DESPACHO XXXX

Titular responsable Letrado D.

Colegiado número xxxxx del Ilustre Colegio de Abogados de Xxxxxxxxxxxxxxx.

**DOCUMENTO DE SEGURIDAD DE NIVEL ALTO DE LOS FICHEROS NO AUTOMATIZADOS QUE CONTIENEN DATOS DE CARÁCTER PERSONAL**

**(Este documento es una propuesta ejemplificativa. En ningún caso debe obviarse la posible presencia de errores en su confección, no sirviendo sin su previa revisión y actualización como modelo a los fines establecidos en la vigente LOPD).**

**INFORMACIÓN GENERAL Y NORMAS DE USO**.

El presente documento, de acuerdo con lo establecido en el apartado 1, del artículo 88 y en el apartado 1.h del artículo 105, 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 (LOPD) , es de obligado cumplimiento para todo el personal del DESPACHO XXXX que tenga acceso a los datos de carácter personal, y a los sistemas de información , referidos a los ficheros definidos en este documento.

El documento será de aplicación únicamente a ficheros NO AUTOMATIZADOS y, consecuentemente, recogerá las medidas contempladas para este tipo de ficheros en el Capítulo IV, del Título VIII, del referido Reglamento de la LOPD.

El documento deberá mantenerse en todo momento actualizado y, de acuerdo con lo contemplado en el artículo 88.7 del Reglamento de la LOPD, será revisado cuando se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados.

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

Todo ello de acuerdo, en general, con lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, citado y, en particular, con lo especificado en los apartados 7 y 8 del artículo 88 de dicha norma.

No obstante, conviene recordar que las medidas de seguridad contempladas en el Reglamento tienen la condición de mínimos exigibles y, consecuentemente, las medidas de seguridad a adoptar serán, además de las contempladas en este documento, las que se consideren necesarias para garantizar la seguridad de lo datos de carácter personal y que eviten su alteración, pérdida, tratamiento o acceso no autorizado.

ÍNDICE

1.- Introducción………………………………………………………………………………………………………...Página .

2.- Ámbito de aplicación…………………………………………………………………………………………Página .

2.1 Encargado del tratamiento...........................................................................................................Página .

2.2 Prestaciones de servicios sin acceso a datos personales...............................................Página .

2.3 Recursos protegidos…………………………………………………………………………………………...Página .

2.4 Delegación de autorizaciones…………………………………………………………………………....Página .

3.- Medidas, normas, procedimientos de actuación, reglas y estándares……………Página .

3.1 Auditoría de Seguridad……………………………………………………………………………………...Página .

3.2 Criterios de archivo……………………..…………………………………………………………………...Página .

3.3 Identificación y autenticación…………………………………………………………………………...Página .

3.4 Dispositivos de almacenamiento………………………….…………………………………………...Página .

3.5 Custodia de los soportes……………………………………….…………………………………………...Página .

3.6 Régimen de trabajo fuera de los locales……………………………….………………………...Página .

4.- Funciones y obligaciones del personal………………………….………………………………...Página .

4.1 Responsable de Seguridad…………………………….………………………………………………...Página .

5.- Control de acceso ……………………………………………………………………………………………...Página .

5.1 Control de acceso físico …………………………………………………………………………………...Página .

5.2 Registro de accesos……………………..……………………………………………………………………...Página .

6.- Gestión de soportes y documentos………………….………………………………………………...Página .

6.1 Sistema de Registro de Entrada/Salida de soportes………………….………………...Página .

6.2 Baja del soporte del inventario………………………………………………………………………...Página .

6.3 Salida de soportes por operaciones de mantenimiento………………………………...Página .

6.4 Distribución de soportes…………………………………………………………………………………...Página .

7.- Estructura de los ficheros y descripción de los sistemas de información……..Página .

8.- Procedimiento de notificación, gestión y respuesta ante las incidencias…….Página .

8.1 Registro de incidencias……………………………………………………………………………………...Página .

**ANEXOS**

ANEXO I: Notificaciones a la Agencia Española de Protección de Datos de haber procedido a la inscripción de cada uno de los ficheros.

ANEXO II: Ficheros y su descripción.

ANEXO III: Contenido de cada fichero.

ANEXO IV: Inventario de soportes físicos en los que se almacenan datos de carácter personal.

ANEXO V: Funciones y documentación de las funciones del personal del DESPACHO XXXX.

ANEXO VI: Delegación de autorizaciones y autorizaciones necesarias para el tratamiento de datos personales.

Anexo VII: Registro de entrada de soportes.

Anexo VIII: Registro de salida de soportes.

ANEXO IX: Circulares comunicadas a toda persona que tiene acceso a datos de carácter personal en el DESPACHO XXXX.

ANEXO X: Encargados del tratamiento.

ANEXO XI: Controles periódicos.

**1.- INTRODUCCIÓN**

El presente documento, que girará bajo el nombre de “Documento de Seguridad de Nivel Alto de los ficheros no automatizados que contienen datos de carácter personal“, se crea por el responsable de los ficheros (DESPACHO XXXX ), de acuerdo con la obligación establecida en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), y en consonancia con los estándares establecidos en el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Los ficheros a los que es de aplicación, todos ellos inscritos en el Registro General de Protección de Datos (RGPD) de la Agencia Española de Protección de Datos, y que forman parte del sistema de información sobre el que se centra el presente Documento de Seguridad, son los siguientes:

**NOMBRE DEL FICHERO Nº DE INSCRIPCIÓN EN EL RGPD**

**Clientes \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Proveedores \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Personal \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

(se adjunta, como ANEXO I, las notificaciones de la Agencia Española de Protección de Datos con la indicación de haber procedido a la inscripción de cada uno de los ficheros).

Se ha considerado, de acuerdo con lo establecido en el apartado 3, del artículo 81, del Reglamento de la LOPD, que estos ficheros deben ser tipificados como de los que les es exigible el NIVEL ALTO, al tratarse de ficheros que contienen datos de carácter personal que se encuentran en las medidas de seguridad reforzadas a las que hace referencial citado Reglamento.

De acuerdo con ello, el presente documento responde a las exigencias establecidas para las "Medidas de Seguridad de Nivel Alto aplicables a los ficheros no automatizados", en el Título VIII y, en particular, en su Capítulo IV, del Real Decreto 1720/2007.

**2.- ÁMBITO DE APLICACIÓN**

El ámbito de aplicación del presente documento abarca a todo el personal del DESPACHO XXXX con acceso a los datos de carácter personal que se encuentran en los ficheros referidos, y se centra sobre todos los recursos protegidos , cada uno de ellos en particular, y, en general, sobre los sistemas de información que contienen los datos y a partir de los que se accede a los mismos.

De esta forma, mediante circular informativa y de obligado cumplimiento, que se adjunta en el ANEXO IX, el abogado titular del despacho y, por tanto, responsable de los ficheros, ha puesto en conocimiento de todas las personas que acceden a los mismos sus obligaciones y responsabilidad respecto al almacenamiento, consulta y tratamiento de datos de carácter personal en los ficheros, así como sobre las medidas de seguridad a aplicar.

**2.1 Encargado del tratamiento**

Cuando un tercero acceda a los datos de carácter personal referidos, a los soportes que los contengan o a los recursos del sistema de información que los traten para prestar un servicio al DESPACHO XXXX, y dicho acceso se realice en los locales del DESPACHO XXXX, dicho tercero habrá suscrito un contrato con la entidad en cumplimiento de lo especificado en el artículo 12 de la LOPD y será considerado como encargado del tratamiento, comprometiéndose su personal al cumplimiento de las medidas de seguridad previstas en este documento.

Si el servicio que se contrata fuera prestado por el encargado del tratamiento en sus propios locales y, consecuentemente, exista un traslado de los datos de carácter personal referidos, de los soportes que los contengan o de alguno de los recursos del sistema de información que los traten, fuera de los locales del DESPACHO XXXX, el encargado del tratamiento deberá elaborar un documento de seguridad que reúna todas los requisitos exigidos en el artículo 88 y en el Capítulo IV, del Título VIII, del Reglamento de la LOPD o, si ya hubiera elaborado su propio documento, le deberá completar, identificando el fichero o tratamiento y al responsable del mismo (DESPACHO XXXX), e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

En todos los casos referidos, estas circunstancias se harán constar en el presente documento de seguridad, indicando todas las cuestiones necesarias para una correcta información y documentación de la situación, bien sea referida al acceso a los datos por el encargado del tratamiento en los locales del DESPACHO XXXX, bien sea la prestación del servicio y consecuente traslado de los datos a los locales del Encargado del Tratamiento.

Todo ello figurará debidamente documentado en el ANEXO X referido a los Encargados del Tratamiento.

**2.2 Prestaciones de servicios sin acceso a datos personales**

Se han tomado las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contienen o a cualquier recurso del sistema de información, cuando el trabajo que realizan no implica el tratamiento de datos personales.

Para el personal ajeno al DESPACHO XXXX, como puede ser el del servicio de limpieza de las oficinas o locales, mantenimiento de equipos e instalaciones y otros, el contrato de prestación de servicios recoge expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

**2.3 Recursos protegidos**

Entendiendo por recurso cualquier parte componente del sistema de información, estos serán los ficheros referidos, así como los soportes y equipos empleados para el almacenamiento y tratamiento de los datos de carácter personal. Debido a las características de los soportes de los ficheros no automatizados, el concepto alcanza también a los muebles, carpetas, archivadores, en su caso, a los locales y a cualesquiera otro elemento o material utilizado para la conservación, acceso, almacenamiento o depósito. Todos ellos garantizan la confidencialidad y adecuada custodia de los ficheros y los datos que contienen.

La descripción de los recursos en el presente documento se ha realizado, metodológicamente, individualizándola por ficheros y haciendo constar por cada uno del ellos su nombre, ubicación, breve descripción del contenido, finalidad, soporte físico sobre el que se encuentran los datos y, en general, del fichero y accesos, con identificación de la persona o personas que están autorizadas para acceder a los datos de carácter personal y, en su caso, la o las medidas de seguridad lógicas para garantizar la confidencialidad.

En particular, se refieren los siguientes recursos, por tratarse de los empleados para el almacenamiento y tratamiento de datos de carácter personal, a los que figuran en el documento denominado “Ficheros y su descripción” (Se adjunta como ANEXO II).

Los ficheros y/o los soportes que han sido indicados no pueden salir del local en el que se encuentran y que ha quedado descrito, sin autorización expresa del abogado responsable del fichero.

**2.4 Delegación de autorizaciones**

Cuando, de acuerdo con lo especificado en el Título VIII del Reglamento de la LOPD, sea necesaria la autorización del abogado responsable del fichero para realizar cualquier acción o actividad relativa al tratamiento de los datos o a las medidas de seguridad a adoptar, éstas autorizaciones pueden ser delegadas ya sea en su totalidad, ya sea individualmente o en grupos. Esta circunstancia constará en el ANEXO VI indicando las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación.

**3.- MEDIDAS, NORMAS, PROCEDIMIENTOS DE ACTUACIÓN, REGLAS Y ESTÁNDARES**

Solamente tienen acceso a los ficheros las personas referidas e identificadas en los apartados "accesos" y "relación de usuarios actualizada" del ANEXO II y con los controles de seguridad especificados.

También se ha especificado en el mismo apartado "accesos", del ANEXO II, la persona encargada del DESPACHO XXXX que gestiona los permisos de acceso de los usuarios, el procedimiento de asignación de estos permisos y la forma de concederlos y documentarlos durante su vigencia, para que no puedan ser conocidos por quien no tiene derecho o acceso autorizado a ello.

**3.1. Auditoría de Seguridad.**

Los ficheros objeto de este documento de seguridad se someterán, cada dos años, a una auditoría, interna o externa, que verifique el cumplimiento de lo contemplado en el Capítulo IV, del Título VIII del Reglamento de la LOPD.

El informe de auditoría dictaminará sobre la adecuación de las medidas y controles al Reglamento de Seguridad, identificará sus deficiencias y propondrá las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de auditoría serán analizados por el abogado responsable del fichero que adoptará las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos.

Con carácter extraordinario se realizará esta auditoría cada vez que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicial cómputo de dos años señalado.

Todo ello de acuerdo con lo establecido en el Capítulo IV, del Título VIII del Real Decreto 1720/2007, de 21 de diciembre y, en particular con lo especificado en el artículo 110 de dicha norma.

**3.2 Criterios de archivo.**

El abogado responsable del fichero ha establecido los criterios y procedimientos de actuación que deben seguirse para el archivo. Estos criterios garantizan la correcta conservación de los documentos, la localización y consulta de la información y posibilitan el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En particular, los criterios de archivo para los soportes o documentos objeto de este documento de seguridad, figuran en el apartado “Criterios de archivo” del ANEXO II.

**3.3 Identificación y autenticación.**

Se ha establecido un procedimiento que permite la identificación de forma inequívoca y personalizada de toda aquella persona que intenta acceder al sistema de información, comprobando, mediante los procedimientos adecuados, que quien accede está autorizado para ello en los límites de su autorización. Estos procedimientos se encuentran en el apartado “Identificación y autenticación” del ANEXO II.

**3.3 Dispositivos de almacenamiento.**

Los dispositivos de almacenamiento de los documentos que contienen datos de carácter personal disponen de mecanismos que obstaculizan su apertura en la forma que figura en el apartado “Soportes” del ANEXO II.

Los armarios, archivadores u otros elementos en los que se almacenan los ficheros objeto de este documento de seguridad se encuentran en áreas o espacios en las que el acceso está protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Estas áreas o espacios permanecen cerrados cuando no es preciso el acceso a los documentos incluidos en los ficheros.

**3.5 Custodia de los soportes.**

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

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

**3.6 Régimen de trabajo fuera de los locales.**

Cuando los datos se traten fuera de los locales del DESPACHO XXXX existirá una autorización previa del abogado responsable del fichero y se garantizará el nivel de seguridad correspondiente al tipo de fichero tratado (ver ANEXO VI).

**3.7 Copia o reproducción.**

La generación de copias o la reproducción de documentos únicamente se realiza bajo el control del abogado responsable del fichero o de persona autorizada de acuerdo con lo contemplado en el apartado “copia o reproducción de documentos” del ANEXO II.

Cuando una copia o reproducción es desechada se procede a su destrucción de forma que se imposibilite el acceso a la información contenida en las mismas o su recuperación posterior.

**3.8 Acceso a la documentación.**

El acceso a la documentación está limitado exclusivamente a las personas autorizadas que figuran en el ANEXO II.

Se ha establecido un mecanismo (ANEXO II), que permite identificar los accesos realizados en los casos en los que los documentos pueden ser utilizados por más de un usuario o usuarios.

Cuando tienen que acceder a la documentación, o a algún documento en particular, alguna persona no autorizada en el presente documento de seguridad, se ha establecido un procedimiento mediante el que, debidamente justificado, el acceso queda registrado con la autorización correspondiente.

**3.9 Traslado de documentación.**

Cuando se procede al traslado físico de la documentación contenida en un fichero, se adoptan medidas dirigidas a impedir el acceso o manipulación de la información objeto del traslado de acuerdo con lo establecido en el apartado “traslado de documentación” del ANEXO II.

**4.- FUNCIONES Y OBLIGACIONES DEL PERSONAL.**

Las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con el tratamiento de los datos de carácter personal, en el ámbito de aplicación del presente documento, pueden clasificarse en dos grupos:

a) Abogados responsables de un asunto, cliente o procedimiento que tiene asignado.

b) Usuarios de administración o servicios que, para su trabajo, necesitan acceder al fichero o a los datos de carácter personal.

En la descripción de los recursos han quedado perfectamente identificadas las personas que acceden a los ficheros y las que, por sus funciones u obligaciones en el DESPACHO XXXX, tienen alguna relación con las diferentes fases descritas en el tratamiento de datos de carácter personal.

Las funciones y obligaciones del personal para cada uno de los grupos son las que se establecen con carácter general para el tipo de actividad en el DESPACHO XXXX, pero, independientemente de estas funciones, cada una de estas personas se encuentra obligada a cumplir con lo especificado en este documento, conoce su contenido en lo que afecta al fichero que le atañe, ha sido informada de su responsabilidad en el almacenamiento, tratamiento o consulta de datos de carácter personal en el fichero, ha sido también informada y tiene a su disposición toda la información necesaria y el acceso al personal del DESPACHO XXXX que puede solucionar los problemas o dudas que tuviera sobre el particular.

Todo lo especificado en el presente documento es de obligado cumplimiento, en la parte en que a cada una le corresponde, para todas estas personas que se ha establecido, que quedan afectadas por la normativa, que conocen sus obligaciones y responsabilidades en la forma que se ha referido, y que son las que tienen alguna actividad relacionada con las fases de almacenamiento, tratamiento y/o consulta de datos de carácter personal sobre los recursos referidos.

Las funciones de control o autorizaciones delegadas por el responsable del fichero han quedado identificadas y documentadas en el ANEXO VI.

**4.1. Responsable de Seguridad.**

Se designa Responsable de Seguridad, de acuerdo con lo establecido en el artículo 95 y 109 del Reglamento de la LOPD, al abogado responsable del despacho. Dicho Responsable de Seguridad estará encargado de coordinar y controlar las medidas que se definen en el presente documento, respecto a las personas y accesos del DESPACHO XXXX, así como respecto a los recursos de la misma. **DEBE ESTABLECERSE LA MENCIÓN AL RESPOSANBLE DE SEGURIDAD CASO DE QUE SEA ALGUIEN DISTINTO DE UN LETRADO DEL DESPACHO.**

En ningún caso la designación efectuada supone una delegación de responsabilidad, que corresponde siempre al abogado responsable del despacho de acuerdo con lo dispuesto en el Reglamento de la LOPD.

En el ANEXO XI se harán figurar los controles periódicos que se realicen para verificar el cumplimiento de lo dispuesto en este documento.

**5.- CONTROL DE ACCESO**

Los ficheros se encuentran físicamente protegidos en los locales correspondientes de ubicación y con las medidas de seguridad física correspondientes al soporte en el que se encuentran. El personal responsable de cada uno de ellos conoce sus obligaciones para proteger físicamente los soportes en los que se encuentran los ficheros y no permitir su manejo, utilización ni, tan siquiera, identificación del soporte, por personas que no se encuentren autorizadas en el presente documento respecto al fichero de que se trate.

Desde El punto de vista lógico, cada usuario tiene acceso solamente a aquellos datos y recursos a los que se encuentra autorizado, habiéndose establecido procedimientos de seguridad física y lógica para que usuarios no autorizados no tengan acceso a los ficheros que no les correspondan, de acuerdo con lo especificado y establecido en este documento.

En la relación de usuarios creada, y que figura en los apartados "accesos" y "usuarios" del ANEXO II, se señala el acceso autorizado para cada uno de los usuarios, acceso que conoce el usuario y el abogado responsable del fichero.

La modificación de algún dato o información sobre la concesión, alteración, modificación, inclusión o anulación de los accesos autorizados y los usuarios que figuran en la relación correspondiente de este documento, ya referida, corresponde exclusivamente a quien figura como abogado responsable del fichero en el Anexo II.

**5.1. Control de acceso físico**

Los locales en los que se ubican los componentes del sistema de información gozan de protección especial que garantiza la confidencialidad de los datos. Esta protección especial está descrita en el ANEXO II.

Exclusivamente el personal autorizado que figura en el ANEXO II podrá tener acceso a los locales o ubicación física de los equipos que den soporte al sistema de información con datos de carácter personal que es objeto de este documento.

**6.- GESTIÓN DE SOPORTES Y DOCUMENTOS**

Los soportes en los que se encuentran los ficheros son los especificados en el apartado "***soporte físico***" del Anexo II.

Los soportes quedan identificados en su carátula, o elemento en los que se encuentren, con descripción sencilla pero identificadora del contenido; se encuentran inventariados en el documento de inventario correspondiente del DESPACHO XXXX y están almacenados con las debidas precauciones para que solamente tengan acceso a ellos las personas autorizadas de acuerdo con lo ya especificado en este documento.

Cuando vaya a desecharse un documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior, tal y como se contempla en el ANEXO II y de dará de baja en el inventario de soportes.

No se pueden sacar soportes de los locales que tienen asignados sin permiso expreso y por escrito del abogado responsable del fichero. A tal fin, será necesaria autorización del abogado responsable del fichero conforme a lo previsto en el Anexo VI y la cumplimentación del registro de salida de soportes que consta en el Anexo VIII.

La salida de soportes y documentos que tengan datos de carácter personal fuera de los locales bajo el control del responsable del fichero o tratamiento (el DESPACHO XXXX), deberá ser autorizada por el responsable del fichero o, en su caso, estar autorizada tal y como se contempla en el ANEXO VI.

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

Como se trata de soportes autónomos e independientes, la persona encargada de su vigilancia y control tomará las medidas necesarias para que no puedan acceder a dicho soporte físico aquellos que no se encuentren autorizados de acuerdo con lo establecido en este documento.

Los ficheros se encuentran bajo la responsabilidad del abogado responsable del fichero, quien se encargará del almacenamiento y puesta a disposición solamente de aquellos que se encuentren autorizados.

**6.1 Sistema de Registro de Entrada/Salida de soportes.**

Se establece un sistema de registro de entrada de soportes que permite conocer el tipo de documento o soporte, la fecha y hora de entrada, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que, en todos los casos, estará autorizada para ello, tal y como consta en el Anexo VII.

De igual forma, se establece un sistema de registro de salida de soportes que permite conocer el tipo de documento o soporte, la fecha y hora de salida, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que, en todos los casos, estará autorizada para ello, y que figura en el Anexo VIII.

**6.2 Baja del soporte del inventario.**

El Responsable de Seguridad ha adoptado las medidas necesarias, para que, en caso de que un soporte vaya a ser desechado o reutilizado, no pueda recuperarse la información en él contenida, habiéndose dado de baja el mismo en el inventario.

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

Toda la información impresa o escrita, en soporte papel o cualquier otro, recogida de papeleras o contenedores de papel es destruida conforme al procedimiento descrito en el Anexo II.

**7.- ESTRUCTURA DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL Y DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE LOS TRATAN.**

Los ficheros de datos de carácter personal a los que es de aplicación el presente Documento de Seguridad, son los que se han indicado en el apartado 1, y que figuran en el Anexo II.

La ubicación física de los ficheros se recoge en el apartado "***ubicación***" del Anexo II.

El contenido lógico de cada uno de ellos, con la descripción detallada de sus componentes, son los que, para cada fichero, figuran en el Anexo III.

Los sistemas de información que tratan estos ficheros y, consecuentemente, los datos de carácter personal que en ellos se encuentran, son los que figuran en los apartados "***soporte físico***", "***almacenamiento***" y "***dispositivos de almacenamiento***" del Anexo II de este documento.

**8.- PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.**

A efectos del presente Documento de Seguridad, se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos; esto es, será una incidencia cualquier circunstancia que pueda darse y afecte al fichero, o a los datos, de forma que constituya, o pueda constituir, un riesgo o inseguridad para la confidencialidad e integridad de los propios ficheros y de los datos de carácter personal que contienen.

Por tanto, con el fin de garantizar la confidencialidad e integridad de la información contenida en los ficheros, se establece un procedimiento de notificación y gestión de incidencias con vistas a prevenir el peligro que representen para la seguridad de la información y para poder tener conocimiento del lugar, fecha, hora y motivo por el que se ha producido la incidencia y el responsable o responsables de la misma.

**8.1 Registro de incidencias.**

A estos efectos se crea un libro registro de incidencias, bajo la responsabilidad del abogado responsable del fichero, en el que se harán constar el tipo de incidencia, el momento -día y hora- en el que se ha producido, o en su caso, detectado, la persona que realiza la notificación de la incidencia, a quien se le comunica, los efectos que se hubieran derivado de la incidencia y las medidas correctoras aplicadas.

De esta forma, todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento y/o consulta de datos de carácter personal en los ficheros objeto de este documento, tiene conocimiento, mediante la correspondiente circular que se les ha hecho llegar y cuya copia figura en el Anexo IX, del procedimiento para actuar en caso de incidencia; este procedimiento se les ha dado a conocer con instrucciones en las que se especifican:

a) Que cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad o a la integridad de la información deberá comunicarlo inmediatamente al abogado responsable del fichero, con identificación clara del tipo de incidencia producida y su descripción detallada, en la que figurarán las intervenciones de personas que hayan podido tener relación con la producción de la incidencia, el momento -día y hora- en el que se ha producido, o en su caso, detectado, la persona que realiza la notificación de la incidencia, a quien se le comunica y los efectos que se hubieran derivado de la incidencia así como las medidas correctoras aplicadas.

b) Que una vez comunicada la incidencia deberá solicitar del abogado responsable del fichero un acuse de recibo en el que se haga constar que ha recibido la notificación de la incidencia y que ésta notificación contiene todos los requisitos que se han establecido en el anterior apartado a).

El presente documento ha sido redactado y aprobado por el abogado responsable del DESPACHO XXXX, y, ratificándose en él, aceptándolo en su totalidad y ordenando su ejecución y cumplimiento, en particular todos aquellos a quienes afecta en tanto que participan en el tratamiento de datos personales de especial sensibilidad, y en general todo el personal del DESPACHO XXXX, para lo que se comprometen a acatar las medidas señaladas en el presente documento, así como a contribuir a su implementación y desarrollo sobre la base de las instrucciones que por escrito pudieran darse por el responsable de cumplimiento.

A tal fin, todos ellos suscriben con su forma el presente documento, lo que hacen en la ciudad de Barcelona, a xx, de Xxxxxxx, de 20xx.

**ANEXO I:**

**NOTIFICACIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DE HABER PROCEDIDO A LA INSCRIPCIÓN DE CADA UNO DE LOS FICHEROS**

**(ACÚDASE AL SISTEMA NOTA DE LA AEPD)**

ANEXO II:

FICHEROS Y SU DESCRIPCIÓN

FICHERO CLIENTES

NOMBRE FICHERO

CLIENTES

UBICACIÓN

Calle de Xxxxxx, número xx, piso x, puerta x.

DESCRIPCIÓN DEL CONTENIDO

Contiene los datos necesarios para la gestión de la relación con los clientes, encontrándose dos grupos diferenciados

- Gestión del asunto jurídico (asesoramiento, demanda, dictamen, etc.)

- Gestión de la facturación

ESTRUCTURA DEL FICHERO

Existe un fichero de clientes que está formado por las diversas carpetas de cada uno de los clientes.

Por cada cliente, existe un registro que contiene los documentos necesarios para su gestión desde los dos ámbitos descritos:

1. Gestión del asunto jurídico en el que se identifican los siguientes apartados:

a) Identificación del cliente (nombre, dirección, etc.)

b) Número de expediente

c) Tipo de gestión (orden jurisdiccional civil, penal, administrativo, dictamen, asesoramiento, etc.)

d) Etc. (poner todos los apartados que pueden ser identificados y/o tratados en forma autónoma, por ejemplo, procuradores, teléfonos, …)

2. Gestión de la facturación en el que se identifican los siguientes apartados

a) Identificación del cliente (nombre, dirección, etc.)

b) Número de expediente

c) Datos bancarios

d) Gestión contable (facturas, etc.)

SOPORTES

Los ficheros se encuentran en estanterías en armarios habilitados para su almacenamiento que disponen de llave. La llave está bajo el control único del abogado responsable del fichero o de la persona autorizada de acuerdo con lo contemplado en el ANEXO VI

Cada fichero está formado por tantos registros como clientes haya, a razón de un registro por cliente. Los registros se encuentran en carpetas archivadoras.

El fichero está formado por múltiples registros, uno por cada cliente, que se encuentran en carpetas aptas para el almacenamiento (de anillas, fundas plastificadas, etc.)

Los armarios se encuentran en una habitación independiente, conocida con el nombre de “***archivo***”, que se encuentra siempre cerrada y está dotada de llave con candado de tipo clave, y a la que solamente tiene acceso el abogado titular del despacho y la persona autorizada de acuerdo con lo que figura en el ANEXO VI de este documento.

**(NOTA: Si, atendidas las características de los locales de que dispusiera el abogado responsable del fichero, no fuera posible cumplir con lo anterior, se adoptarán medidas alternativas que, debidamente motivadas, se incluirán en este documento de seguridad)**

SOPORTE FÍSICO

a) Identificación: las carpetas se identifican mediante etiquetas con los apartados señalados de identificación del cliente.

b) Inventario: existe un inventario de los soportes tal y como se indica en el Anexo IV del presente documento.

c) El conjunto de carpetas forma el fichero al que se accede en su propia estantería con medidas de seguridad física (llave) independiente.

ACCESOS

a) Permiso de acceso a los usuarios

El abogado responsable del fichero concede, altera o anula los accesos de los diferentes usuarios de acuerdo con sus funciones y la necesidad de acceder, tratar o conocer datos de carácter personal. Se establecen perfiles de usuarios de acuerdo con la función del personal en el despacho.

b) Alcance del acceso

El alcance del acceso será el necesario para realizar sus funciones de acuerdo con el puesto de trabajo. El criterio de concesión le establece el abogado responsable del fichero.

c) Autorización del acceso

El acceso a los ficheros, documentos y datos de carácter personal le autoriza el abogado responsable del fichero en virtud de que se trate de una persona concreta que necesite el acceso a los datos para cumplir sus funciones.

RELACIÓN DE USUARIOS ACTUALIZADA

(Deben indicarse por medio de un listado los usuarios y sus razones de accesos – por ejemplo, los abogados del despacho tienen acceso a los expedientes de clientes para el desarrollo de labores de defensa y asesoramiento, pero el personal administrativo tiene acceso a los expedientes de facturación)

CRITERIOS DE ARCHIVO Y DE ACCESO

Cada cliente tiene su propio registro con la organización y contenido que se ha expresado en el apartado “estructura del fichero”.

Dentro de la carpeta de cada cliente, se ordenan los documentos que, dependiendo del tipo de asunto, pueden ser de múltiples clases (p.e. escrito de demanda, contestación a la demanda, etc.). Estos documentos están identificados por su contenido, teniendo una carátula u hoja primera que así lo identifica y se puede acceder por ellos cronológicamente (o por datos del cliente, o por orden alfabético, etc.)

Cuando se crea un expediente nuevo se abre una carpeta registro dependiendo del tipo de expediente que es. Se genera una carátula con los datos ya indicados y queda archivado en su fichero y en el armario correspondiente.

El archivo de los soportes y/o documentos se realiza de acuerdo con los criterios previstos en su legislación específica y, en caso de no existir esta, de acuerdo con los criterios aquí establecidos.

Cuando una persona solicita un expediente o registro de un cliente, el abogado titular del despacho, o la persona autorizada de acuerdo con lo contemplado en el ANEXO VI, comprueban que esa persona figura en el presente documento de seguridad, personalmente o por su perfil profesional, como autorizado para acceder a dicho registro y, tras comprobar su identidad y posibilidad de acceso, le facilitan el expediente quedando constancia del acceso y los documentos a los que accede y si, en su caso, se lleva materialmente el expediente completo o unos u otros documentos. La persona que realiza el acceso firma el recibí del expediente y se queda encargada de su custodia y garantía de confidencialidad e impedirá en todo momento que pueda ser accedido por persona no autorizada durante el tiempo que le tiene en su poder que, en ningún caso, puede superar el tiempo de la jornada laboral.

Al terminar dicha jornada laboral, o cuando ya no necesita el acceso o consulta, devuelve el expediente a la misma persona que le autorizó la recogida y se firma un documento de entrega del expediente, que queda nuevamente archivado y depositado en su lugar de ubicación, dentro de su carperta, en el armario y todo ello (armario y habitación en la que se encuentra) cerrado con llave y en habitación independiente también cerrada, que queda bajo el único control del abogado titular del despacho o la persona autorizada en los términos ya referidos.

Cuando los documentos tengan que ser utilizados por más de un usuario, se verificará por el abogado responsable del fichero, o la persona autorizada, la licitud del acceso de cada uno de acuerdo con lo anteriormente establecido y se procederá, mediante un procedimiento de entregas y devoluciones documentadas (entrega firmada, motivo y devolución documentada y firmada), aceptadas y firmadas por el usuario y la persona que autoriza, qué documento, registro, o parte de ellos, está en poder de cada usuario.

Cuando tiene que acceder a la documentación, o a algún documento en particular, alguna persona no autorizada en el presente documento de seguridad, se ha establecido un procedimiento mediante el que, debidamente justificado, el acceso queda registrado con la autorización correspondiente, documentada, firmada y argumentada, del abogado responsable del fichero o de la persona autorizada de acuerdo con lo establecido en este documento.

UTILIDAD FINAL DEL FICHERO.

Se trata de una obviedad que puede generalizarse bajo una cita del tipo “Llevar a cabo la gestión de la relación contractual entre los clientes (hojas de encargo, desarrollo de la actividad, recepción de documentación, entrega trabajo final, facturación, etc.) y el Letrado director o el Despacho XXXXX.

SISTEMA DE REGISTRO DE ENTRADA DE SOPORTES INFORMÁTICOS

Véase el Anexo VII.

a) Tipo de soporte o documento:

b) Fecha y hora:

c) Emisor:

d) Número de soportes o documentos incluidos en el envío:

e) Tipo de información contenida:

f) Forma de envío:

g) Responsable recepción (que deberá estar debidamente autorizado):

SISTEMA DE REGISTRO DE SALIDA DE SOPORTES INFORMÁTICOS

Véase el Anexo VIII.

a) Tipo de soporte o documento:

b) Fecha y hora:

c) Destinatario:

d) Número de soportes o documentos incluidos en el envío:

e) Tipo de información contenida:

f) Forma de envío:

g) Responsable de la entrega (que deberá estar debidamente autorizado):

SOPORTES REUTILIZADOS

Si los soportes que almacenan datos de carácter personal (archivadores, carpetas), van a ser reutilizados, previamente se destruyen todos los datos anteriores para impedir la identificación de su utilización anterior.

SOPORTES DESECHADOS

En el caso de que los soportes que contengan datos de carácter personal vayan a ser desechados se destruyen.

Si se trata de papel se utiliza una destructora de papel que garantiza la imposibilidad de identificación de ningún dato en el papel así destruído. Resulta totalmente imposible identificar o leer dato alguno del papel así destruido.

Si se trata de carpetas o archivadores, se quitan todas sus etiquetas identificativas que contengan datos y se destruyen en la forma indicada. En caso de imposibilidad, se somete a la carpeta o archivador a un proceso de destrucción manual que impida totalmente la identificación, recuperación o simple lectura de un dato anterior.

EJECUCIÓN TRATAMIENTO FUERA DE LOCALES

Cuando los soportes o documentos en los que se almacenan los datos de carácter personal tengan que salir fuera de la ubicación física del fichero deberá contarse con la autorización por escrito del responsable del fichero en los términos previstos en el Anexo VI.

IDENTIFICACIÓN

Solamente las personas autorizadas pueden acceder a los datos del fichero, La identificación de la persona autorizada a acceder a los ficheros o a los documentos se realiza por el titular del despacho o persona autorizada de acuerdo con lo contemplado en el presente ANEXO (en el aparatado “criterios de archivo y de acceso”), comprobando que esa persona necesita por su función acceder a los datos.

ACCESOS

Control de accesos:

i) El abogado responsable del fichero es la persona que controla los accesos y concede los permisos de acceso a los diferentes usuarios dependiendo de sus funciones y necesidad de tratamiento de los datos.

ii) Alcance del acceso: el alcance del acceso a los datos es el necesario para desarrollar las funciones propias del puesto de trabajo.

iii) El criterio de concesión, alteración o anulación del acceso es el que ha establecido y hecho figurar en este documento de seguridad el abogado responsable del fichero.

Cuando una persona solicita un expediente o registro de un cliente, el abogado titular del despacho, o la persona autorizada de acuerdo con lo contemplado en el ANEXO VI, comprueban que esa persona figura en el presente documento de seguridad, personalmente o por su perfil profesional, como autorizado para acceder a dicho registro y, tras comprobar su identidad y posibilidad de acceso, le facilitan el expediente quedando constancia del acceso y los documentos a los que accede y si, en su caso, se lleva materialmente el expediente completo o unos u otros documentos. La persona que realiza el acceso firma el recibí del expediente y se queda encargada de su custodia y garantía de confidencialidad, impidiendo el acceso a personas no autorizadas, durante el tiempo que le tiene en su poder que, en ningún caso, puede superar el tiempo de la jornada laboral.

FUNCIONES DEL PERSONAL

Las funciones del personal del despacho con acceso a los datos de carácter personal están descritas en el Anexo V del presente documento.

DOCUMENTACIÓN FUNCIONES DEL PERSONAL

Las funciones del personal del despacho con acceso a los datos de carácter personal están documentadas en el Anexo V del presente documento.

COPIA O REPRODUCCIÓN DE DOCUMENTOS

Si por cualquier motivo, debidamente argumentado y documentado, es necesario realizar una copia o reproducir un documento, ésta tendrá que ser autorizada por el abogado responsable del fichero o la persona autorizada de acuerdo con lo contemplado en el ANEXO VI.

La copia se realizará bajo la supervisión de estas personas y se destruirá una vez que ya no sea necesaria para la función que la justificó.

Se quedará debidamente registrada la copia realizada de forma que esté identificada quién la ha realizado, con qué fin y la autorización concedida. La persona que recibe la copia firma un documento a modo de recibí y se queda encargada de su custodia y garantía de confidencialidad, impidiendo el acceso a personas no autorizadas, durante el tiempo que le tiene en su poder.

ACCESO A LA DOCUMENTACIÓN

El acceso a la documentación está limitado exclusivamente a las personas autorizadas que figuran en el presente ANEXO, de acuerdo con sus funciones (ver ANEXO V funciones del personal).

Se ha establecido un mecanismo (ver “criterios de archivo y de acceso”), que permite identificar los accesos realizados en los casos en los que los documentos pueden ser utilizados por más de un usuario o usuarios.

Cuando tienen que acceder a la documentación, o a algún documento en particular, alguna persona no autorizada en el presente documento de seguridad, se ha establecido un procedimiento mediante el que, debidamente justificado, el acceso queda registrado con la autorización correspondiente (ver “criterios de archivo y acceso”).

TRASLADO DE DOCUMENTACIÓN

Cuando se procede al traslado físico de la documentación contenida en el fichero, se adoptan medidas dirigidas a impedir el acceso o manipulación de la información objeto del traslado y, entre ellas, identificación autónoma e independiente de los documentos, en sobre cerrado y firmado por el abogado responsable del fichero en su solapa, que queda bajo la responsabilidad y custodia de la persona encargada del traslado que, a su vez, tiene que estar autorizada por el abogado responsable del fichero o persona en quien delegue de acuerdo con lo contemplado en el ANEXO VI del presente documento.

RESPONSABLE DE SEGURIDAD

El responsable de seguridad es el abogado titular del Despacho

PROCEDIMIENTO DE INCIDENCIAS

Véase el Anexo IX en el apartado CIRCULAR SOBRE PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

a) Notificación:

b) Gestión:

c) Respuesta:

REGISTRO DE INCIDENCIAS

Para lograr un control sobre las incidencias que tengan lugar respecto de los ficheros del despacho es necesario crear un Registro que recoja la siguiente información de cada incidencia que se produzca.

a) Tipo de incidencia:

b) Momento de su producción o momento en que se ha detectado:

c) Persona que lo notifica:

d) Persona a la que se comunica:

e) Efectos derivados de la incidencia:

f) Medidas correctoras aplicadas

AUDITORÍA

a) Realización cada dos años:

b) Informe de auditoría:

i) Adecuación medidas:

ii) Adecuación controles:

iii) Identificación deficiencias:

iv) Propuesta medidas correctoras o complementarias:

v) Documentación conclusiones:

- Datos

- Hechos

- Observaciones

MEDIDAS CORRECTORAS

En su caso, se adoptarán las medidas correctoras o complementarias que se hayan propuesto en el informe de auditoría realizado.

ACTUALIZACIÓN DEL DOCUMENTO

Se actualizará cuando sea necesario, conforme a los cambios que se produzcan en el sistema de información o en la normativa vigente en materia de medidas de seguridad.

REVISIÓN DOCUMENTO POR CAMBIOS RELEVANTES EN S.I.

Será revisado si se producen cambios relevantes en el sistema de información o en la organización del mismo.

ADECUACIÓN DEL DOCUMENTO

Se adecuará a los cambios que se produzcan en el sistema de información y en la normativa sobre medidas de seguridad.

ANEXO III:

CONTENIDO DE CADA FICHERO

DESPACHO XXXX

Titular responsable Letrado D.

Colegiado número xxxxx del Ilustre Colegio de Abogados de Xxxxxxxxxxxxxxx.

(En este ANEXO se expondrá el contenido de cada fichero, con explicación detallada de los documentos que incorpora. A modo de ejemplo, hemos realizado una plantilla que se puede rellenar por cada fichero respondiendo a lo que debe figurar)

FICHERO CLIENTES

I. CARACTERÍSTICAS DEL FICHERO

Nombre Clientes

Ubicación calle( tal número cual)

Descripción

Finalidad y usos previstos

II. CONTENIDO – DATOS DE BASE

Carácter identificativo Nombre y apellidos, Dirección (postal, electrónica), Teléfono, Otros (Organización)

Productos o servicios

Datos facturación

Económico-financieros Datos bancarios.

III. DOCUMENTOS AUTÓNOMOS IDENTIFICABLES

En este apartado se relacionarán por su identificación inequívoca, aquellos documentos independientes que, unidos al fichero o adjuntados de alguna forma a su contenido, contengan datos de carácter personal que, si no estuvieran así especificados, sería añadidos a los datos de base del fichero (por ej. escrituras, nóminas, contratos de arrendamiento, etc.).

IV. SOLICITUD DE INFORMACIÓN O AUTORIZACIÓN

En el caso de que una persona no autorizada en el documento de seguridad del fichero, tuviera necesidad de obtener información o acceso a datos contenidos en el mismo o de utilizar documentos que formen parte del fichero, incluso realizando fotocopias de alguno de sus componentes, deberá obtener un permiso previo de acceso en el que, por persona autorizada, se especifique el alcance del acceso y la realización de fotocopias.

V. DATOS ESPECIALMENTE PROTEGIDOS

Este fichero no contiene ningún dato que sea considerado por la LOPD como especialmente protegido. En su caso, poner esta otra redacción:

***En este fichero se encuentran datos que la LOPD califica como “especialmente protegidos” (datos referentes a ideología, afiliación sindical, religión, creencias, salud, origen racial y vida sexual), y sobre los cuales hay que tomar unas medidas especiales de acceso y tratamiento. Consultar con el responsable del fichero sobre estas medidas y tener en consideración todas las características especiales de protección.***

VI. MEDIDAS DE SEGURIDAD

Nivel de Seguridad Alto

Responsable de seguridad El abogado titular del despacho

Control de acceso De acuerdo con lo que figura en el ANEXO II

Autorización De acuerdo con lo que figura en el ANEXO VI

Tratamiento fuera del lugar de ubicación – Fotocopias De acuerdo con lo que figura en el ANEXO II

Borrado De acuerdo con lo que figura en el ANEXO II

Destrucción De acuerdo con lo que figura en el ANEXO II

Copia o reproducción de los datos De acuerdo con lo que figura en el ANEXO II

Registro de incidencias De acuerdo con lo que figura en el ANEXO IX

VII. CESIÓN O COMUNICACIÓN DE DATOS

Previstas, con consentimiento o por excepción legal.

No prevista, siempre con consentimiento

VIII. ENCARGADO DEL TRATAMIENTO

No existen encargados del tratamiento para este fichero. En el caso de que existan encargados del tratamiento, todas las características figuran en el ANEXO X

IX. DELEGACIONES/AUTORIZACIONES

No existen delegaciones ni autorizaciones para este fichero o, en su caso, las delegaciones y autorizaciones previstas en el Reglamento de la LOPD figuran en el ANEXO VI

ANEXO IV:

SOPORTES FÍSICOS EN LOS QUE SE ALMACENAN DATOS DE CARÁCTER PERSONAL

INVENTARIO DE LOS SOPORTES FÍSICOS EN LOS QUE SE ALMACENAN DATOS DE CARÁCTER PERSONAL

**NOMBRE DEL FICHERO**

**TIPO DE SOPORTE S/N ALTA IDENTIFICACIÓN REUTILIZACIÓN DESTRUCCIÓN BAJA**

**Carpeta Cliente (Fecha) (Fecha)**

**Carpeta Procurador (Fecha) (Fecha)**

**Carpeta Contabilidad (Fecha) (Fecha)**

**Otros soportes (Fecha) (Fecha)**

ANEXO V:

FUNCIONES Y DOCUMENTACIÓN DE LAS FUNCIONES DEL PERSONAL DE DESPACHO XXXX

ANEXO VI:

DELEGACIÓN DE AUTORIZACIONES Y AUTORIZACIONES NECESARIAS PARA EL TRATAMIENTO DE DATOS PERSONALES

En este ANEXO figurará una autorización para cada caso de los que se contemplan en el cuerpo del documento de seguridad (ponemos, a modo de ejemplo, una autorización para tratamiento fuera de los locales de ubicación del fichero)

Las autorizaciones que se atribuyen en el documento de seguridad al abogado responsable del fichero podrán ser delegadas en las personas que éste considere convenientes. En este ANEXO deberán constar las personas habilitadas para otorgar las autorizaciones así como aquéllas en las que recae dicha delegación.

AUTORIZACIÓN DEL TRATAMIENTO FUERA DE LOS LOCALES DE UBICACIÓN DEL FICHERO

DATOS DEL RESPONSABLE DEL FICHERO:

D. \_\_\_\_\_\_\_\_\_\_\_\_\_\_, como responsable del fichero, y en cumplimiento del artículo 86 del Real Decreto 1720/2007, de 21de Diciembre, por el que se aprueba el Reglamento de la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal, autoriza expresamente mediante el presente documento a D. …………………………………………….(en este punto cabe un concreto usuario o a un perfil de usuario genérico), para que pueda realizar el tratamiento de los datos de carácter personal relativos al fichero denominado \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ fuera del local en el que se encuentra ubicado el mismo, situado en (dirección) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

D. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ se compromete a aplicar las medidas de seguridad de nivel (básico, medio o alto) que correspondan a este fichero, en virtud de la naturaleza de los datos que son tratados en él .

Esta autorización tiene un período de validez de 30 días a partir de la fecha en que es concedida.

En \_\_\_\_\_\_\_\_\_\_\_\_ , a \_\_, de \_\_\_\_\_\_\_\_\_\_\_\_ de 200\_

Fdo.

ANEXO VII:

REGISTRO DE ENTRADA DE SOPORTES

SOPORTE O DOCUMENTO

Tipo de soporte o documento:

Número de soportes o documentos incluidos en el envío:

Tipo de información que contienen:

INFORMACIÓN DE LA RECEPCIÓN

Fecha:

Hora:

Forma de envío:

EMISOR

Emisor:

AUTORIZACIÓN

Persona responsable de la recepción (debidamente autorizada):

ANEXO VIII:

REGISTRO DE SALIDA DE SOPORTES

SOPORTE O DOCUMENTO

Tipo de soporte o documento:

Número de soportes o documentos incluidos en el envío:

Tipo de información que contienen:

INFORMACIÓN DEL ENVÍO

Fecha:

Hora:

Forma de envío:

DESTINATARIO

Destinatario:

AUTORIZACIÓN

Persona responsable de la entrega (debidamente autorizada):

ANEXO IX:

CIRCULARES COMUNICADAS A TODA PERSONA QUE TIENE ACCESO A DATOS DE CARÁCTER PERSONAL EN DESPACHO XXXX

CIRCULAR SOBRE IMPLANTACIÓN DE MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

En Barcelona, a \_\_\_\_ de \_\_\_\_ de 200

En cumplimiento de lo previsto por la actual normativa sobre protección de datos de carácter personal, y en especial de lo prescrito por el Capítulo IV, del Título VIII, 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 (LOPD), se le comunica, como persona que tiene acceso a dichos datos de carácter personal, sus obligaciones y responsabilidad respecto al almacenamiento, consulta y tratamiento de datos de carácter personal en los ficheros a los que tiene acceso según las funciones que desarrolla en DESPACHO XXXX.

En este sentido, se le señala su obligación de respetar el deber de secreto y confidencialidad sobre los datos de carácter personal a los que se tiene acceso así como su utilización única y exclusiva para los fines para los que han sido recabados.

Las medidas de seguridad para los ficheros que tienen datos de carácter personal se encuentran detalladas en el pertinente documento de seguridad que usted conoce, debe cumplir y que se halla a su disposición en xxxx (poner dónde), para cualquier información sobre sus obligaciones específicas al respecto.

El incumplimiento de dichas medidas de seguridad constituye paral responsable del fichero una infracción grave sancionable con multa de hasta 300.506,05 €, por lo que cuando dicho incumplimiento se asocie a un individuo concreto será sancionado a nivel interno disciplinariamente según se acuerde por el Responsable del Fichero.

\_\_\_\_\_\_\_\_\_

Responsable del fichero

CIRCULAR SOBRE PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

En Barcelona, a \_\_\_\_ de \_\_\_\_\_\_ de 200

En cumplimiento de lo previsto por la actual normativa sobre protección de datos de carácter personal, y en especial de lo prescrito por el Capítulo IV, del Título VIII, 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 (LOPD), se le comunica, como persona que tiene acceso a dichos datos de carácter personal, el procedimiento a seguir en caso de que conozca alguna incidencia en su tratamiento, entendida ésta como “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”, esto es cualquier circunstancia que pueda darse y afecte al fichero de forma que constituya, o pueda constituir, un riesgo o inseguridad para la confidencialidad e integridad del propio fichero y de los datos de carácter personal que contiene.

Este procedimiento consta de dos pasos diferenciados:

I. Notificación al responsable del fichero en caso de que la incidencia sea comunicada por un tercero, esto es, al abogado titular del despacho, en la que se hagan constar los siguientes extremos:

1. Identificación clara del tipo de incidencia producida

2. Descripción detallada de la incidencia:

a) Intervenciones de personas que hayan podido tener relación con la producción de la incidencia.

b) Momento -día y hora- de su producción o, en su caso, cuándo se ha detectado.

c) Persona que notifica la incidencia

d) Persona a la que se comunica la incidencia

e) Efectos derivados de la incidencia

f) Medidas correctoras aplicadas

II. Solicitar de dicho responsable un acuse de recibo en el que se haga constar que ha recibido la notificación de la incidencia y que contiene todos los extremos mencionados en el apartado I.

\_\_\_\_\_\_\_\_\_

Responsable del fichero

ANEXO X:

CONTRATOS CON ENCARGADOS DEL TRATAMIENTO

En este ANEXO deberán figurar todos los contratos con encargados del tratamiento (ver figura de encargado del tratamiento en la guía práctica).En dichos contratos figurarán todas las exigencias del artículo 12 de la LOPD y de los apartados 5 y 6, del artículo 88 del Reglamento que la desarrolla (artículo 88.5). Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

De conformidad con el artículo 88.6, en aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este Reglamento.

ANEXO XI:

CONTROLES PERIÓDICOS

**En este ANEXO deberán figurar detallada y documentalmente los controles periódicos que se realicen para verificar el cumplimiento de lo dispuesto en este documento. Se trata de establecer unas hojas de supervisión donde se anoten las fechas de los controles efectuados y la persona concreta que los lleva a cabo, así como su resultado (generalmente, “sin incidencias reseñables” o “sin incidencias”).**