DOCUMENTO DE SEGURIDAD

Responsable del Fichero : **Associación Matissos**

Nombre del Fichero: **Associación Matissos**

Fecha: ***18/01/2021***

INDICE

1. Objeto del documento

El documento de seguridad está redactado cumpliendo lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 1720/2007, de 21 de diciembre), en el que se recogen las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica de Protección de Datos (Ley Orgánica 15/1999, de 13 de diciembre).

El fichero de datos de carácter personal de la **Asociación Matissos** está clasificado como de nivel **bajo**

Este documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

2. Ámbito de aplicación

El responsable del fichero **Asociación Matissos** ha elaborado este documento comprometiéndose a implantarlo y actualizarlo.

Especificar la estructura de los ficheros con datos de carácter personal y la descripción de los sistemas de información que los tratan es una medida de seguridad de nivel básico. Se trata de una medida de índole técnica y organizativa necesaria para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

El fichero **socios** contiene datos de carácter personal de nivel **bajo**. Por tanto, se tomarán las medidas de seguridad correspondientes a este nivel.

Este fichero de socios únicamente estará compuesto de los datos personales y los datos bancarios de los socios de la Asociación Matissos

3. Recursos protegidos

Los recursos que quedan protegidos son:

Los centros de tratamiento y locales donde se encuentren ubicados los ficheros o se almacenen los soportes que los contengan.

Los puestos de trabajo, bien locales o remotos, desde los que se pueda tener acceso al fichero.

Los servidores y el entorno de sistema operativo y de comunicaciones en el que se encuentra ubicado el fichero.

Los sistemas informáticos, o aplicaciones establecidos para acceder a los datos.

El período mínimo de conservación de los datos registrados será de **5 años**.

4. Funciones y obligaciones del personal

Las personas con acceso a los datos de carácter personal y a los sistemas de información deben tener sus funciones y obligaciones claramente definidas.

El responsable del fichero adoptará 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 personal que tenga acceso a los datos del fichero debe conocer y respetar las medidas que afectan a las funciones que tiene encomendadas.

Si existiese alguna incidencia, el personal debe notificarla al responsable del fichero o al responsable de seguridad.
Las personas empleadas que colaboren deben guardar secreto con respecto a los datos del fichero de los que tengan conocimiento en el desarrollo de sus funciones.

5. Normas y procedimientos de seguridad

Régimen de trabajo fuera de los locales de la ubicación del fichero. La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por **el presidente** y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado (nivel **bajo**).

Ficheros temporales.

Los ficheros temporales deberán cumplir el nivel de seguridad **bajo**.

Todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

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 asegure el nivel de seguridad correspondiente al tipo de fichero tratado (**bajo**).

Identificación y autenticación.

El responsable del fichero debe encargarse de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de que se establezcan procedimientos de identificación y autenticación para dicho acceso.

Las contraseñas han de cambiarse cada **seis meses**.

Mientras estén vigentes, se almacenarán de forma ininteligible.

El responsable del fichero 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.

Identificación del responsable de seguridad. El responsable del fichero es a su vez el responsable de seguridad dado que el nivel de seguridad básico del fichero nos permite no tener este.

Control de accesos.

El personal sólo puede acceder a los datos que sean necesarios para el desarrollo de sus funciones:

Únicamente E**l presidente** estará autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos.

Únicamente **el presidente** estará autorizado para llevar a cabo el procedimiento de alta, modificación y baja de las autorizaciones de acceso.

Control de accesos físico.

Tanto los datos físicos, como los dos ordenadores portátiles se encuentran en la sede de la Asociación C/ Vilaseca 1D 08031 de Barcelona
Los datos guardados en papel se encuentran en un armario cerrado con llave únicamente **el presidente *y el Tesorero*** estarán autorizados para ***acceder mediante una llave al armario*** de los locales en los que se encuentren el libro de socios y que corresponden ***al fichero físico de socios de la Asociación Matissos***

Eduardo Ortega será el único responsable de dar el alta de socio en el libro de socios y en el fichero físico de socios de la Asociación Matissos.

Las personas que tengan acceso a los ordenadores de la Asociación deberán acceder con una contraseña que les proporcionara el presidente dicha contraseña deberá cambiarse cada 6 meses

Telecomunicaciones (transmisión telemática de datos).

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

Registro de accesos

Cada acceso a los datos del fichero **Asociación Matissos** ha de quedar registrado, dando constancia del nombre del usuario, la fecha, la hora, el nombre del fichero, el tipo de acceso y si hay autorización o no.

Los datos anotados en el registro de accesos serán conservados por un período de tiempo de dos años.

La información registrada debe ser revisada de manera periódica. Esta función será desempeñada por el responsable de seguridad y la hará constar en un informe.

Procedimiento de notificación, gestión y respuesta ante las incidencias.

El responsable del fichero Eduardo Ortega será el encargado de registrar las incidencias según anexo

El procedimiento de notificación y gestión de incidencias debe contener:

• El tipo de incidencia.

• El momento en que se ha producido.

• La persona que realiza la notificación.

• A quién se le comunica.

• Los efectos que se hubieran derivado de la misma. El sistema informático utilizado en caso de tratarse de gestión automatizada.

Registro de incidencias.

En los procedimientos ejecutados para la recuperación de los datos habrá que indicar la persona que ejecutó el proceso, los datos que han sido restaurados y, en su caso, los datos que han tenido que ser grabados manualmente.

Para ello será necesaria la autorización del responsable del fichero.

Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El responsable del fichero debe verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

Estos procedimientos deben garantizar la reconstrucción en el estado en que se encontraban los datos al tiempo de producirse la pérdida o destrucción.

Las copias han de llevarse a cabo como mínimo una vez por semana, salvo que no se hubiera producido ningún cambio durante ese período.

Copias de respaldo y recuperación.

La copia de respaldo y de los procedimientos de recuperación de los datos se conservarán ***en un disco duro de la Asociación Matissos***

Revisión del documento de seguridad.

El documento ha de mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización.

Deberá, además, estar adecuado a las disposiciones legales vigentes en cada momento en materia de seguridad de los datos.

Auditorías.

Se someterán a una auditoría interna los sistemas de información e instalaciones de tratamiento de datos para verificar el cumplimiento del Reglamento de Medidas de Seguridad, de los procedimientos y de las instrucciones vigentes en materia de seguridad de datos.

Se hará una auditoría, al menos, cada dos años.

Tras la auditoría, se redactará un informe para dictaminar sobre la adecuación de las medidas y controles, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Deberá también incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Estos informes serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas, y quedarán a disposición de la Agencia de Protección de Datos.

ANEXOS

ANEXO I

DESCRIPCIÓN DE FICHEROS

Actualizado a: *17 de Enero de 2021*

FICHERO 1:

Descripción: *Datos personales de los socios*

- Nivel de medidas de seguridad a adoptar: *básico*.
- Estructura del fichero: *Nombre y apellidos, D.N.I. y datos bancarios*
- Encargados de tratamiento autorizados a tratar los datos: el presidente, el tesorero

Información sobre el fichero o tratamiento.

Finalidad y usos previstos. Gestión socios de la entidad.
Personas o colectivos: *Personas*
Procedimiento de recogida: Alta socio primero en ficha física y posteriormente, los autorizados, pasan los datos al ordenador
Sistema de tratamiento: *mixto*.
Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: matissos8@gmail.

ANEXO II

DESCRIPCION DEL SISTEMA INFORMATICO, LOCALES, UBICACIÓN y FISICA

1. Entorno de Sistema Operativo y de Comunicaciones del Fichero

Dos ordenadores portátiles

2. Locales y equipamiento de los centros de tratamiento

Local C/ Vilaseca 1 D 08031 Barcelona

Locales

Descripción de la ubicación física: Despacho
Tipo de acceso: Llave

Ubicación física habitual

Lugar donde se almacenan los soportes del fichero habitualmente: Armario con llave
Tipo de contenedor de los soportes: archivadores dentro del armario.

Mecanismos de seguridad de los contenedores: cerraduras de llave.

ANEXO III

PERSONAL AUTORIZADO PARA ACCEDER FICHEROS

RESPONSABLE DEL FICHERO

Nombre y apellidos	Cargo	Alta	Baja
Eduardo Ortega			

RESPONSABLE DE SEGURIDAD

Nombre y apellidos	Cargo	Alta	Baja

ADMINISTRADORES DEL SISTEMA

Nombre y apellidos	Organismo / Unidad Administrativa	Alta	Baja

USUARIOS DEL FICHERO

Nombre y apellidos	Puesto de trabajo	Ficheros a los que tiene acceso	Fecha de Alta	Fecha de Baja
	Secretario	Ficheros mixtos		
	Tesorero	Ficheros mixtos		
	Responsable facturación	Ficheros mixtos		

ANEXO IV
REGISTRO DE INCIDENCIAS

Modelo de notificación de incidencias:

Incidencia Nº: |_____| (Este número será rellenado por el Responsable de seguridad)	
Fecha de notificación: /__/__/____/	
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)	
Medidas correctoras aplicadas:	
Persona que realiza la comunicación: Fdo.:_____	