en cada momento integren el grupo al que pertenece FUNDACIÓN JPV y a terceros que, del mismo u otros sectores, contraten o presten tales servicios a FUNDACIÓN JPV y/o proporcionen al usuario los servicios ofrecidos por FUNDACIÓN JPV. A los efectos previstos en la LOPD, el usuario se da por notificado de dichas cesiones. No

obstante, le usuario podrá oponerse al envío de tales comunicaciones señalando la casilla que a estos efectos aparece indicada en cada uno de los formularios o de acuerdo con lo establecido en las comunicaciones.

El usuario tiene derecho a acceder al fichero que contenga sus datos personales, de cuyo tratamiento FUNDACIÓN JPV, a fin de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, mediante correo postal ordinario dirigido a FUNDACIÓN JPV, Avenida del Percebe, s/n, 08080, Barcelona, Asunto: LOPD, aportando fotocopia del DNI, solicitud que se realiza, indicación del domicilio a efectos de notificaciones, fecha y firma. Para su mayor comodidad, podrá igualmente obtener información acerca del ejercicio de estos derechos telefónicamente, a través del apartado de contacto de la propia Web. Por último y si usted utiliza habitualmente el canal telefónico, o un medio de comunicación por vía electrónica en su relación con FUNDACIÓN JPV, podrá ejercitar igualmente dichos derechos a través de estos canales debiendo utilizar para ellos los medios de identificación habitualmente requeridos.

Asimismo, FUNDACIÓN JPV cancelará, borrará y/o bloqueará los datos cuando resulten inexactos, incompletos o hayan dejado de ser necesarios o pertinentes para su finalidad, de conformidad con lo previsto en la legislación en materia de protección de datos. A estos efectos, le rogamos que nos comunique inmediatamente cualquier modificación de sus Datos a fin de que la información contenida en nuestros ficheros esté en todo momento actualizada y no contenga errores.

En los formularios de regida de datos (tanto físicos como electrónicos por medio de la Web), los campos obligatorios vendrán señalados específicamente, por lo que en caso de que el Usuario no facilite los datos correspondientes, FUNDACIÓN JPV podrá a su sola discreción denegar el correspondiente servicio.

ANEXO XVI POLÍTICA DE COOKIES PÁGINA WEB	DOC. DE SEGURIDAD VERSIÓN 2.0

En nuestro sitio Web http://www.fundacionjpv.org/ utilizamos cookies para facilitar la relación de los visitantes con nuestro contenido y para recabar información acerca del uso del sitio web.

En cumplimiento de la **Directiva 2009/136/CE**, desarrollada en nuestro ordenamiento por el apartado segundo del artículo 22 de la Ley de Servicios de Sociedad de la Información, siguiendo las directrices de la Agencia Española de Protección de Datos procedemos a informarle detalladamente del uso que se realiza en nuestra web

¿QUÉ SON LAS COOKIES?

Se **denominan cookies** a unos pequeños archivos que se graban en el navegador utilizado por cada visitante de nuestra web para que el servidor pueda recordar la visita de ese usuario con posterioridad cuando vuelva a acceder a nuestros contenidos. Esta información no revela su identidad, ni dato personal alguno, ni accede al contenido almacenado en su PC, pero sí que permite a nuestro sistema identificarle a usted como un usuario determinado que ya visitó la web con anterioridad, visualizó determinadas páginas, etc. y además permite guardar sus preferencias personales e información técnica como por ejemplo las visitas realizadas o páginas concretas que visite.

Si usted no desea que se guarden cookies en su navegador o prefiere recibir una información cada vez que una cookie solicite instalarse, puede configurar sus opciones de navegación para que se haga de esa forma. La mayor parte de los navegadores permiten la gestión de las cookies de 3 formas diferentes:

- Las cookies son siempre rechazadas;
- El navegador pregunta si el usuario desea instalar cada cookie;
- Las cookies son siempre aceptadas;

Su navegador también puede incluir la posibilidad de seleccionar con detalle las cookies que desea que se instalen en su ordenador. En concreto, el usuario puede normalmente aceptar alguna de las siguientes opciones:

- rechazar las cookies de determinados dominios;
- rechazar las cookies de terceros;
- aceptar cookies como no persistentes (se eliminan cuando el navegador se cierra);
- permitir al servidor crear cookies para un dominio diferente.

TIPOS DE COOKIES Y SU FINALIDAD

COKIES TÉCNICAS: Son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan, como por ejemplo, controlar el tráfico y la comunicación de datos o identificar la sesión.

COOKIES DE PERSONALIZACIÓN: Son aquellas que permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el terminal de usuario, como por ejemplo serían el idioma, el tipo de navegador a través del cual accede el servicio, la configuración regional desde donde accede al servicio, etc.

COOKIES DE ANALISIS: Son aquellas que permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de cookies se utiliza en la mediación de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.

En el caso de las cookies de **Google Analytics**, esta empresa almacena las cookies en servidores ubicados en Estados Unidos y se compromete a no compartirla con terceros, excepto en los casos en los que sea necesario para el funcionamiento del sistema o cuando la ley obligue a tal efecto. Según Google no guarda su dirección IP. Google Inc. es una compañía adherida al Acuerdo de Puerto Seguro que garantiza que todos los datos transferidos serán tratados con un nivel de protección acorde a la normativa europea.

CONSENTIMIENTO

Al navegar y continuar en el sitio web estará consintiendo el uso de las cookies antes enunciadas y en las condiciones contenidas en la presente Política de Cookies.

Annex V. Document de seguretat d'Atticus S.L.

[Protección de Datos de Carácter Personal]

DOCUMENTO DE SEGURIDAD

ATTICUS, S.L.

Versión 2.0

Diciembre 2015

ÍNDICE

1. OBJETO DEL DOCUMENTO

El presente documento responde a la obligación establecida en el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en el que se regulan entre otras, las medidas de seguridad para los ficheros y tratamientos automatizados que contengan datos de carácter personal.

Los ficheros de datos a los que se refiere este documento se encuentran legalmente clasificados como nivel de seguridad **ALTO,** atendiendo a las condiciones descritas en el artículo 81 del Real Decreto citado, siendo por tanto aplicables todas las medidas de seguridad de nivel **ALTO** que se establecen en el Capítulo III del Título VIII, del citado Reglamento.

2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

ATTICUS, S.L. como consecuencia de las actividades desarrolladas dentro de su objeto social, trata información en ficheros que contienen datos de carácter personal que hayan bajo la responsabilidad de ATTICUS, S.L. incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, las personas que intervienen en el tratamiento y los locales en los que se ubican, todo ello que debe ser protegido de acuerdo con lo dispuesto en la normativa vigente.

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

FICHERO	**TIPO DE SISTEMA**	**NIVEL DE SEGURIDAD**
CLIENTES Y/O PROVEEDORES (Dominio GrupoJPV y SAP R/3)	MIXTO	ALTO
RECURSOS HUMANOS (Dominio GrupoJPV)	MIXTO	BÁSICO
VIDEOVIGILANCIA Y CONTROL DE ACCESO	MIXTO	BÁSICO

En el **ANEXO I** (“FICHEROS INSCRITOS EN EL REGISTRO GENERAL DEL PROTECCIÓN DE DATOS”) se describen detalladamente cada uno de los ficheros o tratamientos, juntos con los aspectos que les afecten de manera particular.

Las medidas de seguridad definidas en el presente documento van encaminadas a proteger todos los ficheros, aplicaciones y herramientas de actualización, consulta, recursos del sistema operativo, redes de telecomunicaciones, soportes y equipos informáticos, gestionados por ATTICUS, S.L. o por cualquier otra empresa con la que haya suscrito un contrato de prestación de servicios que conlleve el tratamiento de los datos de carácter personal que componen los ficheros inscritos en el Registro General de Protección de Datos así como las aplicaciones y sistemas que los tratan, los equipos informáticos que la soportan y los locales donde se ubican.

En la actualidad ATTICUS, S.L. ha suscrito diversos contratos de prestación de servicios con terceras entidades actuando en calidad de prestatario, que conllevan el tratamiento de datos de carácter personal de los ficheros de ATTICUS, S.L. por estas entidades.

3. RESPONSABLE DE SEGURIDAD

ATTICUS, S.L. ha designado como responsable de seguridad en materia de protección de datos, en adelante, el "Responsable de Seguridad", a CALPURNIA CONSULTING, S.L., quien se ocupará de la coordinación de todos los asuntos relacionados con esta materia dentro de la organización.

4. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

4.1 Identificación y autentificación

Medidas y normas relativas a la identificación y autentificación del personal autorizado para acceder a los datos personales.

El Responsable del Fichero elabora una relación actualizada de usuarios que tengan acceso autorizados al sistema de información.

El Responsable de Seguridad custodia y actualiza la relación de todos los usuarios de la red que tienen acceso autorizado al sistema de información. Es competencia del Responsable de Seguridad que la atribución y asignación de contraseñas así como la custodia de la relación de usuarios se realice de forma que se garantice su confidencialidad e integridad.

El procedimiento seguido por ATTICUS, S.L. para la identificación y autentificación de los usuarios cuando intentan acceder al sistema o a las aplicaciones, está basada en la combinación de un código de identificación de usuario y una contraseña, en red.

A cada usuario le ha sido asignado un identificador único tanto para el acceso al sistema, como para el acceso a las aplicaciones, no existe un procedimiento para la asignación de contraseñas.

El control de acceso al sistema se limitará a tres (3) intentos fallidos. En caso de agotar los intentos, se procederá a la revocación del usuario que, para volver a acceder al sistema, deberá solicitarlo.

Los números de identificación y claves de acceso asignadas a cada usuario de la red corporativa del Responsable del Fichero, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de las mismas.

Las contraseñas de los usuarios autorizados son alfanuméricas, tienen una longitud mínima de ocho caracteres, se modifican con una periodicidad de 45 días y no es posible la repetición de las cinco últimas contraseñas introducidas. El administrador del sistema informático indica la obligatoriedad de cambio de contraseña en la cuenta del usuario y éste debe cambiarla en el plazo establecido. Durante el tiempo que estén vigentes, las contraseñas se almacenan de forma inteligible.

Este proceso de caducidad de contraseñas lo realiza el Responsable de Seguridad, por medio de los profesionales designados al efecto que tienen las potestades para el acceso a los datos estrictamente necesarios para el desempeño de su trabajo y están sometidos a las mismas obligaciones que el personal de la empresa en materia de protección de datos, especialmente a la del secreto respecto de los datos personales que hubiese podido conocer con motivo de la prestación del servicio. Las contraseñas se almacenan de forma inteligible y cifrada. En el entorno de red se utiliza un mecanismo “desafío-respuesta” HMAC-MD5, de forma que las contraseñas nunca viajan por la red para la transmisión de la información.

Las operaciones susceptibles de seguimiento que se realicen en la red corporativa del Responsable del Fichero quedan registradas en los archivos de registro del servidor (que proporcionan constancia de los accesos a los fichero de la empresa mediante identificación del usuario que accede, la fecha y la hora de acceso si este ha sido autorizado o denegado).

El uso del usuario o la contraseña asignados a cada persona implica la aceptación, como documento probatorio de la operación efectuada, de los registros generados en dichos archivos *LOG* y almacenados en el sistema informático de la empresa. Salvo prueba en contrario, se presume que los actos que se llevan a cabo con el usuario y la contraseña asignados a cada persona implica la aceptación, como documento probatorio de la operación efectuada, de los registros generados en dichos archivos *LOG* y almacenados en el sistema informático de la empresa. Salvo prueba en contrario, se presume que los actos que se lleven a cabo con el usuario y la contrasella asignados han sido realizados en realidad por la persona titular de los mismos.

El Responsable del Fichero posee los mecanismos necesarios para obtener una relación actualizada de los usuarios que tienen acceso autorizado a los sistemas de información de la compañía y establece los procedimientos de identificación y autentificación necesarios para garantizar la seguridad de dicho acceso.

El mecanismo de identificación se basa en la asignación de usuarios a cada una de las personas que acceden a los sistemas de información y el mecanismo de autenticación se basa en la existencia de contraseñas.

Cuando el tratamiento se realiza por el encargado del tratamiento mediante acceso remoto a los sistemas del Responsable del Tratamiento, se ha establecido una limitación, cuyo procedimiento es la incorporación de datos a los sistemas o soportes distintos de los del responsable.

4.2 Gestión de soportes

Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y serán almacenados en los locales bajo el control tanto del encargado del tratamiento como del responsable del tratamiento, lugares de acceso restringido al que solo tendrán acceso las personas autorizadas.

4.3 Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

4.4 Copias de respaldo o recuperación

Se realizarán copias de respaldo y recuperación, salvo que no se hubiese producido ninguna actualización de los datos, este procedimiento se realizará con una periodicidad diaria.

La copia de respaldo se realiza en un soporte extraíble que es depositado en una caja de seguridad ignífuga. Con esta medida se evita la necesidad de traslado de los mismos a otra ubicación fuera de las instalaciones.

En caso de traslado de los soportes físicos estos deberán cifrarse para evitar el acceso a la información que contienen.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizan su construcción en el estado en el que se encontraban al tiempo de producirse la pérdida o destrucción, así como se realizan cifradas para que en caso de sustracción o pérdida sea totalmente imposible descifrarlas. El sistema de copia de seguridad identifica los soportes mediante un sistema de etiquetado.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

4.5 Control de acceso

Los usuarios tanto en la red como en los puestos individuales, deben identificarse y autenticar el acceso a sistemas y aplicaciones, mediante clave de usuario y contraseña, para poder acceder de forma autorizada.

La introducción de una clave distinta a la autorizada impide el acceso a la red, ofreciendo la posibilidad de subsanar errores de teclado, con un límite de tres (3) accesos no autorizados.

El Responsable del Fichero es el encargado del mantenimiento de los usuarios del sistema y aplicaciones en base a los criterios establecidos por la Dirección. Todo usuario estará obligado a bloquear su equipo en el momento en que se va a ausentar de su puesto de trabajo, es decir el equipo deberá estar configurado para que se bloquee automáticamente tras un cierto tiempo de inactividad.

Con el alta de la contraseña de cada usuario se identifica qué grupo de acceso debe ser asignado, tanto para los datos como para el acceso a determinadas aplicaciones.

5. GESTIÓN DE INCIDENCIAS

5.1 Objeto

Al no existir en ATTICUS, S.L., un protocolo a atender cualquier eventualidad que afecte a la seguridad de los daos, el procedimiento será acudir a los asesores informáticos.

No obstante, en ATTICUS, S.L. se recogerán cuantas incidencias de seguridad se produzcan sobre los datos que trata, tales como:

- ✓ Incidencias que afecten a la identificación y autentificación de usuarios.
- ✓ Incidencias que afecten a los derechos de acceso a los datos.
- ✓ Incidencias que afecten a la gestión de soportes.
- ✓ Incidencias que afecten a los procedimientos de copias de seguridad y recuperación.
- ✓ 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.

En este Documento de Seguridad se establecen los mecanismos de actuación por parte de los usuarios de los sistemas de información de ATTICUS, S.L., para la comunicación de las incidencias.

5.2 Ámbito de aplicación

Al igual que en el caso de los ficheros temporales, el Reglamento de Medidas de Seguridad tampoco define el concepto de incidencia. Únicamente se indica como incidencia de seguridad de manera explícita, los procesos de recuperación de datos. ATTICUS, S.L. intentará contemplar en el sentido más amplio del concepto de incidencia, entendió por tal cualquier situación que contravenga las medidas descritas en la normativa de seguridad, así como el mal

funcionamiento de las medidas físicas y lógicas que pudieran afectar a su disponibilidad y 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 afectan a la identificación y autentificación de los usuarios.

  - ✓ Pérdida de confidencialidad de las 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 desactivada.
  - ✓ Detección de contraseñas escritas en los puestos de trabajo,
  - ✓ Revisión de los informes de seguridad.

- Incidencias que afectan a la revisión de soportes:

  - ✓ Comunicación de pérdida de soportes.
  - ✓ Comunicación de localización de soportes en lugares inadecuados.
  - ✓ Errores de contenido en los soportes recibidos.

- Incidencias que afectan a los procedimientos de copias de salvaguardia y recuperación:

  - ✓ Errores en los procesos de realización de copias de salvaguardia.
  - ✓ 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 todos los usuarios de los sistemas de información de ATTICUS, S.L., empleados y colaboradores externos.

5.3 Responsabilidades

- El Responsable de Seguridad es responsable de la redacción y del mantenimiento de este procedimiento, así como su custodia y archivo.
- Todos los usuarios de ATTICUS, S.L., deben informar de cualquier incidencia producida en materia de seguridad.
- El Responsable de Seguridad debe ocuparse del seguimiento de las incidencias en materia de protección de datos de carácter personal.

5.4 Comunidades de incidencias

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. La difusión de la Circular implica que todos los usuarios de ATTICUS, S.L., son conocedores de su obligación de comunicar las incidencias en materia de seguridad al Responsable de Seguridad. Todas las comunicaciones deberán efectuarse al Responsable de Seguridad indicando el momento en que se detectaron y utilizando el medio de comunicación más rápido, a ser posible personal o telefónicamente.
Para que quede constancia de la comunicación, el usuario, además, la realizará por correo electrónico.

5.5 Registros

El Responsable de Seguridad procederá a incluir las incidencias en el registro, y si afectan a la seguridad de los datos de carácter personal, las marcará como tales. 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 incidencias.

El registro contará con los siguientes campos:

- Tipo de incidencia.
- Momento en que se ha producido o se ha detectado la incidencia.
- Persona que la notifica.
- Persona a la que se le notifica.
- Efectos causados por la misma.

También se llevará un registro de resolución de incidencias, que recoja la información sobre las medidas adoptadas. En el caso en que la incidencia implique la ejecución de un proceso de recuperación de datos, el registro de resolución de incidencias contendrá, además, la siguiente información:

- Persona que ejecutó el proceso.
- Datos restaurados.
- En su caso, datos que fue necesario gravar manualmente para su recuperación.

En el **ANEXO II** se recogen los modelos para proceder al registro de incidencias y de su resolución.

6. INFORMACIÓN Y OBLIGACIONES DEL PERSONAL

Con el objeto de dar el debido cumplimiento a la normativa de protección de datos de carácter personal, el Responsable del Fichero impone a su personal el cumplimiento de las siguientes obligaciones, las cuales deberán ser conocidas, aceptadas y respetadas por todo el personal.

6.1 Obligaciones del personal

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

- *ATTICUS, S.L* emitirá una circular donde se recogerán las principales obligaciones en materia de seguridad sobre datos de carácter personal, incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de los recursos informáticos para otras finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral, así como la obligación de mantener el deber de secreto sobre todos los datos tratados con motivo del desempeño de su puesto de trabajo y de no comunicar los referidos datos a ninguna otra persona o entidad sin la autorización pertinente.

Las normas aplicables al personal con acceso a los datos de carácter personal se recogen en el **ANEXO III**, cuyo contenido y detalle se actualiza periódicamente en función de las decisiones empresariales al respecto y de los cambios normativos o jurisprudenciales que, en su caso, se produzcan.

6.2 Información al personal

El Reglamento 1720/2007, dispone la obligación de adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

El Responsable de Seguridad ha sido personalmente informado de las funciones que le han sido asignadas y que figuran en el apartado siguiente al presente Documento de Seguridad.

6.3 Obligaciones del Responsable del Fichero o Responsable del Tratamiento

Además de las que a continuación se detallan, cualesquiera otras obligaciones que le sean atribuidas por la normativa o por el presente Documento:

- ✓ Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.

- ✓ Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por el Responsable del Fichero.
- ✓ Determinar el ámbito del Documento de Seguridad.
- ✓ Determinar y describir los recursos informáticos a los que se aplicará el Documento de Seguridad.
- ✓ Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
- ✓ Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos.
- ✓ Comprobar el cumplimiento de la periodicidad establecida para la realización de copias de respaldo.
- ✓ Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al sistema informático del Responsable del Fichero con especificación del nivel de acceso que tiene cada usuario.
- ✓ Establecer y comprobar la aplicación del procedimiento de identificación y autentificación de usuarios.
- ✓ Establecer y comprobar la aplicación del procedimiento de asignación distribución y almacenamiento de contraseñas.
- ✓ Comprobar el mantenimiento de la confidencialidad de las contraseñas de los usuarios.
- ✓ Establecer y comprobar la aplicación de un procedimiento de cambio periódico de las contraseñas de los usuarios.
- ✓ Establecer y comprobar la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma inteligible.
- ✓ Conceder, alterar o anular el acceso autorizado a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.
- ✓ Establecer y comprobar la aplicación de un sistema que permita identificar, inventariar y almacenar en un lugar seguro de los soportes informáticos que contienen datos de carácter personal.
- ✓ Autorizar la entrada y salida de soportes informáticos que contienen datos de carácter personal.
- ✓ Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas, para el establecimiento de las correspondientes sanciones.
- ✓ Coordinar y controlar las medidas definidas en el Documento de Seguridad.
  Traslado de documentación.

7. CONTRATOS DE PRESTACIÓN DE SERVICIOS.

En este apartado aparece una relación exhaustiva de los datos tratados por terceros, como consecuencia de un contrato de prestación de servicios. A continuación se presenta un modelo de tabla para recoger esta información:

PRESTADOR DEL SERVICIO	FINALIDADES	DATOS FACILITADOS	LUGAR DE TRABAJO	SISTEMA DE TRATAMIENTO
SEGURIN CIA. COMPAÑÍA DE SEGURIDAD, S.A.	VIDEOVIGILANCIA Y CONTROL DE ACCESO A LA SEDE	EMPLEADOS PARTICIPANTES EN LAS ACTIVIDADES REALIZADAS EN EL CENTRO HÍPICO CAVALL FORT	Sede Segurin	MIXTO
JPV INVERSIONES, S.L.	CLIENTES Y PROVEEDORES	CLIENTES Y PROVEEDORES	JPV INVERSIONES, S.L. (Avenida de la Del Percebe, s/n, 08080, Barcelona)	MIXTO
JPV INVERSIONES, S.L.	RECURSOS HUMANOS	EMPLEADOS	JPV INVERSIONES, S.L. (Av. de la Del Percebe, s/n, 08080, Barcelona.)	MIXTO
MARTA PENA VILAJOAN (psicóloga equinoterapia)	PARTICIPANTES EN EQUINOTERAPIA	PATOLOGÍAS PSIQUICAS DE LOS ALUMNOS	Centro hípico CAVALL FORT (St. Quirze del Vallés 2, 08013, Barcelona)	MIXTO

8. GESTIÓN DE LOS PARTICIPANTES EN CURSOS, CAMPAMENTOS Y EQUINOTERAPIA ORGANIZADOS POR ATTICUS, S.L.

8.1 Inscripción de alumnos en la escuela de equitación/ campamentos de verano

Únicamente el Responsable de Seguridad tiene competencias para dar de alta los identificadores de participantes en los cursos de equitación y asociarlos a perfiles definidos para los distintos niveles de acceso a las aplicaciones y ficheros.

Los responsables directos de los usuarios que tengan que dar de alta a un nuevo alumno en el sistema o a las aplicaciones, deberán notificárselo al Responsable de Seguridad, empleando el modelo establecido al efecto e indicando en la solicitud los derechos de acceso, rectificación, cancelación y oposición. Será la dirección de la empresa quien tenga la última decisión sobre los derechos ARCO.

Los prestadores de servicios, tienen acceso total a todos los datos de los alumnos, siendo su función legalmente la de encargados de tratamiento pero a la vez alimentan la base de datos.

El procedimiento de inscripción se realiza cumplimentando el formulario que se adjunta a este Documento de Seguridad como **ANEXOS XVIII, XIX y XX.** Asimismo, dicho formulario figura accesible en la página web del centro hípico CAVALL FORT.

Igualmente, los alumnos participantes en la escuela de equitación y los participantes en el campamento de verano, deberán firmar un formulario de autorización de captación de imágenes para menores que deberá ser firmado por sus representantes legales en caso de ser menores de edad, y que se adjuntan como **ANEXO XIII y ANEXO XIV.**

En los referidos formularios únicamente se requieren datos de nivel BÁSICO.

8.2 Inscripción de los alumnos en Equitación Terapéutica Adaptada

Únicamente el Responsable de Seguridad tiene competencias para dar de alta los identificadores de participantes en los cursos de equitación y asociarlos a perfiles definidos para los distintos niveles de acceso a las aplicaciones y ficheros.

Los responsables directos de los usuarios que tengan que dar de alta a un nuevo alumno en el sistema o en las aplicaciones, deberán notificárselo al Responsable de Seguridad, empleando el modelo establecido al efecto e indicando en la solicitud los derechos de acceso, rectificación, cancelación y oposición. Será la dirección de la empresa quien tenga la última decisión sobre los derechos arco.

Los prestadores de servicios, en este caso, el psicólogo/a que da las clases de equitación terapéutica, tiene acceso total a los datos de los alumnos, incluidos los datos de salud y los médicos, siendo su función legal la de encargado/a de tratamiento pero a la vez alimenta la base de datos, y en este caso concreto, alimenta la base de datos con datos de **NIVEL ALTO**.

Los participantes en este tipo de actividad deben cumplimentar un formulario donde se recoge la autorización para la comunicación de apoyo para el psicólogo/a.

En esta actividad se recaban datos de salud de los participantes, lo cual implica la obligación de adoptar medidas de seguridad de **NIVEL ALTO**.

Al ser datos no automatizados, estos deberán estar siempre almacenados y guardados en un armario bajo llave, al que solo puedan tener acceso el encargado del tratamiento y el responsable del mismo. En ningún momento pueden facilitarse los soportes físicos que contengan esos datos a la vista de personas ajenas al tratamiento de los mismos.

Asimismo, tanto la psicóloga/o y los empleados que traten a los datos de carácter personal de nivel alto de los alumnos, además del contrato deberán firmar un acuerdo de confidencialidad como encargados del tratamiento de datos de carácter personal de **NIVEL ALTO** el referido acuerdo de confidencialidad se adjunta a este Documento de Seguridad como **ANEXO V.3.**

8.3 Concursos

A lo largo del año se organizan tres concursos hípicos: El Concurso de Salto Internacional de Verano, El Concurso de Salto Internacional de Invierno y la Liga Trofeo CAVALL FORT.

La participación en los dos primeros concursos se realiza a través de la correspondiente inscripción de los jinetes en los mismos. Para ello deben cumplimentar la Hoja de Registro de Jinetes, en la que se recogen sus datos personales, bancarios y de los caballos con los que van a participar. Por tanto, y con el objeto de cumplir con el deber de información exigible al responsable del fichero, se incluye en dicho formulario de inscripción una cláusula relativa al tratamiento de sus datos, la cual se adjunta como **ANEXO XXV** en el presente Documento de Seguridad.

El concurso Liga Trofeo CAVALL FORT tiene como participantes jinetes jóvenes. La inscripción de los mismos en el concurso se realiza a través de la cumplimentación de una hoja de inscripción en la que se recogen los datos del jinete y los de domiciliación bancaria necesaria para realizar la facturación de los costes de participación en el concurso y el abono de los posibles premios. Por tanto, y al igual que en el supuesto anterior, se incluye en dicho formulario la misma cláusula adjunta como **ANEXO XXV**.

La organización de todas las competiciones y eventos hípicos antes mencionados se lleva a cabo a través de la empresa JUMP SPORT, S.L. (en adelante, “JUMP”), con quien ATTICUS ha firmado el correspondiente contrato de prestación de servicios. Asimismo,

JUMP tiene desplazados dos trabajadores en las instalaciones del Centro Hípico CAVALL FORT con la finalidad de desarrollar la actividad organizativa. Para prestar todos los servicios objeto del contrato, JUMP debe acceder a los datos que se encuentran en los ficheros titularidad de ATTICUS por lo que actuará como encargado del tratamiento. Este tratamiento está amparado en el Pacto 8º *Tratamiento automatizado de datos*, el cual se recoge en el contrato firmado entre ambos el 13 de febrero de 2013.

9. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a la normativa vigente en cada momento sobre protección de datos de carácter personal.

ANEXO I FICHEROS INSCRITOS EN EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS	DOC. DE SEGURIDAD VERSIÓN 2.0

En el presente Anexo se recoge información relativa a los ficheros responsabilidad de ATTICUS, S.L. que se hallan inscritos en el Registro General de Protección de Datos, indicando el entorno donde se encuentran ubicados y las aplicaciones que los gestionan.

NOMBRE DEL FICHERO	**DATOS TRATADOS**	**FECHA DE INSCRIPCIÓN**	**CÓDIGO DE INSCRIPCIÓN**	**UBICACIÓN Y MODO DE TRATAMIENTO**	**NIVEL DE SEGURIDAD**
CLIENTES Y/O PROVEEDORES	Datos de clientes y suministradores de la sociedad			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	ALTO
RECURSOS HUMANOS	Datos del personal de la sociedad			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	BÁSICO
VIDEOVIGILANCIA	Datos de empleados y personas ajenas a la sociedad que accedan a los edificios			**Ubicación:** Responsable del fichero **Modo de tratamiento:** Mixto	MEDIO

ANEXO II REGISTRO DE INCIDENCIAS	DOC. DE SEGURIDAD VERSIÓN 2.0

NOTIFICACIÓN Y REGISTRO DE INCIDENCIAS	
Numero de incidencia:	
Fecha de notificación: Hora:	
Usuario que realiza la notificación:	
Personas a las que se le comunica la incidencia:	
DESCRIPCION DE LA INCIDENCIA	
Fecha de la incidencia: Hora:	
Tipo de incidencia (intrusión, pérdida de datos, etc.):	
Descripción detallada de la incidencia:	
Posibles efectos de la incidencia	
Firma del notificante:	Firma receptor:

REGISTRO DE RESOLUCION DE INCIDENCIAS		
Numero de incidencia:		
Medidas adoptadas y pasos realizados:		
Resultado de las medidas:		
Fecha de resolución:		
RECUPERACION DE DATOS: **(A rellenar solo si procede. Precisa de autorización del Responsable del fichero)**		
Procedimiento realizado:		
Fecha de realización:		
Datos restaurados:		Datos grabados manualmente:
Persona que realiza el procedimiento:		
Fecha y lugar:	Firma del Responsable del Fichero:	

ANEXO III NORMAS APLICABLES A PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL	DOC. DE SEGURIDAD VERSIÓN 2.0

El Documento de Seguridad de ATTICUS, S.L. enumera detalladamente las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal con arreglo a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y al Real Decreto 1720/2007, por el que se aprobó el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El personal sobre el que recaen dichas obligaciones y funciones podrá acceder al contenido del Documento de Seguridad, siempre previa solicitud al Responsable de Seguridad. No obstante, y a efectos aclaratorios, en el presente Anexo se recogen las principales obligaciones en materia de protección de datos de carácter personal para conocimiento directo de los trabajadores, quienes deberán dar íntegro cumplimiento a las mismas:

OBLIGACIONES DEL PERSONAL CON ACCESO A DATOS DE CARÁCTER PERSONAL

CONTRASEÑAS:

1) Las contraseñas de los usuarios serán personales e intransferibles.
2) Las contraseñas deberán ser alfanuméricas y tener una longitud máxima de ocho caracteres.
3) Las contraseñas caducarán cada 45 días, momento en el cual el usuario deberá designar una nueva contraseña que no podrá coincidir con las últimas cinco contraseñas introducidas.

EQUIPOS INFORMÁTICOS:

4) Se prohíbe al personal la instalación de cualquier tipo de aplicación en los equipos informáticos sin autorización previa.
5) Se prohíbe la utilización de los equipos y soportes informáticos para finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral.
6) Los usuarios estarán obligados a bloquear su equipo en el momento de ausentarse de su puesto de trabajo, requiriendo la introducción de usuario y contraseña para volver a acceder al equipo.

SECRETO Y CONFIDENCIALIDAD:

7) Los usuarios deberán mantener el secreto sobre todos los datos tratados con motivo del desempeño de su puesto de trabajo.
8) No podrán, asimismo, comunicar los referidos datos a ninguna otra persona o entidad, salvo autorización pertinente.

INCIDENCIAS:

9) Los usuarios deberán informar al Responsable de Seguridad sobre cualquier incidencia producida en materia de seguridad de acuerdo con el procedimiento establecido en el punto 4.4 del Documento de Seguridad.
10) Los usuarios deberán participar en la implantación y seguimiento de la política de seguridad mediante la firma de la Circular que les será entregada a cada uno.

OTROS:

11) Todas las obligaciones anteriores deberán mantenerse, incluso tras la extinción de la relación laboral con ATTICUS, S.L..
12) El trabajador será responsable tanto frente a ATTICUS, S.L., como frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores, pudiendo ATTICUS, S.L. reclamar las indemnizaciones pertinentes.

Para cualquier aclaración al respecto se puede contactar con la Responsable de Seguridad, CALPURNIA CONSULTING, S.L.

ANEXO IV CIRCULAR A LOS TRABAJADORES	DOC. DE SEGURIDAD VERSIÓN 2.0

Nombre: _____ NIF: _____

En mi capacidad de empleado (ya sea fijo, o temporal) y en consideración de la relación laboral que mantengo con ATTICUS, S.L., así como del acceso que se me permite a sus Bases de Información, constato que:

- Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja ATTICUS, S.L. En concreto he leído, entiendo y me comprometo a cumplir los Procedimientos de Seguridad de los Sistemas de Información que corresponden a mi función en la empresa (Descritos en el Documento de Seguridad).

- Entiendo que el incumplimiento de cualesquiera de las normas aplicables al personal con acceso a datos de carácter personal incluidas todas ellas en el Documento de Seguridad de ATTICUS, S.L., intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empresa y la posible reclamación por parte de la misma de los daños causados.

En_____, a __ de_____ de 20__.

Firma,

El empleado/a

ANEXO V ACUERDO DE CONFIDENCIALIDAD (TRABAJADORES Y ENCARGADOS DEL TRATAMIENTO)	DOC. DE SEGURIDAD VERSIÓN 2.0

1) ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO:

En _____, a___ de _____ de 20__.

ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO

REUNIDOS

De una parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

De otra parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

INTERVIENEN

La primera lo hace en nombre y representación de ATTICUS, S.L., con domicilio en Avda. Del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº B-00000003, en su calidad de _____ de la sociedad.

La segunda lo hace en nombre y representación de _____, con domicilio social en _____, y CIF nº _____, en su calidad de _____ de la sociedad (en adelante, el "**Encargado del Tratamiento**").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que las Partes se hallan vinculadas por un contrato de prestación de servicios de fecha ___ de _____ de _____, en virtud del cual el Encargado del Tratamiento se obligaba al tratamiento de datos por cuenta del responsable de los ficheros, esto es ATTICUS, S.L.

II.- Que, el artículo 10 de La Ley Orgánica de Protección de Datos de Carácter Personal (en adelante, "LOPD"), en su artículo 10 refiriéndose al deber de secreto, establece la obligación al secreto profesional y al deber de guardar los datos, por parte de todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal.

III.- Que, en cumplimiento de lo establecido en la LOPD, las Partes suscriben el presente Acuerdo de Confidencialidad, de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- INFORMACIÓN CONFIDENCIAL.

Se considerará información confidencial a toda aquella a la que el Responsable del Tratamiento acceda con motivo de la realización de sus funciones y obligaciones, independientemente del soporte en el que esté contenida.

SEGUNDA.- OBLIGACIÓN DE SECRETO.

El Encargado del Tratamiento no podrá revelar a persona alguna ajena a ATTICUS, S.L., cualesquiera datos confidenciales, protegidos por la LOPD, a los que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

TERCERA.- USO DE LA INFORMACIÓN.

El Encargado del Tratamiento se limitará a utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en relación al contrato de prestación de servicios suscrito con ATTICUS, S.L. No pudiendo disponer de tal información de ninguna otra forma o con otra finalidad.

CUARTA.- DURACIÓN.

Las obligaciones contenidas en el presente Acuerdo seguirán rigiendo de manera indefinida en el tiempo, aun tras la finalización de la relación contractual entre las Partes.

QUINTA.- INCUMPLIMIENTOS.

En caso de incumplimiento, el Responsable del Tratamiento se hace responsable ante cualquier daño que pueda ocasionar tanto a ATTICUS, S.L., como a terceros, debiendo resarcir a ATTICUS, S.L., de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y en prueba de conformidad, ambas partes firman el presente documento por duplicado, a un solo efecto y en lugar y fecha ut supra.

_____	_____
Fdo. D./Dña. _____	Fdo. D./Dña._____
EL RESPONSABLE DEL TRATAMIENTO	**ATTICUS, S.L.**

2) ACUERDO DE CONFIDENCIALIDAD CON TRABAJADORES:

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD. 15/99), en su artículo 10 refiriéndose al Deber de Secreto, establece que:

> "*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*

Como consecuencia de lo anterior, el abajo firmante, D/Dña _____, con DNI _____, y domicilio en _____ en el marco de la **relación laboral** que le une con ATTICUS, S.L., se compromete a:

PRIMERA.- Teniendo en cuenta que los datos de carácter personal, tanto automatizados como en soporte papel, a los cuales va a tener acceso, en muchos casos son considerados por la legislación vigente en materia de protección de datos, como especialmente protegidos, se establece en la presente cláusula la obligatoriedad de no revelar a persona alguna ajena a ATTICUS, S.L., la información referente a la que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones del abajo firmante o a las impuestas por las leyes o normas que resulten de aplicación; o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

SEGUNDA.- Utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en ATTICUS, S.L., y no disponer de ella de ninguna otra forma o con otra finalidad.

TERCERA.- No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado, y que no sea necesaria para el desempeño de sus funciones en ATTICUS, S.L.

CUARTA.- Cumplir, en el desempeño de sus funciones en ATTICUS, S.L., la normativa vigente relativa a la Protección de Datos de Carácter Personal y, en particular la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y disposiciones complementarias o cualquier otra norma que la sustituya en el futuro.

QUINTA.- Cumplir los compromisos anteriores incluso después de extinguida, por cualquier causa, la relación laboral que le une con ATTICUS, S.L.

SEXTA.- El trabajador transmite a ATTICUS, S.L. que adquiere, todos los derechos que pudieran corresponderle sobre los programas de ordenador, aplicaciones informáticas y bases de datos desarrolladas por aquel en el marco de su relación laboral, trabajos, informes, estando estos

realizados utilizando medios y recursos a los que haya tenido acceso con ocasión de su vinculación con ATTICUS, S.L.

SÉPTIMA.- El trabajador, se compromete a guardar Deber de Secreto, en concordancia con lo estipulado en el artículo 10 de la LOPD, de la información a la que tenga acceso en el desempeño de sus funciones en ATTICUS, S.L.

OCTAVA.- El abajo firmante se hace responsable frente a ATTICUS, S.L., y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores y resarcirá a ATTICUS, S.L., de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y para que surta plenos efectos, firmo la presente declaración,

En _____, a___ de _____ de 20__.

Firma del trabajador

Fdo.: D/Dña:

3) ACUERDO DE CONFIDENCIALIDAD CON TRABAJADORES CON ACCESO A DATOS DE NIVEL ALTO:

En _____, a___ de _____ de 20__.

ACUERDO DE CONFIDENCIALIDAD CON ENCARGADOS DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DE NIVEL ALTO

REUNIDOS

De una parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

De otra parte, D./Dña._____, con DNI nº _____ y domicilio en _____.

INTERVIENEN

La primera lo hace en nombre y representación de ATTICUS, S.L., con domicilio en Avda. Del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº B-00000003, en su calidad de _____ de la sociedad.

La segunda lo hace en nombre y representación de _____, con domicilio social en _____, y CIF nº _____, en su calidad de _____ de la sociedad (en adelante, el "**Encargado del Tratamiento**").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que las Partes se hallan vinculadas por un contrato de prestación de servicios de fecha ___ de _____ de _____, en virtud del cual el Encargado del Tratamiento se obligaba al tratamiento de datos de carácter personal de nivel alto por cuenta del responsable de los ficheros, esto es ATTICUS, S.L.

II.- Que, el artículo 10 de La Ley Orgánica de Protección de Datos de Carácter Personal (en adelante, "LOPD"), en su artículo 10 refiriéndose al deber de secreto, establece la obligación al secreto profesional y al deber de guardar los datos, por parte de todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal.

III.- Que, en cumplimiento de lo establecido en la LOPD, las Partes suscriben el presente Acuerdo de Confidencialidad, de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- INFORMACIÓN CONFIDENCIAL.

Se considerará información confidencial a toda aquella a la que el Encargado del Tratamiento acceda con motivo de la realización de sus funciones y obligaciones, independientemente del soporte en el que esté contenida.

SEGUNDA.- OBLIGACIÓN DE SECRETO.

El Encargado del Tratamiento no podrá revelar a persona alguna ajena a ATTICUS, S.L., cualesquiera datos confidenciales, protegidos por la LOPD, a los que haya tenido acceso en el desempeño de sus funciones, excepto en el caso de que ello sea necesario para dar debido cumplimiento a obligaciones impuestas por las leyes o normas que resulten de aplicación, o sea requerido para ello por mandato de la autoridad competente con arreglo a Derecho.

TERCERA.- USO DE LA INFORMACIÓN.

El Encargado del Tratamiento se limitará a utilizar la información a la que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en relación al contrato de prestación de servicios suscrito con ATTICUS, S.L. No pudiendo disponer de tal información de ninguna otra forma o con otra finalidad.

CUARTA.- DURACIÓN.

Las obligaciones contenidas en el presente Acuerdo seguirán rigiendo de manera indefinida en el tiempo, aun tras la finalización de la relación contractual entre las Partes.

QUINTA.- INCUMPLIMIENTOS.

En caso de incumplimiento, el Encargado del Tratamiento se hace responsable ante cualquier daño que pueda ocasionar tanto a ATTICUS, S.L., como a terceros, debiendo resarcir a ATTICUS, S.L., de las indemnizaciones, sanciones o reclamaciones que ésta se vea obligada a satisfacer como consecuencia de dicho incumplimiento.

Y en prueba de conformidad, ambas partes firman el presente documento por duplicado, a un solo efecto y en lugar y fecha ut supra.

_____	_____
Fdo. D./Dña. _____	Fdo. D./Dña._____
EL RESPONSABLE DEL TRATAMIENTO	**ATTICUS, S.L.**

ANEXO VI INVENTARIO DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

En el presente Anexo se inventariarán los soportes que contengan datos de carácter personal de manera detallada, de acuerdo con el siguiente cuadro de información:

NOMBRE DE LA ETIQUETA	**CONTENIDO DEL SOPORTE**	**TIPO DE SOPORTE**	**UBICACIÓN**	**FRECUENCIA DE UTILIZACIÓN**	**PROCEDIMIENTO DE DESTRUCCIÓN DEL SOPORTE**	**FECHA DE ALTA Y DE BAJA**	**CIFRADO**
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □
							Sí □ No □

En caso de soportes cuya especial naturaleza impida su correcto registro según lo establecido más arriba, se procederá a dejar constancia de tal situación, indicando los aspectos que se puedan especificar.

ANEXO VII REGISTRO DE ENTRADA Y SALIDA DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

REGISTRO DE ENTRADA

Nº DE SOPORTES	**FECHA**	**HORA**	**TIPO DE SOPORTE**	**REMITENTE**	**MODO DE ENVÍO**	**CONTENIDO**	**RECEPTOR**	**DEPARTAMENTO**	**ESTADO**

REGISTRO DE SALIDA

Nº DE SOPORTES	FECHA	HORA	TIPO DE SOPORTE	DESTINATARIO	MODO DE ENVÍO	CONTENIDO	EMISOR	DEPARTAMENTO

ANEXO VIII SALIDAS AUTORIZADAS DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

La dirección de ATTICUS, S.L., ha aprobado la relación de salidas periódicas de soportes que contienen datos de carácter personal que han sido autorizados por la entidad.

A continuación se presenta la relación que será actualizada cada vez que se produzcan modificaciones al respecto.

DATOS ENVIADOS	DESTINATARIO	PERIODICIDAD

ANEXO IX CONTROL DE ENTRADA / SALIDA DE SOPORTES	DOC. DE SEGURIDAD VERSIÓN 2.0

CONTROL DE ENTRADA / SALIDA DE SOPORTES

Referencia Nº _____ **Fecha y hora de la operación** _____

ENTRADA ☐ **SALIDA** ☐ **DEVOLUCIÓN** ☐

TIPO DE SOPORTES _____ **NÚMERO DE SOPORTES** _____

NÚMERO DE IDENTIFICACIÓN DEL SOPORTE _____

CONTENIDO _____

FINALIDAD _____

FICHERO DEL QUE PROCEDEN LOS DATOS _____

IDENTIFICACIÓN DE LA DELEGACIÓN / ENTIDAD (ORIGEN / DESTINO)

NOMBRE DELEGACIÓN / ENTIDAD _____

DESTINATARIO _____

DIRECCIÓN _____

TELEFONO DE CONTACTO _____

DATOS DEL RESPONSABLE DE LA ENTREGA / RECEPCIÓN (AUTORIZADO)

NOMBRE Y APELLIDOS _____

CARGO / PUESTO _____

PERSONA QUE AUTORIZA _____

FECHA DE ENTRADA _____ /_____ / _____

FECHA DE SALIDA _____ / _____ /_____

FECHA DE DEVOLUCIÓN _____ /_____ /_____

FORMA Y PRECAUCIONES DE ENVÍO _____

OBSERVACIONES _____

_____

_____

Fdo. _____

ANEXO X MODELO DE CONTRATO DE ENCARGADO DEL TRATAMIENTO DE LOS DATOS POR CUENTA DE TERCEROS.	DOC. DE SEGURIDAD VERSIÓN 2.0

En _____, a __ de _____ de 20__.

CONTRATO DE ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

REUNIDOS

De una parte, D./Dña._____, con D.N.I_____, que actúa en nombre y representación de ATTICUS, S.L., con domicilio en Avda. Del Percebe, s/n, C.P. 08080, Barcelona, y con CIF nº B-00000003, en su calidad de _____, (en adelante, "EL RESPONSABLE DEL FICHERO").

Y de otra parte, D./Dña._____, con D.N.I_____, que actúa en nombre y representación de (SOCIEDAD), con domicilio social en_____, Y con C.I.F. nº _____, en su calidad de _____, (en adelante, "EL ENCARGADO DEL TRATAMIENTO").

En adelante, a los intervinientes se denominarán conjuntamente como las "Partes".

Las Partes se reconocen recíprocamente la capacidad legal necesaria para otorgar el presente Acuerdo de Confidencialidad (en adelante "el Acuerdo") y

EXPONEN

I.- Que ambas Partes se hallan vinculadas por un contrato de prestación de servicios, en virtud del cual la (SOCIEDAD) tiene acceso a datos de carácter personal protegidos por la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (en adelante, "LOPD").

II.- Que, las Partes han acordado la suscripción del presente contrato de Acceso a los Datos por Cuenta de Terceros en cumplimiento con lo dispuesto en el artículo 12 de la LOPD, para el tratamiento de dichos datos de carácter personal, cumpliendo con los requisitos legales correspondientes y de acuerdo con las siguientes

CLÁUSULAS

PRIMERA.- DEFINICIONES.

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.

SEGUNDA.- OBJETO.

El objeto del presente contrato es el tratamiento por parte de EL ENCARGADO DEL TRATAMIENTO de los datos personales relativos a: _____ con la finalidad de poder realizar los servicios contratados, para lo cual previamente deberá ésta poner a disposición del encargado del tratamiento dichos datos personales.

Dicho tratamiento se realizará de conformidad con lo establecido en la LOPD y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante "RLOPD"), o normativa que los sustituya.

TERCERA.- DATOS A LOS QUE SE DA ACCESO Y NIVEL DE SEGURIDAD.

Los datos personales que forman parte de los ficheros del RESPONSABLE DEL FCHERO, a los que tendrá acceso el encargado del tratamiento son los siguientes:

- Fichero: _____.
    - Datos afectados por el tratamiento: _____.
    - Nivel de seguridad: _____.
- Fichero: _____.
    - Datos afectados por el tratamiento: _____.
    - Nivel de seguridad: _____.

CUARTA.- OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO.

4.1 EL ENCARGADO DEL TRATAMIENTO solamente tratará los datos que se le han encomendado conforme a las instrucciones del responsable del fichero.

4.2 Los datos facilitados no se aplicarán ni utilizarán con una finalidad diferente a la que figura en este documento, ni EL ENCARGADO DEL TRATAMIENTO los comunicará, ni siquiera a efectos de su conservación, a terceros.

4.3 EL ENCARGADO DEL TRATAMIENTO y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de los datos que les han sido confiados para su tratamiento.

4.4 EL ENCARGADO DEL TRATAMIENTO deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural. Las medidas de

seguridad que deberán ser observadas dependerán del nivel de seguridad de los datos objeto de tratamiento, por ello, dichas medidas podrán ser de nivel básico, medio o alto, según lo estipulado en la LOPD y el RLOPD.

4.5 En caso de resolución del presente contrato, los datos serán destruidos en su totalidad o devueltos al RESPONSABLE DEL FICHERO, teniendo en cuenta los distintos soportes o documentos donde estos puedan constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc.

4.6 Una vez se haya realizado la operación mencionada en el punto anterior, EL ENCARGADO DEL TRATAMIENTO se compromete a entregar una declaración por escrito al RESPONSABLE DEL FICHERO donde conste que así se ha realizado.

4.7 Será de aplicación en todo caso, en lo no previsto en este contrato, la normativa vigente en materia de protección de datos personales.

4.8 En el caso de que EL ENCARGADO DEL TRATAMIENTO incumpla con las obligaciones antes establecidas, pasará a tener la consideración de responsable del tratamiento o fichero, respondiendo de las infracciones en que hubiera incurrido personalmente.

QUINTA.- DURACIÓN Y RESOLUCIÓN DEL CONTRATO.

El presente contrato se considera accesorio del contrato de prestación de servicios de existente entre las partes, por lo que su duración y extinción queda supeditada al mismo.

SEXTA.- LEY APLICABLE Y FORO.

El presente contrato se regirá e interpretará conforme a la legislación española vigente, en aquello que no esté expresamente regulado, sometiéndose las partes, para todas las controversias que pudieran surgir en relación con el mismo, a la competencia de los Juzgados y Tribunales de la ciudad de Barcelona, con renuncia a cualquier otro foro que les pudiera corresponder.

Y en prueba de su conformidad, firman las partes el presente contrato en duplicado ejemplar y a un sólo efecto, en lugar y fecha señalados en el encabezamiento.

ATTICUS, S.L.	**(_____)**
EL RESPONSABLE DEL FICHERO	**EL ENCARGADO DEL TRATAMIENTO**

ANEXO XI CLÁUSULA LOPD PARA E-MAILS/FAX	DOC. DE SEGURIDAD VERSIÓN 2.0

La información contenida en este mensaje y en cualquier archivo o documento que se adjunte al mismo es confidencial y privilegiada.

Esta dirigida exclusivamente para el uso privado del destinatario y no debe ser diseminada o utilizada por otra personal.

ATTICUS, S.L. no garantiza la transmisión de mensajes electrónicos en forma segura y libre de errores debido a que la información puede ser interceptada, dañada, perdida, destruida, pueda llegar tarde, incompleta, o conteniendo virus.

ATTICUS, S.L. no acepta responsabilidad por cualquier error u omisión en el contenido de este mensaje, que puede surgir como resultado de la transmisión de este mensaje electrónico.

Los empleados y usuarios del sistema de correo electrónico/fax están expresamente advertidos de no crear o enviar enunciados difamatorios y de no cometer ninguna violación a los derechos de autor u otras disposiciones legales, a través de comunicaciones por mensaje electrónico/fax. Cualquier comunicado de esta naturaleza es contrario a la política de ATTICUS, S.L., esta no acepta ninguna responsabilidad.

ANEXO XII CLÁUSULA LOPD PARA FACTURAS	DOC. DE SEGURIDAD VERSIÓN 2.0

En cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le comunicamos que los datos que usted nos facilite quedarán incorporados y serán tratados en los ficheros titularidad de ATTICUS, S.L. con el fin de poderle prestar nuestros servicios, así como para mantenerle informado sobre cuestiones relativas a la actividad de la Empresa. ATTICUS, S.L. se compromete a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros.

Asimismo, le informamos de la posibilidad que tiene de ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal de forma presencial en las oficinas de ATTICUS, S.L., acompañando copia de DNI, o bien mediante correo postal dirigido a: Av. Del Percebe, s/n, 08080, Barcelona.

ANEXO XIII AUTORIZACIÓN A TRATAMIENTO DE IMÁGENES DE MENORES DE EDAD	DOC. DE SEGURIDAD VERSIÓN 2.0

Por otra parte, ATTICUS, S.L. informa a los interesados que, de acuerdo con la LOPD y con la Ley 1/1982 de protección civil, derecho al honor, intimidad personal y familiar y la propia imagen, durante la estancia del menor podrán realizarse fotografías y grabaciones del campamento o actividades en las que participen los menores de edad. Dichas imágenes y/o grabaciones podrán ser publicadas en los medios de comunicación de ATTICUS, S.L., convencionales y electrónicas (Internet) que ATTICUS, S.L. estime convenientes, para dar publicidad al referido campamento o actividad.

ATTICUS, S.L. advierte al padre/madre/tutor/ representante legal que la publicación de las fotografías y/o grabaciones mencionadas implica la cesión de dichos datos a terceros y en particular, a las personas físicas y/o jurídicas que accedan a los mismos desde cualquier país, incluidos los sitios fuera del territorio del Espacio Económico Europeo o en Estados que no ofrecen un nivel adecuado de protección conforme a lo previsto en la normativa vigente sobre protección de datos personales.

ATTICUS, S.L. necesita contar con la autorización expresa de los interesados para poder realizar los tratamientos descritos, por lo que se ruega al interesado que marque la casilla correspondiente:

☐ Autorizo a la realización de fotografías y grabaciones del campamento o actividad en las que participen los menores de edad. Dichas imágenes y/o grabaciones podrán ser publicadas en los medios de comunicación de ATTICUS, S.L., electrónicos o no.

☐ No autorizo al tratamiento de imágenes arriba señalado en el correspondiente campamento o actividad.

ANEXO XIV AUTORIZACIÓN AL TRATAMIENTO DE IMÁGENES	DOC. DE SEGURIDAD VERSIÓN 2.0

D/Dª _____con DNI número _____

ATTICUS, S.L. informa a los interesados que, de acuerdo con la LOPD y con la Ley 1/1982 de protección civil, derecho al honor, intimidad personal y familiar y la propia imagen, durante su estancia podrán realizarse fotografías y grabaciones de las actividades en las que usted participe. Dichas imágenes y/o grabaciones podrán ser publicadas en los medios de comunicación de ATTICUS, S.L., convencionales y electrónicas (Internet), que ATTICUS, S.L. estime convenientes, para dar publicidad a la referida actividad.

ATTICUS, S.L. necesita contar con la autorización expresa de los interesados para poder realizar los tratamientos descritos, por lo que se ruega al interesado que marque la casilla correspondiente:

☐ Autorizo a la realización de fotografías y grabaciones en las actividades en las que yo participe. Dichas imágenes y/o grabaciones podrán ser publicadas en los medios de comunicación de ATTICUS, S.L. electrónicos o no.

☐ No autorizo al tratamiento de imágenes arriba señalado en la correspondiente actividad.

1. Información legal y aceptación.

Las presentes disposiciones regulan el uso del servicio de la web corporativa (en adelanta, la "Web Corporativa" o la "Web") que ATTICUS, S.L., (en adelante, ATTICUS) pone a disposición de los usuarios de Internet. ATTICUS con domicilio social en Avd. da Del Percebe, s/n, 08080, Barcelona, C.I.F. número B-00000003 está inscrita en el Registro Mercantil de Barcelona.

La utilización de la Web atribuye la condición de usuario de la Web (en adelante, el "Usuario") e implica la aceptación de todas las condiciones incluidas en este Aviso Legal. La prestación del servicio de la Web tiene una duración limitada al momento en el que el Usuario se encuentre conectado a la Web o a alguno de los servicios que a través del mismo se facilitan. Por tanto, el Usuario debe leer atentamente el presente Aviso Legal en cada una de las ocasiones en que se proponga utilizar la Web, ya que éste y sus condiciones de uso recogidas en el presente Aviso Legal pueden sufrir modificaciones.

2. Objeto.

El objeto de las presente condiciones generales es regular el uso que puede realizar los Usuarios de la Web corporativa de ATTICUS que actualmente se encuentra en la URL www.cavallfort.com, sin perjuicio de que ciertos servicios o contenidos dentro de la Web Corporativa se sometan a sus propias condiciones particulares, reglamentos e instrucciones que, en su caso, sustituyen, complementan y/o modifican el presente Aviso Legal y que deberán ser aceptadas por el Usuario antes de iniciarse la prestación del servicio correspondiente.

3. Acceso.

El acceso y el uso de la Web Corporativa, tiene carácter gratuito para los Usuarios (salvo en lo relativo al coste de conexión a través de la red de telecomunicaciones suministrada por el proveedor de acceso contratado por los usuarios) y no exige el registro previo del usuario con carácter general. No obstante, el acceso y uso de determinadas informaciones y servicios ofrecidos a través de la Web Corporativa solo pueden hacerse previo registro del usuario.

En caso del registro de usuarios a través de identificadores y contraseñas, tanto el identificador como la contraseña pertenecerán exclusivamente a la persona a la que se le conceden. El usuario deberá mantener bajo su exclusiva responsabilidad tanto el identificador como la contraseña en la más estricta y absoluta confidencialidad, asumiendo,

por tanto, cuantos daños o consecuencias de todo tipo se deriven del quebrantamiento o revelación del secreto.

4. Propiedad intelectual e industrial.

Todos los contenidos de la Web, entendiendo por estos a título meramente enunciativo los textos, fotografías, software, links y demás contenidos audiovisuales o sonoros, así como su diseño gráfico, códigos fuente, estructuras de navegación y demás servicios o productos telemáticos integrados en la Web Corporativa (en adelante, los "Contenidos") son propiedad exclusiva de ATTICUS o de terceros, sin que pueda entenderse cedidos al usuario ninguno de los derechos de explotación reconocidos por la normativa vigente en materia de propiedad intelectual sobre los mismos, salvo aquellos que resulten estrictamente necesarios para el uso del la Web, por lo que el usuario se compromete a no infringir ningún derecho derivado de la propiedad intelectual o industrial, quedando expresamente prohibida la reproducción total o parcial de los mismos, su comunicación pública, distribución o cualquier forma de explotación, salvo consentimiento expreso y por escrito por parte de ATTICUS, S.L. El usuario se compromete a utilizar dicha información y servicios exclusivamente para sus propias necesidades y a no realizar directa o indirectamente una explotación comercial de los servicios a los que tiene acceso o de los resultados obtenidos gracias a la utilización de la Web Corporativa, salvo que haya obtenido consentimiento expreso de ATTICUS, S.L. El usuario se obliga a no utilizar las facilidades y capacidades de la Web Corporativa para realizar o sugerir actividades prohibidas por la ley o para intentar atraer a los usuarios hacia otros servicios competidores.

Las marcas, nombres comerciales o signos distintivos son titularidad de ATTICUS o terceros, y están protegidos por la legislación vigente en materia de propiedad industrial, sin que pueda entenderse que el acceso a la Web atribuya ningún derecho sobre las citadas marcas, nombres comerciales y/o signos distintivos.

5. Condiciones generales de uso.

5.1 General.

El usuario se obliga a hacer un uso correcto de la Web de conformidad con la Ley y el presente Aviso Legal. El usuario responderá frente a ATTICUS o frente a terceros, de cualesquiera daños o perjuicios que pudiera causarse como consecuencia del incumplimiento de dicha obligación.

ATTICUS se reserva el derecho de bloquear el acceso de los usuarios que hagan un uso de la Web contrario a la Ley o a las condiciones del presente Aviso Legal, pudiendo anular o bloquear, en su caso, el identificador y contraseña de los usuarios registrados.

Queda expresamente prohibido el uso de la Web con usos lesivos de bienes o intereses de ATTICUS o de terceros o que de cualquier otra forma sobrecarguen, dañen o inutilicen las redes, servidores y demás equipos informáticos (hardware) o productos y aplicaciones informáticas (software) de ATTICUS o de terceros.

5.2 Contenidos.

El usuario se compromete a utilizar los contenidos de conformidad con la Ley y el presente Aviso Legal, así como con las demás condiciones, reglamentos e instrucciones que en su caso pudieran ser de aplicación de conformidad con lo dispuesto en la cláusula 2. Con carácter meramente enunciativo, el usuario de acuerdo con la legislación vigente deberá abstenerse de:

- Reproducir, copiar, distribuir, poner a disposición, comunicar públicamente, transformar o modificar los Contenidos salvo en los casos autorizados en la ley o expresamente consentidos por ATTICUS o por quien ostente la titularidad de los derechos de explotación en su caso.
- Reproducir, copiar para uso privado los Contenidos que pueden ser considerados como Software o Base de Datos de conformidad con la legislación vigente en materia de propiedad intelectual, así como su comunicación pública o puesta a disposición de terceros cuando estos actos impliquen necesariamente la reproducción por parte del usuario o de un tercero.
- Extraer y/o reutilizar la totalidad o una parte sustancial de los Contenidos integrantes de la Web así como de las bases de datos que ATTICUS ponga a disposición de los usuarios.

5.3 Formularios de recogida de datos.

Sin perjuicio de lo dispuesto en la cláusula 7 del presente Aviso Legal, así como en las políticas de privacidad accesibles desde la Web y que pudieran resultar aplicables en cada momento, la utilización de ciertos servicios o solicitudes dirigidos a ATTICUS están condicionados a la previa cumplimentación del registro de usuario.

Toda la información que facilite el usuario a través de los formularios de la Web a los efectos anteriores o cualesquiera otros deberá ser veraz. A estos efectos, el usuario garantiza la autenticidad de todos aquellos datos que facilite garantiza la autenticidad de todos aquellos datos que comunique y mantendrá la información facilitada a ATTICUS perfectamente actualizada de forma que responda, en todo momento, a la situación real del usuario. En todo caso será el usuario el único responsable de las manifestaciones falsas o inexactas que realice y de los perjuicios que cause a ATTICUS o a terceros por la información que facilite.

5.4 Introducción de enlaces a la Web.

El usuario de internet que quiera introducir enlaces desde sus propias páginas web a la Web deberá cumplir con las condiciones que se detallan a continuación sin que el desconocimiento de las mismas evite las responsabilidades derivadas de la Ley:

- El enlace podrá vincular a cualquier página web- a excepción de aquellas que incorporen datos personales, bases de datos u otra información sometida a LOPD pero no podrá reproducirla de ninguna forma (online, links, copia de los textos, gráficos, etc.).
- Quedará en todo caso prohibido, de acuerdo con la legislación aplicable y vigente en cada momento, establecer frames o marcos de cualquier tipo que envuelvan a la Web

o permitan la visualización de los Contenidos a través de direcciones de internet distintas de las de la Web y, en cualquier caso, cuando se visualicen conjuntamente con contenidos ajenos a la Web de forma que: (I) produzca, o pueda producir, error, confusión o engaño en los usuarios sobre la verdadera procedencia del servicio o Contenidos; (II) suponga un acto de comparación o imitación desleal; (III) sirva para aprovechar la reputación de la marca y prestigio de ATTICUS; (IV) de cualquier otra forma resulte prohibido por la legislación vigente.

- No se realizarán desde la página que introduce el enlace ningún tipo de manifestación falsa, inexacta o incorrecta sobre ATTICUS, sus socios, empleados o clientes sobre la calidad de los servicios que presta.
- En ningún caso, se expresará en la página donde se ubique el enlace que ATTICUS ha prestado su consentimiento para la inserción del enlace o que de otra forma patrocina, colabora, verifica o supervisa los servicios del remitente.
- Está prohibida la utilización de cualquier marca denominativa, gráfica o mixta o cualquier otro signo distintivo de ATTICUS, y en concreto la denominación "CAVALL FORT", dentro de la página del remitente salvo en los casos permitidos por la ley o expresamente autorizados por ATTICUS y siempre que se permita, en estos casos, un enlace directo con la Web en la forma establecida en esta cláusula.
- La página que establezca deberá cumplir fielmente con la ley y no podrá en ningún caso disponer o enlazar con contenidos propios o de terceros que: (I) sean ilícitos, nocivos o contrarios a la moral y a las buenas costumbres (pornográficos, violentos, racistas, etc.); (II) induzcan o puedan inducir en el usuario la falsa concepción de que ATTICUS suscribe, respalda, se adhiere o que de cualquier manera apoya, las ideas, manifestaciones o expresiones, lícitas o ilícitas, del remitente; (III) resulten inapropiados o no pertinentes con la actividad de ATTICUS en atención al lugar, contenidos y temática de la página web del remitente.

6. Exclusión de responsabilidad.

6.1 De la información.

El acceso a la Web no implica la obligación por parte de ATTICUS de comprobar la veracidad, exactitud, adecuación, idoneidad, exhaustividad y actualidad de la información suministrada a través del mismo. Los contenidos de esta Web son de carácter general y no constituyen, en modo alguno, la prestación de un servicio de asesoramiento deportivo en la modalidad de la equitación, por lo que dicha información resulta insuficiente para la toma de decisiones personales por parte del usuario.

ATTICUS no se responsabiliza de las decisiones tomadas a partir de la información suministrada en la Web ni de los daños y perjuicios producidos en el usuario o terceros con motivo de actuaciones que tengan como único fundamento la información obtenida en la Web.

6.2 De la calidad del servicio.

El acceso a la Web no implica la obligación por parte de ATTICUS de controlar la ausencia de virus, gusanos o cualquier otro elemento informático dañino. Corresponde al usuario, en todo caso, la disponibilidad de herramientas adecuadas para la detección y desinfección de programas informáticos dañinos.

ATTICUS no se responsabiliza de los daños producidos en los equipos informáticos de los usuarios o de terceros durante la prestación del servicio de la Web.

6.3 De la disponibilidad del servicio.

El acceso a la Web requiere de servicios y suministros de terceros, incluidos el transporte a través de redes de telecomunicaciones cuya finalidad, calidad, continuidad y funcionamiento no corresponde a ATTICUS. Por consiguiente, los servicios proveídos a través de la Web pueden ser suspendidos, cancelados o resultar inaccesibles, con carácter previo o simultáneo a la prestación del servicio de la Web.

ATTICUS no se responsabiliza de los daños o perjuicios de cualquier tipo producidos en el usuario que traigan causa de fallos o desconexiones en las redes de telecomunicaciones que produzcan la suspensión, cancelación o interrupción del servicio de la Web durante la prestación del mismo o con carácter previo.

ATTICUS podrá realizar las modificaciones que estime convenientes en la Web, pudiendo incluir servicios y contenidos adicionales a los actuales o, en su caso, suprimirlos. ATTICUS podrá modificar la Web Corporativa cuando considere oportuno y podrá bloquear el acceso a todos o parte de los usuarios de la misma para proceder a realizar modificaciones o las reparaciones que considere necesarias en cualquier momento. En ningún caso, ATTICUS será responsable del inadecuado funcionamiento del sistema si ello obedece a una defectuosa configuración de los equipos del usuario o a su insuficiente capacidad para soportar los sistemas informáticos indispensables para poder hacer uso del servicio.

6.4 De los contenidos y servicios enlazados a través de la Web.

El servicio de acceso a la Web incluye dispositivos técnicos de enlace, directorios e incluso instrumentos de búsqueda que permiten al usuario acceder a otras páginas y portales de internet (en adelante, “Sitios Enlazados”). En estos casos, ATTICUS actúa como prestador de servicios de intermediación de conformidad con el artículo 17 de la Ley 34/2002, de 12 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI) y solo será responsable de los contenidos y servicios suministrados en los Sitios Enlazados en la medida en que tenga conocimiento efectivo de la ilicitud y no haya desactivado el enlace con la diligencia debida. En el supuesto de que el usuario considere que existe un Sitio Enlazado con contenidos ilícitos o inadecuados podrá comunicárselo a ATTICUS de acuerdo con el procedimiento y los efectos establecidos en la cláusula 8, sin que en ningún caso esta comunicación conlleve la obligación de retirar el correspondiente enlace. En ningún caso, la existencia de Sitios Enlazados debe de presuponer la existencia de acuerdos con los responsables o titulares de los mismos, ni la recomendación, promoción o identificación de ATTICUS con las manifestaciones, contenidos o servicios proveídas.

ATTICUS no conoce los contenidos y servicios de los Sitios Enlazados y por tanto no se hace responsable por los daños producidos por la ilicitud, calidad, desactualización, indisponibilidad, error o inutilidad de los contenidos y/o servicios de los Sitios Enlazados ni de cualquier otro daño que no sea directamente imputable a ATTICUS.

7. Protección de datos personales.

Los datos recabados a través de formularios de recogida de datos de la Web será incorporados a un fichero automatizado de datos de carácter personal del que es responsable ATTICUS.

De acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "la LOPD"), el abonado y/o usuario (en adelante, "el cliente") presta su consentimiento para que sus datos personales se incorporen a los ficheros, automatizados o no, propiedad de ATTICUS, que tienen como finalidad la gestión de los clientes, premiar su finalidad y mantenerlos informados (envíos de la información sobre nuevas actividades y celebración de campeonatos hípicos por ejemplo) por cualquier medio (electrónico o no) de todas las ofertas de productos y/o servicios, y/o promociones incluyendo el análisis y la formación de perfiles y, en general, la realización de acciones comerciales, de promoción y/o marketing relacionadas con las actividades propias del objeto social de ATTICUS, así como con el deporte ocio, salud, bienestar, proveedores de transporte, seguros, servicios inmobiliarios, publicidad y la prestación de servicios de valor añadido.

El cliente tiene derecho a acceder al fichero que contiene sus datos de carácter personal, de cuyo tratamiento es responsable ATTICUS, a fin de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, mediante correo postal ordinario dirigido a ATTICUS, S.L., Avda. da Del Percebe, s/n (Edificio Inditex)- Polígono de Sabón, 08080, Barcelona, Asunto: LOPD, aportando fotocopia del DNI, solicitud que se realiza, indicación del domicilio a efectos de notificaciones, fecha y firma. Para su mayor comodidad, podrá igualmente obtener información para el ejercicio de estos derechos telefónicamente, a través del número que se indica en el apartado 1 de este Aviso Legal.

Asimismo, ATTICUS cancelará, borrará y/o bloqueará los datos cuando resulten inexactos, incompletos o hayan dejado de ser necesarios o pertinentes para su finalidad, de conformidad con lo previsto en la legislación en materia de protección de datos de carácter personal. A estos efectos, le rogamos que nos comunique inmediatamente cualquier modificación de sus Datos a fin de que la información contenida en nuestros ficheros esté en todo momento actualizada y no contenga errores.

En los formularios de recogida de datos, los campos obligatorios vendrán señalados, específicamente, por lo que en caso de que el usuario no facilite los datos correspondientes, ATTICUS podrá a su sola discreción denegar el correspondiente servicio.

ATTICUS adopta los niveles de seguridad requeridos por el Reglamento de Medidas de Seguridad aprobado por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de

Protección de Datos de Carácter Personal. No obstante lo anterior, la seguridad técnica en un medio como un medio como Internet no es inexpugnable y pueden existir filtraciones por actuaciones dolosas de terceros.

ATTICUS podrá utilizar cookies durante la prestación del servicio de la Web. Las cookies son procedimientos automáticos de recogida de información relativa a las preferencias determinadas por un usuario durante su visita a una determinada página web. Esta información se registra en pequeños archivos que son guardados en los equipos informáticos del usuario correspondiente de forma imperceptible. Cada vez que el usuario vuelve a acceder al sitio web en cuestión estos archivos se activan automáticamente de manera que se configura el sitio web con las preferencias señaladas en anteriores visitas. En definitiva, las cookies son ficheros físicos de información personal alojados en el propio terminal del usuario y asociados inequívocamente a este terminal.

Las cookies no pueden leer los archivos cookies creados por otros proveedores.

El usuario tiene la posibilidad de configurar su programa navegador de manera que se impida la creación de los archivos cookie o se advierta del momento en que eso ocurre la Web es accesible sin que estén activadas las opciones referentes a los archivos cookie, si bien pueden impedir el correcto funcionamiento de mecanismos de seguridad para servicios excluidos o determinados servicios que requieren de mayor seguridad. Por norma general, la finalidad de los archivos cookie de la Web es la de facilitar la navegación del usuario.

8. Comunicación de carácter ilícito e inadecuado.

En el caso de que el usuario o cualquier otro usuario de internet tuvieran conocimiento de que los Sitios Enlazados remiten a páginas cuyos contenidos o servicios son ilícitos, nocivos, denigrantes, violentos o contrarios a la moral podrá ponerse en contacto con ATTICUS indicando los siguientes extremos:

- Datos personales del comunicante: nombre, dirección, número de teléfono y dirección de correo electrónico;
- Descripción de los hechos que revelan el carácter ilícito o inadecuado del Sitio Enlazado;
- En el supuesto de violación de derechos, tales como propiedad intelectual e industrial, los datos personales del titular del derecho infringido cuando sea persona distinta del comunicante;
- Asimismo, deberá aportar el título que acredite la legitimación del titular de los derechos y, en su caso, el de representación para actuar por cuenta del titular cuando sea persona distinta del comunicante;
- Declaración expresa de que la información contenida en la reclamación es exacta.

La recepción por parte de ATTICUS de la comunicación prevista en esta cláusula no supondrá, según lo dispuesto en la LSSI, el conocimiento efectivo de las actividades y/o contenidos por el comunicante.

9. Legislación.

El presente Aviso Legal se rige en todos y cada uno de sus extremos por la ley española.

ANEXO XVI POLÍTICA DE PRIVACIDAD PÁGINA WEB	DOC. DE SEGURIDAD VERSIÓN 2.0

DATOS PERSONALES REGISTRADOS: ATTICUS, S.L. (Avd. da Del Percebe, s/n, 08080, Barcelona) y CIF número B-00000003, como responsable del fichero, en cumplimiento de lo establecido en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, comunica a los usuarios de la Página Web: www.cavallfort.com, en adelante "la Página Web", que los datos facilitados mediante los correspondientes formularios y los e-mails recibidos solicitando información y que tienen consideración de datos de carácter personal, se incluirán en un fichero automatizado o no de carácter confidencial.

Asimismo, se informa y los usuarios de la Página Web consientes su utilización mediante sistemas automáticos de decisión, segmentación y valoración respecto de las solicitudes que se realicen con la finalidad de gestión sus usuarios, la obtención de estadísticas diversas, la realización de prospecciones de mercado y el envío por parte de la Página Web, de publicidad e información en relación con los servicios prestados, y que estén relacionados con el uso de la plataforma, atendiendo a las preferencias que cada usuario haya configurado en la Página Web incluso después de finalizada la relación. Dicho fichero se encuentra inscrito en la Agencia Española de Protección de Datos conforme a la legislación vigente y normativa de desarrollo.

Asimismo, y de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante, "la LOPD"), el abonado o usuario (en adelante, "el cliente") presta su consentimiento para que sus datos personales se incorporen a los ficheros, automatizados o no, propiedad de ATTICUS, S.L., que tienen como finalidad la gestión de clientes, mantenerlos informados , por cualquier medio (electrónico o no), de todas las ofertas y servicios y/o promociones, incluyendo el análisis y formación de perfiles, y en general, la realización de acciones comerciales de promoción y/o marketing relacionadas con las actividades propias del objeto social de ATTICUS, S.L. así como servicios inmobiliarios, proveedores de transporte, seguros, servicios inmobiliarios, publicidad y la prestación de servicios de valor añadido.

Pulsando el botón "enviar" del correspondiente formulario y a los efectos de los dispuesto en el artículo 21 de la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, el cliente autoriza expresamente a ATTICUS, S.L. a remitirle comunicaciones comerciales, promociones publicitarias, por correo electrónico o por cualquier otro medio de comunicación electrónica o no electrónica equivalente. Asimismo, pulsando el botón "enviar" o equivalente a este del correspondiente formulario el cliente prestará también su consentimiento expreso para que sus datos personales puedan ser comunicados, con idénticos fines, a las sociedades que en cada momento integren el grupo al que pertenece ATTICUS, S.L. y a terceros que, del mismo u otros sectores, contraten o presten tales servicios a ATTICUS, S.L. y/o proporcionen al cliente los productos y/o servicios ofrecidos por ATTICUS, S.L.. A los efectos previstos en la LOPD, el cliente se da por notificado de dichas cesiones. No obstante, le usuario podrá oponerse al envío de tales comunicaciones señalando la casilla que

a estos efectos aparece indicada en cada uno de los formularios o de acuerdo con lo establecido en las comunicaciones.

El cliente tiene derecho a acceder al fichero que contenga sus datos personales, de cuyo tratamiento ATTICUS, S.L., a fin de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, mediante correo postal ordinario dirigido a ATTICUS, S.L., Avenida da Del Percebe, s/n, 08080, Barcelona, Asunto: LOPD, aportando fotocopia del DNI, solicitud que se realiza, indicación del domicilio a efectos de notificaciones, fecha y firma. Para su mayor comodidad, podrá igualmente obtener información acerca del ejercicio de estos derechos telefónicamente, a través del apartado de contacto de la propia Web. Por último y si usted utiliza habitualmente el canal telefónico, o un medio de comunicación por vía electrónica en su relación con ATTICUS, S.L., podrá ejercitar igualmente dichos derechos a través de estos canales debiendo utilizar para ellos los medios de identificación habitualmente requeridos.

Asimismo, ATTICUS, S.L. cancelará, borrará y/o bloqueará los datos cuando resulten inexactos, incompletos o hayan dejado de ser necesarios o pertinentes para su finalidad, de conformidad con lo previsto en la legislación en materia de protección de datos. A estos efectos, le rogamos que nos comunique inmediatamente cualquier modificación de sus Datos a fin de que la información contenida en nuestros ficheros esté en todo momento actualizada y no contenga errores.

En los formularios de regida de datos (tanto físicos como electrónicos por medio de la Web), los campos obligatorios vendrán señalados específicamente, por lo que en caso de que el Usuario no facilite los datos correspondientes, ATTICUS, S.L. podrá a su sola discreción denegar el correspondiente servicio.

ANEXO XVII POLÍTICA DE COOKIES PÁGINA WEB	DOC. DE SEGURIDAD VERSIÓN 2.0

En nuestro sitio Web www.cavallfort.com utilizamos cookies para facilitar la relación de los visitantes con nuestro contenido y para recabar información acerca del uso del sitio web.

En cumplimiento de la **Directiva 2009/136/CE**, desarrollada en nuestro ordenamiento por el apartado segundo del artículo 22 de la Ley de Servicios de Sociedad de la Información, siguiendo las directrices de la Agencia Española de Protección de Datos procedemos a informarle detalladamente del uso que se realiza en nuestra web

¿QUÉ SON LAS COOKIES?

Se **denominan cookies** a unos pequeños archivos que se graban en el navegador utilizado por cada visitante de nuestra web para que el servidor pueda recordar la visita de ese usuario con posterioridad cuando vuelva a acceder a nuestros contenidos. Esta información no revela su identidad, ni dato personal alguno, ni accede al contenido almacenado en su pc, pero sí que permite a nuestro sistema identificarle a usted como un usuario determinado que ya visitó la web con anterioridad, visualizó determinadas páginas, etc. y además permite guardar sus preferencias personales e información técnica como por ejemplo las visitas realizadas o páginas concretas que visite.

Si usted no desea que se guarden cookies en su navegador o prefiere recibir una información cada vez que una cookie solicite instalarse, puede configurar sus opciones de navegación para que se haga de esa forma. La mayor parte de los navegadores permiten la gestión de las cookies de 3 formas diferentes:

- Las cookies son siempre rechazadas;
- El navegador pregunta si el usuario desea instalar cada cookie;
- Las cookies son siempre aceptadas;

Su navegador también puede incluir la posibilidad de seleccionar con detalle las cookies que desea que se instalen en su ordenador. En concreto, el usuario puede normalmente aceptar alguna de las siguientes opciones:

- rechazar las cookies de determinados dominios;
- rechazar las cookies de terceros;
- aceptar cookies como no persistentes (se eliminan cuando el navegador se cierra);
- permitir al servidor crear cookies para un dominio diferente.

TIPOS DE COOKIES Y SU FINALIDAD

COKIES TÉCNICAS: Son aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan, como por ejemplo, controlar el tráfico y la comunicación de datos o identificar la sesión.

COOKIES DE PERSONALIZACIÓN: Son aquellas que permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el terminal de usuario, como por ejemplo serían el idioma, el tipo de navegador a través del cual accede el servicio, la configuración regional desde donde accede al servicio, etc.

COOKIES DE ANALISIS: Son aquellas que permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de cookies se utiliza en la mediación de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.

¿QUE TIPO DE COOKIES UTILIZA LA PAGINA WEB CSICASASNOVAS. COM?

COOKIE-AGREED: Indica si el usuario ha aceptado el uso de cookies de esta web, según la normativa europea. Sirve para saber si se ha de mostrar o no el aviso acerca de las cookies.

HAS_JS: Permite al servidor saber si puede contar con javascript activado en el ordenador, para mejorar el interfaz del usuario.

SESS: Identificador de sesión aleatorio, utilizado para el acceso de usuarios autenticados en la página.

CASASNOVAS_RESPONSIVE: Almacena el estado de menús desplegables y pestañas activas dentro de la web, para restablecerlas de nuevo al cambiar de página. Mejoran la experiencia del usuario en la web.

_GA_GAT (cookies de google analytics): Registran información anónima de los visitantes de la página, con el objeto de generar estadísticas de acceso. Estas cookies solo se generan si esta aceptado su uso.

En el caso de las cookies de **Google Analytics**, esta empresa almacena las cookies en servidores ubicados en Estados Unidos y se compromete a no compartirla con terceros, excepto en los casos en los que sea necesario para el funcionamiento del sistema o cuando la ley obligue a tal efecto. Según Google no guarda su dirección IP. Google Inc. es una compañía adherida al Acuerdo de Puerto Seguro que garantiza que todos los datos transferidos serán tratados con un nivel de protección acorde a la normativa europea.

CONSENTIMIENTO

Al navegar y continuar en el sitio web estará consintiendo el uso de las cookies antes enunciadas y en las condiciones contenidas en la presente Política de Cookies.

ANEXO XXI CLÁUSULA A INCLUIR EN EL FORMULARIO: EQUITACIÓN TERAPÉUTICA ADAPTADA	DOC. DE SEGURIDAD VERSIÓN 2.0

De acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "la LOPD"), el alumno y/o sus padres o tutores aceptan expresamente el tratamiento de sus datos personales y datos médicos relativos a salud que él mismo pueda facilitar, con la finalidad de la adecuada prestación de los servicios que solicite en cada momento.

Asimismo, y de acuerdo con lo establecido en la citada LOPD, el alumno y/o sus padres o tutores prestan su consentimiento para que sus datos personales se incorporen a los ficheros, automatizados o no, propiedad de ATTICUS, S.L. que tienen como finalidad la preparación y prestación de clases de equitación terapéutica.

El alumno queda informado que, en caso de incumplimiento de las obligaciones contractuales asumidas con ATTICUS, S.L., y de conformidad con lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, los datos relativos al impago podrán ser inmediatamente comunicados a ficheros de información sobre solvencia patrimonial y de crédito.

El alumno tiene derecho a acceder al fichero que contenga sus datos personales, de cuyo tratamiento es responsable ATTICUS, S.L., a fin de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, mediante correo postal ordinario dirigido al Servicio de Atención al Público de ATTICUS, S.L. , Asunto: LOPD, aportando fotocopia del D.N.I., solicitud que se realiza, indicación del domicilio a efectos de notificaciones, fecha y firma y, en su caso, documentos acreditativos de la petición.

ANEXO XXII CLAUSULADO DE FORMULARIOS FÍSICOS ATTICUS, S.L.	DOC. DE SEGURIDAD VERSIÓN 2.0

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal le informamos que todos los datos que se incorporen a la presente solicitud, serán incorporados a un fichero cuyo responsable es ATTICUS, S.L. (en adelante, ATTICUS), con domicilio en Avenida da Del Percebe, s/n, CP. 08080, Barcelona (Barcelona), con la finalidad de proceder a su inscripción a la actividad solicitada, así como para mantener y ejecutar la relación derivada de la misma. Asimismo, queda informado y consiente que sus datos personales recogidos en el apartado "Domiciliación Bancaria" sean comunicados a la Entidad Bancaria correspondiente con la única finalidad de proceder al cobro de los servicios prestados.

Igualmente, le informamos que puede ejercer sus derechos de acceso, rectificación, cancelación y oposición mediante comunicación escrita dirigida a ATTICUS, a la dirección indicada anteriormente, adjuntando copia del DNI y como asunto: LOPD.

Fdo: Padres o tutores. Fdo: El alumno

ANEXO XXIII FORMULARIO PARA EL EJERCICIO DE LOS DERECHOS ARCO	DOC. DE SEGURIDAD VERSIÓN 2.0

DATOS DEL RESPONSABLE DEL TRATAMIENTO

ATTICUS, S.L. C.I.F.: B-00000003.

Domicilio: Avda. Del Percebe, s/n.

Localidad: Barcelona. Provincia: Barcelona C.P.: 08080

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

☐ Hombre ☐ Mujer

Nombre y apellidos: _____ D.N.I.: _____

Domicilio: _____

Localidad: _____ Provincia: _____ C.P.: _____

Telf. de contacto: _____

Que, mediante la presente solicito ejercitar el siguiente derecho de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal:

☐ Derecho de **acceso**, para ser informado de los datos de carácter personal sometidos a tratamiento por parte de ATTICUS, S.L.

☐ Derecho de **rectificación**, de los datos de carácter personal que señalo a continuación:

_____
_____
_____
_____

☐ Derecho de **cancelación**, de los datos de carácter personal que señalo a continuación:

_____
_____

_____
_____

☐ Derecho de **oposición**, de manera que no se lleve a cabo tratamiento alguno de mis datos de carácter personal por los siguientes motivos y en relación con:

_____
_____
_____
_____

En relación con la solicitud expuesta, adjunto los siguientes documentos:
_____
_____

SOLICITO, que sea atendido mi ejercicio del derecho mencionado en los términos anteriormente expuestos.

Fecha: ___ de _____ de _____

Fdo.: _____

ANEXO XIV CLÁUSULA A INCLUIR EN LOS FORMULARIOS: ESCUELA DE EQUITACIÓN, RENOVACIÓN DE PLAZAS, CAMPAMENTO VERANO Y GIMNASIO	DOC. DE SEGURIDAD VERSIÓN 2.0

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal le informamos que sus datos serán incorporados a un fichero del que es responsable ATTICUS, S.L. (en adelante, ATTICUS), con domicilio en Avenida de la Del Percebe s/n, CP. 08080, Barcelona (Barcelona), con la finalidad de proceder a su inscripción en la actividad solicitada, así como para mantener y ejecutar la relación derivada de la misma. Asimismo, queda informado y consiente que sus datos personales recogidos en el apartado "Domiciliación Bancaria" sean comunicados a la Entidad Bancaria correspondiente con la única finalidad de proceder al cobro de los servicios prestados.

Igualmente, le informamos que puede ejercer sus derechos de acceso, rectificación, cancelación y oposición, mediante comunicación escrita dirigida a ATTICUS, a la dirección indicada anteriormente y adjuntando copia de su DNI.

Fdo.: Padres o tutores Fdo.: El alumno.

Nota para la Firma del formulario:

Además de los padres o tutores, si el menor que va a desarrollar la actividad tiene 14 años o más, nuestra recomendación es que también él lo firme.

ANEXO XXV CLÁUSULA A INCLUIR EN LA HOJA REGISTRO DE LOS JINETES	DOC. DE SEGURIDAD VERSIÓN 2.0

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal le informamos que sus datos serán incorporados a un fichero del que es responsable ATTICUS, S.L. (en adelante, ATTICUS), con domicilio en Avenida de la Del Percebe s/n, CP. 08080, Barcelona (Barcelona), con la finalidad de realizar la gestión e inscripción de los jinetes en el concurso, así como para la liquidación económica derivada de dichos concursos. Asimismo, queda informado y consiente que sus datos personales recogidos en el presente formulario sean comunicados, en cumplimiento de la normativa vigente, a la/s Federación/es Hípica/s que corresponda/n, así como que, si resulta ganador del concurso o es fotografiado a lo largo del desarrollo del mismo, las fotografías puedan ser publicadas en la página web de CAVALL FORT (www.cavallfort.com).

Finalmente, le informamos que puede ejercer sus derechos de acceso, rectificación, cancelación y oposición, mediante comunicación escrita dirigida a ATTICUS, a la dirección indicada anteriormente y adjuntando copia de su DNI.

Annex VI. Exemple de document realitzat amb l'eina 'Facilita

DOCUMENTACION A REVISAR

Este documento contiene las cláusulas informativas que debe incluir en los formularios de solicitud de información, el documento a anexar en cada uno de los contratos de prestación de servicios, el registro de actividades de tratamiento y un anexo con recomendaciones sobre medidas de seguridad y tratamientos de datos personales (imágenes) captados por cámaras de videovigilancia, las cuales debe implantar en su organización.

La presentación de la documentación está asociada a cada uno de los tratamientos que ha seleccionado al cumplimentar el programa.

TRATAMIENTO DE DATOS DE CLIENTES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de sus clientes, tanto si se realiza en soporte papel como si los recoge a través de un formulario web:

Responsable: Identidad: JPV Inversiones S.L. - CIF: B-00000001 Dir. postal: Avenida del Percebe, s/n, 08080, Barcelona) Teléfono: 931232323 Correo elect: direcciontic@grupjpv.com

"En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado, realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en JPV Inversiones S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Asimismo solicito su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente."

SI ☐

NO ☐

AVISO: Debe tener en cuenta que si su cliente marca la opción NO, en ningún caso podrá enviarle publicidad

TRATAMIENTO DE DATOS DE CANDIDATOS

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de los candidatos a un puesto de trabajo, tanto si se realiza en soporte papel como si los recoge a través de un formulario web:

Responsable: Identidad: JPV Inversiones S.L. - CIF: B-00000001 Dir. postal: Avenida del Percebe, s/n, 08080, Barcelona) Teléfono: 931232323 Correo elect: direccionTIC@grupjpv.com

"En nombre de la empresa tratamos la información que nos facilita con el fin de mantenerle informado de las distintas vacantes a un puesto de trabajo que se produzcan en nuestra organización. Los datos proporcionados se conservarán hasta la adjudicación de un puesto de trabajo o hasta que usted ejerza su derecho de cancelación por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios. Los datos no se cederán a terceros."

Si los candidatos aportan su CV en papel normal, sin formulario, se les pedirá que firmen un formulario fechado en que figure al información antes citada.

TRATAMIENTO DE DATOS DE PROVEEDORES

Clausula informativa:

El texto que se muestra a continuación deberá incluirlo en todos aquellos formularios que utilice para recabar datos personales de los proveedores como por ejemplo en facturas:

Responsable: Identidad: JPV Inversiones S.L. - CIF: B-00000001 Dir. postal: Avenida del Percebe, s/n, 08080, Barcelona) Teléfono: 931232323 Correo elect: direccionTIC@grupjpv.com

"En nombre de la empresa tratamos la información que nos facilita con el fin de realizar pedido y facturar los servicios. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en JPV Inversiones S.L. estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios."

Si los proveedores aportan sus datos mediante otro sistema, se les pedirá que firmen un formulario fechado en que figure al información antes citada.

EMPRESAS DE SERVICIOS

Contratos:

AVISO: En su contrato con la empresa que le presta el servicio deberá incluir las siguientes cláusulas contractuales:

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a Calpurnia Consulting S.L., como encargado del tratamiento, para tratar por cuenta de JPV Inversiones S.L., en calidad

de responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio que en adelante se especifican**.**

El tratamiento consistirá en Mantenimiento Informático.

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la entidad JPV Inversiones S.L. como responsable del tratamiento, pone a disposición de la entidad Calpurnia Consulting S.L. la información disponible en los equipos informáticos que dan soporte a los tratamientos de datos realizados por el responsable.

3. Duración

El presente acuerdo tiene una duración de , renovable.

Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable los datos personales, y suprimir cualquier copia que mantenga en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4. Obligaciones del encargado del tratamiento

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

- ✓ Utilizar los datos personales a los que tenga acceso sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- ✓ Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.

  Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos, el encargado informará inmediatamente al responsable.
- ✓ No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.
- ✓ Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice el contrato.
- ✓ Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.
- ✓ Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
- ✓ Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- ✓ Notificación de violaciones de la seguridad de los datos

  El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida y a través de la dirección de correo electrónico que le indique el responsable, las violaciones de la seguridad de los datos personales a su cargo de

las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

Se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Datos de la persona de contacto para obtener más información.

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

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

- ✓ Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- ✓ Auxiliar al responsable de tratamiento a implantar las medidas de seguridad necesarias para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

- ✓ Destino de los datos

El responsable del tratamiento no conservará datos de carácter personal relativos a los tratamientos del encargado salvo que sea estrictamente necesario para la prestación del servicio, y solo durante el tiempo estrictamente necesario para su prestación.

5. Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a) Facilitar al encargado el acceso a los equipos a fin de prestar el servicio contratado.

b) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

c) Supervisar el tratamiento.

AVISO: No olvide firmar la última hoja de cada uno de los contratos que se han obtenido.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Tratamiento: **Clientes**

Finalidad del tratamiento

Gestión de la relación con los clientes

Descripción de las categorías de clientes y de las categorías de datos personales:

Clientes:

Personas con las que se mantiene una relación comercial como clientes

Categorías de datos personales:

Facturar

De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Administración tributaria

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades

Tratamiento: **Empleados**

Finalidad del tratamiento

Gestión de la relación laboral con los empleados

Descripción de las categorías de empleados y de las categorías de datos personales:

Empleados:

Personas que trabajan para el responsable del tratamiento

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación comercial. Gestionar la nómina, formación

De identificación: nombre, apellidos, número de Seguridad Social, dirección postal, teléfonos, e-mail

Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y porcentaje de minusvalía

Datos académicos

Datos profesionales

Datos bancarios, para la domiciliación del pago de las nóminas

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

No se contempla

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Los previstos por la legislación fiscal y laboral respecto a la prescripción de responsabilidades

Tratamiento: **Candidatos**

Finalidad del tratamiento

Gestión de la relación con los candidatos a un empleo en la empresa

Descripción de las categorías de candidatos y de las categorías de datos personales:

Candidatos:

Personas que desean trabajar para el responsable del tratamiento

Categorías de datos personales:

Los necesarios para gestionar los curriculum de posibles futuros empleados

De identificación: nombre, apellidos, dirección postal, teléfonos, e-mail

Características personales: estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad y otros excluyendo datos de raza, salud o afiliación sindical

Datos académicos

Datos profesionales

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

No se contempla

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Un año desde la presentación de la candidatura

Tratamiento: **Proveedores**

Finalidad del tratamiento

Gestión de la relación con los proveedores

Descripción de las categorías de proveedores y de las categorías de datos personales:

Proveedores:

Personas con las que se mantiene una relación comercial como proveedores de productos y/o servicios

Categorías de datos personales:

Los necesarios para el mantenimiento de la relación laboral

De identificación: nombre, NIF, dirección postal, teléfonos, e-mail

Datos bancarios: para la domiciliación de pagos

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades

Tratamiento: **VideoVigilancia**

Finalidad del tratamiento

Seguridad de las personas y bienes

Descripción de las categorías de interesados y de las categorías de datos personales:

Interesados:

Personas que accedan o intenten acceder a las instalaciones

Categorías de datos personales:

Imágenes

Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:

Administración tributaria

Cuerpos y fuerzas de seguridad del estado

Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos:

Un mes desde su grabación

ANEXO MEDIDAS DE SEGURIDAD

INFORMACIÓN DE INTERÉS GENERAL

Este documento ha sido diseñado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales que incluyan datos personales relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas mínimas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO
    - Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
    - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
    - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

- No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- DERECHOS DE LOS TITULARES DE LOS DATOS

  Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

  - Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

    Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

    Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

    Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

    Para el **derecho de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

  El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL
  - Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos

personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

- CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)
    - **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
    - **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.
    - **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
    - **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.
    - **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.
    - **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.
      No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guías de videovigilancia de la Agencia Española de Protección de Datos que se encuentran a su disposición en la sección de publicaciones de la web www.agpd.es.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- **MALWARE**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

- **CORTAFUEGOS O FIREWALL**: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- **CIFRADO DE DATOS**: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD**: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.

En la Oficina de Seguridad del Internauta (https://www.osi.es) el Instituto Nacional de Ciberseguridad pone a su disposición información y herramientas informáticas gratuitas que pueden ser útiles para garantizar la seguridad de los datos personales en ordenadores y dispositivos electrónicos.

Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales puede consultar la web www.incibe.es donde, entre otros documentos, podrá consultar el decálogo de ciberseguridad o el decálogo de buenas prácticas de seguridad en un departamento de informática donde encontrará los aspectos técnicos generales a tener en cuenta para la seguridad de la información de su empresa.