ANEXO [●]

MEDIDAS DE SEGURIDAD

Este Anexo contiene las medidas de seguridad que, a criterio del Cliente, deberán ser implementadas por el Proveedor de acuerdo **con el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal aprobado en el R.D. 1720/2007, de 21 de diciembre de 2007** ("Reglamento de Medidas de Seguridad") al objeto de garantizar la seguridad y la integridad de los datos de carácter personal a tratar por el Proveedor (como encargado del tratamiento) por cuenta del Cliente (como responsable del tratamiento) al objeto de prestar los Servicios.

Dado que bajo el Reglamento de Medidas de Seguridad, el tipo de datos de carácter personal a tratar en cada caso, condiciona el nivel de medidas de seguridad que deben ser implementadas, se han clasificado las distintas medidas de seguridad en los siguientes tres niveles identificados con los colores mencionados a continuación: Nivel básico (**identificado en color verde**); nivel medio (**identificado en color azul**) y nivel alto (**identificado en color rojo**). Los niveles de seguridad son acumulativos, es decir, el nivel medio incluye también el nivel básico y el nivel alto incluye también los niveles medio y básico. Junto a esto, en algunos casos (**y en color negro**), se incluyen descripciones de los procedimientos específicos que serán aplicados a fin de alcanzar los objetivos perseguidos por las medidas de seguridad.

Las medidas de seguridad a aplicar por el Proveedor bajo el Contrato se corresponden con las de nivel: [●]

1. **DOCUMENTO DE SEGURIDAD**

1.1 Deberá elaborarse e implantarse la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

1.2 El documento deberá contener, como mínimo, los siguientes aspectos:

(a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

(b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Anexo.

(c) Funciones y obligaciones del personal.

(d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

(e) **Medidas de transporte, destrucción de soportes y documentos y reutilización de los últimos.**

(f) Procedimiento de notificación, gestión y respuesta ante las incidencias.

(g) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

(h) La identificación del responsable o responsables de seguridad (véase apartado 8 de este Anexo).

(i) los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

1.3 El contenido del documento deberá adecuarse, en todo momento, a las instrucciones del Cliente como responsable del tratamiento.

1.4 Siempre sujeto a las instrucciones del Cliente como responsable del tratamiento, el documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

1.5 Al objeto de cumplir con las medidas de seguridad previstas en este apartado 1, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

☒ **Elaboración del documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.**

☒ **Gestión de derechos AROC**

2. **DETERMINACIÓN DE LAS FUNCIONES Y OBLIGACIONES DEL PERSONAL**

2.1 Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de medidas de seguridad (apartado 1.2.(c) de este Anexo). También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2.2 Deberán adoptarse 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.

2.3 Al objeto de cumplir con las medidas de seguridad previstas en este apartado 2, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

☒ Políticas internas de tratamiento de datos, así como de procedimientos, guías, instrucciones, descripciones de procesos y normas para la programación, prueba y revelación de datos siempre que los mismos estén relacionados con los datos proporcionados por el Cliente.

☒ Formulación de un concepto de seguridad de los datos;

☐ Examen de las políticas y estándares de la industria;

☒ Concepción de un plan de emergencias (plan de contingencia de recuperación de información).

3. **REGISTRO DE INCIDENCIAS**

3.1 Existirá un procedimiento de notificación y gestión de incidencias.

3.2 Dicho procedimiento contendrá necesariamente un registro en el que se haga constar:

(a) El tipo de incidencia;

(b) el momento en que se ha producido;

(c) la persona que realiza la notificación;

(d) a quién se le comunica;

(e) los efectos que se hubieran derivado de la misma;

(f) **medidas correctoras aplicadas.**

(g) los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación. Será necesaria la autorización por escrito del Cliente (como responsable del fichero) para la ejecución de los procedimientos de recuperación de los datos.

☒ **Procedimiento de notificación y gestión de incidencias;**

☒ **Registro de incidencias;**

☒ **Procedimientos y autorizaciones para recuperación de datos.**

4. **IDENTIFICACIÓN Y AUTENTICACIÓN**

4.1 Existirá una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y se establecerán procedimientos de identificación y autenticación para dicho acceso.

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

4.3 Las contraseñas se cambiarán con la periodicidad que se determine en el documento de seguridad. **Dicha periodicidad no superará la anual.** Mientras estén vigentes se almacenarán de forma ininteligible.

4.4 Se establecerá un mecanismo que permita la identificación **de forma inequívoca y personalizada** de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

4.5 Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

4.6 Sin perjuicio de lo arriba indicado, el Proveedor implantará los siguientes procedimientos de identificación y autenticación (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

- ☒ Autorizaciones;
- ☒ Terminales con clave de acceso de usuario;
- ☒ **Distribución y almacenamiento de contraseñas**
- ☒ **Mecanismos de identificación de usuarios**
- ☒ Identificación del terminal y/o del usuario del equipo terminal frente al sistema del Proveedor;
- ☒ Desconexión automática de la identificación del usuario en supuestos de introducción reiterada de claves erróneas;
- ☒ Archivos de control de incidencias (control de los intentos de acceso no autorizado);
- ☒ Expedición y protección de los códigos de identificación;
- ☒ Asignación de terminales y/o usuarios de terminal individuales;
- ☒ Características de identificación exclusivas para funciones específicas;
- ☒ Autenticación del personal autorizado;
- ☒ Establecimiento de normas específicas de acceso para procedimientos, tarjetas de acceso, métodos de control del proceso, programas de catalogación de autorizaciones;
- ☒ Separación de los entornos de producción y de prueba para librerías y ficheros de datos;
- ☒ Permitir que la entrada a las instalaciones en las que se tratan datos (estancias, dependencias, equipos informáticos y demás equipamientos) pueda permanecer cerrada.

5. CONTROL DE ACCESO A LOS DATOS DE CARÁCTER PERSONAL

5.1 Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

5.2 Se establecerán mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

5.3 La relación de usuarios autorizados para acceder al sistema (véase apartado 4.1 de este Anexo) contendrá el acceso autorizado para cada uno de ellos.

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

5.5 Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

5.6 De cada acceso se guardarán, como mínimo:

(a) La identificación del usuario;

(b) la fecha y hora en que se realizó;

(c) el fichero accedido;

(d) el tipo de acceso; y

(e) si ha sido autorizado o denegado.

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

5.8 Los mecanismos que permiten el registro de los datos de identificación y acceso a los datos de carácter personal estarán bajo el control directo del responsable de seguridad competente (véase apartado 8 de este Anexo) sin que se deba permitir, en ningún caso, la desactivación de los mismos.

5.9 El período mínimo de conservación de los datos de control de acceso registrados será de dos (2) años.

5.10 El responsable de seguridad competente (véase apartado 8 de este Anexo) se encargará de revisar periódicamente la información de control de acceso registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

5.11 **Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que contengan datos de carácter personal que sean accesibles por múltiples usuarios.**

5.12 **La relación de usuarios autorizados para acceder a la documentación que contenga datos de carácter personal estará registrada**

5.13 Sin perjuicio de las medidas arriba indicadas, al objeto de controlar el acceso a los datos de carácter personal de acuerdo con este apartado 5, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

(a) Control de personas:

- ☒ Autorizaciones de acceso para los empleados y para terceras personas, incluidas su respectiva documentación;
- ☒ Tarjetas de acceso;
- ☒ Restricciones relativas a las claves;
- ☒ Normas para terceros;
- ☒ Normas sobre códigos de acceso;
- ☒ Identificación de las personas que dispongan de autorización de acceso;
- ☒ Sistema de alarma o cualesquiera otras medidas de seguridad apropiadas, inclusive fuera del horario laboral;
- ☒ Implementación de medidas de seguridad para los equipos descentralizados de tratamientos de datos y para ordenadores personales;
- ☒ Protección y restricción de las vías de acceso.

(b) Control de acceso a los datos:

- ☐ Bloqueo de los equipos terminales;
- ☒ Asignación de terminales individuales y/o de usuarios de terminal y características de identificación exclusivas, a funciones específicas;
- ☒ Restricciones funcionales y/o de tiempo de las terminares y/o de los usuarios de las terminares y de las características de identificación;
- ☒ Normas para la autorización de usuarios;
- ☒ Obligaciones de secreto respecto a la información;
- ☒ Códigos de usuario para programas informáticos y datos;
- ☐ Rutinas de codificación para archivos;
- ☐ Normas de acceso diferenciadas (ej.: bloqueo parcial);
- ☐ Normas para la organización de ficheros;
- ☐ Análisis del acceso y uso de los ficheros;
- ☐ Control especial de las aplicaciones de los programas ayuda en tanto en cuanto permitan eludir las medidas de seguridad;
- ☐ Guías para la organización de ficheros de datos;

☒ Conservación de los registros de uso de los ficheros de datos;

☒ Destrucción controlada de los soportes de datos;

☒ Desconexión automática de los códigos de identificación de usuarios cuando los mismos no hayan sido utilizados durante un periodo considerable de tiempo;

☐ Sistemas de verificación, ajuste y control;

☒ Utilización de medidas de encriptación para ficheros críticos;

☒ Procedimientos para la verificación y liberación de programas informáticos;

☒ **Control de acceso múltiple y registro de acceso a documentos**

(c) Control de la entrada de datos (capacidad de determinar y revisar retroactivamente el momento y lugar de la grabación de los datos del interesado en el sistema de tratamiento de datos del Proveedor).

☒ Obtención de pruebas de la autorización para la grabación de datos por el Proveedor;

☒ Registro electrónico de la grabación de datos;

☒ Registro electrónico de los tratamientos de datos, en particular, del uso de los datos;

☒ Medidas de protección para el registro de datos en memoria, así como para la lectura y borrado de la información almacenada;

☐ Instrucciones de uso de los formularios de registro/grabación de datos;

6. **GESTIÓN DE SOPORTES Y DOCUMENTACIÓN QUE CONTENGAN DATOS DE CARÁCTER PERSONAL**

6.1 Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

6.2 Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los soportes con datos de carácter personal.

6.3 **El archivo de la documentación que contenga datos de carácter personal se realizará con criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos AROC**

6.4 **El almacenamiento de la documentación que contenga datos de carácter personal se realizará utilizando mecanismos que obstaculicen su apertura.**

6.5 **Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe custodiarla para evitar accesos no autorizados.**

6.6 La salida de soportes y **documentos** que contengan datos de carácter personal, incluidos **los anejos a correos electrónicos,** fuera de los locales en los que está ubicado el fichero, únicamente podrá ser autorizada siguiendo las instrucciones del Cliente como responsable del fichero.

6.7 Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer:

(a) **Documento o tipo de soporte;**

(b) la fecha y hora;

(c) el emisor;

(d) el número de **documentos** o soportes;

(e) el tipo de información que contienen;

(f) la forma de envío; y

(g) la persona responsable de la recepción que deberá estar debidamente autorizada.

6.8 Igualmente, se dispondrá de un sistema de registro de salida de soportes informáticos que permita, directa o indirectamente, conocer:

(a) **Documento o tipo de soporte;**

(b) la fecha y hora;

(c) el destinatario;

(d) el número de **documentos** o soportes;

(e) el tipo de información que contienen;

(f) la forma de envío;

(g) y la persona responsable de la entrega que deberá estar debidamente autorizada.

6.9 Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

6.10 Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

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

6.12 **El uso de dispositivos portátiles que contengan datos de carácter personal fuera de las instalaciones, debe ser autorizado y se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.**

6.13 La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

6.14 **El traslado de documentación que contenga datos de carácter personal se realizará utilizando medidas de seguridad que impidan el acceso o manipulación no autorizada**

6.15 **El almacenamiento de la documentación que contenga datos de carácter personal se realizará en un lugar con acceso restringido o utilizando contenedores que garanticen que dicha información no es accedida por personal no autorizado.**

6.16 **La generación de copias o reproducción de documentos será realizada bajo el control del personal autorizado en el documento de seguridad, destruyendo las copias desechadas.**

6.17 Con el fin de llevar a cabo la gestión de los soportes que contentan datos de carácter personal de conformidad con este apartado 6, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

- ☒ Autenticación;
- ☐ Requisitos internos de verificación (principio de los "cuatro ojos");
- ☒ Designación de las áreas en las que pueden/deben almacenarse **los documentos y/o soportes** de datos;
- ☒ **Control de la eliminación de documentación y soportes de datos;**
- ☒ **Control de las copias de documentación;**
- ☒ Designación de las personas que, en cada área, estará autorizada para eliminar los soportes de datos;
- ☒ Control de los ficheros;
- ☒ Bloqueo de los soportes que contengan datos confidenciales;
- ☐ Armarios de seguridad (security lockers);
- ☐ Prohibición de utilizar bolsos o similares en las áreas de seguridad;
- ☒ Control de la destrucción de los soportes de datos;
- ☒ **Control de dispositivos móviles fuera de las instalaciones;**

☒ Documentación de los procedimientos de transferencia;

☒ Documentación de los procedimientos de recuperación y transmisión;

☒ Documentación de las ubicaciones / destinos remotos a los que se pretende transmitir los datos así como las vías de esa transmisión (logical path);

☒ Política de autorización;

☒ Encriptación de los datos en caso de transmisiones por redes de telecomunicaciones o de transporte por medio de aparatos de almacenamiento de datos (disquetes y cartuchos).

☒ Monitorización de la correcta y completa transmisión de datos (verificación punto a punto);

☒ Encriptación;

☒ Servicios de transporte, recogida personal, consecución del transporte;

☐ Control de la verosimilitud de los datos;

☒ Control de la correcta y completa transmisión;

☒ Supresión de cualquier dato remanente antes de la sustitución de los soportes de datos.

7. **COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS**

7.1 **Se verificarán al menos semestralmente,** la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

7.2 Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

7.3 **En caso de pérdida o destrucción de ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar su reconstrucción total, se procederá a grabar manualmente los datos dejando constancia del motivo en el documento de seguridad**

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

7.5 Con el fin de llevar a cabo la gestión de la producción de copias de respaldo y de recuperación de datos de conformidad con este apartado 7, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

☒ Políticas de control de la producción de copias de respaldo y de recuperación de datos;

☒ **Autorizaciones para recuperación de datos**

8. **NOMBRAMIENTO DE RESPONSABLE DE SEGURIDAD**

8.1 Deberá designarse a uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad.

9. **AUDITORÍA**

9.1 Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del Reglamento de Medidas de Seguridad, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años **y ante cualquier modificación sustancial en los sistemas de información que pueda tener repercusiones en la seguridad.**

9.2 El informe de auditoría deberá:

(a) Dictaminar sobre la adecuación de las medidas y controles al Reglamento de Medidas de Seguridad;

(b) identificar sus deficiencias;

(c) proponer las medidas correctoras o complementarias necesarias; e

(d) incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

9.3 Los informes de auditoría serán analizados por el responsable de seguridad competente (véase apartado 8 de este Anexo), que elevará las conclusiones al Proveedor (como encargado del tratamiento) y al Cliente (como responsable del fichero) para que se adopten las medidas correctoras adecuadas.

9.4 Los informes de auditoría quedarán a disposición de la Agencia Española de Protección de Datos.

9.5 Con el fin de llevar a cabo las auditorías de conformidad con este apartado 9, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

☒ **Control de la Implementación de medidas correctivas de auditorías anteriores**

10. **PRUEBAS CON DATOS REALES**

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se realice previamente una copia de seguridad y se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

10.1 Con el fin de llevar a cabo las auditorías de conformidad con este apartado 10, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

☒ **Control de pruebas con datos reales**

11. **FICHEROS TEMPORALES Y COPIAS DE DOCUMENTOS**

11.1 **Los ficheros temporales o copias de documentos que se hubiesen creado sólo para la realización de trabajos temporales o auxiliares deben cumplir el nivel de seguridad que les corresponda.**

11.2 **Todo fichero temporal o copia de documento se borrará o destruirá una vez deje de ser necesario para los fines que motivaron su creación.**

11.3 Con el fin de llevar a cabo las auditorías de conformidad con este apartado 11, el Proveedor implantará las siguientes medidas de seguridad específicas (las medidas aplicables figuran marcadas mediante una cruz en su correspondiente casilla):

☒ **Eliminación de ficheros temporales**