POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

OBJETIVO: Establecer los criterios para la recolección, almacenamiento, uso, circulación y supresión de los datos personales tratados por **ACPEIM**

Garantizar la protección de los datos personales recolectados, almacenados, usados y tratados por ACPEIM, en cumplimiento de la legislación vigente en Colombia sobre habeas data, asegurando los derechos de los titulares.

ALCANCE: Esta política aplica a todos los datos personales tratados por ACPEIM en el desarrollo de sus actividades con pacientes, familiares, voluntarios, trabajadores, aliados, proveedores, donantes y demás personas naturales con quienes tenga relación.

OBLIGACIONES: Esta política es de obligatorio y estricto cumplimiento para ACPEIM.

RESPONSABLE DEL TRATAMIENTO: **ACPEIM**, sociedad solidaria legalmente constituida, identificada con el NIT 9 0 0 2 7 8 3 3 7-5, con domicilio principal en la CL 11 C 73 82 T 2 601, de la ciudad de Bogotá, República de Colombia. Teléfono 3223082547

TRATAMIENTO Y FINALIDAD: ACPEIM realiza el tratamiento de datos personales con las siguientes finalidades:

- Contactar pacientes y familiares para brindar acompañamiento, asesoría y seguimiento.
- Informar sobre eventos, actividades educativas, campañas de salud y servicios de la asociación.
- Gestionar programas de donación, voluntariado y cooperación.
- Administrar información de empleados, contratistas y proveedores.
- Cumplir obligaciones legales, contractuales y de reporte a entidades públicas.

RESPECTO A LOS TRABAJADORES:
Para cumplir con las normas que rigen la relación laboral, contractual y comercial: para gestionar la vinculación laboral de las personas en la asociación, para afiliaciones a la seguridad social, gestionar programas de bienestar laboral del trabajador y sus familias, gestión de la seguridad y salud en el trabajo; procesos de formación, liquidación de contratos, envió de publicidad, invitaciones a eventos, control y registro de beneficiarios y benefactores, manejo y presentación de indicadores de gestión, desarrollo de programas asociados a nuestro objeto social, registro de nuestros asociados, sus aportes y sus intereses.
Dar cumplimiento a las obligaciones contraídas por **ACPEIM** con el Titular de la Información, con relación al pago de salarios, prestaciones sociales y demás retribuciones consagradas en el contrato de trabajo o según lo disponga la ley, además de las obligaciones contraídas con los asociados, beneficiarios y benefactores

Ofrecer programas de bienestar asociativa y planificar actividades de la asociación, para el titular y sus beneficiarios (hijos, cónyuge, compañero permanente).

RESPECTO A LOS PROVEEDORES:
Para verificar el cumplimiento de las políticas de la entidad en materia de selección y contratación de proveedores, verificar el adecuado cumplimiento de las obligaciones, suministrar u obtener referencias comerciales y/o financieras; manejo y registro contable de las operaciones que se desarrollen durante la vigencia de cualquier relación jurídica, así como todas aquellas que se realicen para la terminación, cierre o liquidación de la misma, adoptar medidas tendientes a la prevención de actividades ilícitas.

RESPECTO A LOS CLIENTES:
Para enviar ofertas, proveer información sobre productos, precios y servicios, realizar eventos o promociones de tipo comercial e informativo; llevar a cabo programas de fidelización y actualización de datos, enviar estados de cuenta de cartera; evaluar la calidad de los productos y/o servicios; realizar actividades de cobranza, recaudo, consultas, verificaciones, control y habilitación de medios de pago; validar mi identidad, adoptar medidas tendientes a la prevención de actividades ilícitas. y demás actividades que faciliten la compraventa de bienes y/o servicios.
Una vez finalice el respectivo contrato, el encargado del tratamiento debe suprimir o devolver al titular el dato.

TRATAMIENTO DE DATOS SENSIBLES: Datos sensibles son aquellos que afectan la intimidad del titular o pueden dar lugar a que lo discriminen, es decir, aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, entre otros.

Los datos sensibles recolectados serán tratados con las siguientes finalidades:

Prestar el servicio de teleasistencia domiciliaria.

Contactar al Titular a través de medios telefónicos para realizar encuestas, estudios y/o confirmación de datos personales necesarios para la ejecución de una relación contractual.

Contactar al Titular a través de medios electrónicos – SMS o chat para el envío de noticias relacionadas con campañas de fidelización o mejora de servicio.

Transferir datos personales fuera del país a la compañía matriz de **ACPEIM** para cumplir con las regulaciones anti lavado de activos que le aplican.

Transmitir los datos personales fuera del país a terceros con los cuales **ACPEIM** haya suscrito un contrato de procesamiento de datos y sea necesario entregársela para el cumplimiento del objeto contractual.

Prestar los servicios ofrecidos por **ACPEIM** y aceptados en el contrato suscrito.

Suministrar la información a terceros con los cuales **ACPEIM** tenga relación contractual y que sea necesario entregársela para el cumplimiento del objeto contratado.

DERECHOS DE LOS TITULARES: Como titular de sus datos personales Usted tiene derecho a:

(i) Acceder de forma gratuita a los datos proporcionados que hayan sido objeto de tratamiento.
(ii) Conocer, actualizar y rectificar su información frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté prohibido o no haya sido autorizado.
(iii) Solicitar prueba de la autorización otorgada.
(iv) Presentar ante la Superintendencia de Industria y Comercio (SIC) quejas por infracciones a lo dispuesto en la normatividad vigente.
(v) Revocar la autorización y/o solicitar la supresión del dato, siempre que no exista un deber legal o contractual que impida eliminarlos.
(vi) Abstenerse de responder las preguntas sobre datos sensibles. Tendrá carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS El área de Atención al es la dependencia que tiene a cargo dar trámite a las solicitudes de los titulares para hacer efectivos sus derechos, a través de la línea telefónica 318510740 y la el correo electrónico ACPEIM@GMAIL.COM

PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA En cumplimiento de las normas sobre protección de datos personales, ACPEIM presenta el procedimiento y requisitos mínimos para el ejercicio de sus derechos: Para la radicación y atención de su solicitud le solicitamos suministrar la siguiente información:

Nombre completo y apellidos Datos de contacto (Dirección física y/o electrónica y teléfonos de contacto), Medios para recibir respuesta a su solicitud, Motivo(s)/hecho(s) que dan lugar al reclamo con una breve descripción del derecho que desea ejercer (conocer, actualizar, rectificar, solicitar prueba de la autorización otorgada, revocarla, suprimir, acceder a la información) Firma (si aplica) y número de identificación. El término

máximo previsto por la ley para resolver su reclamación es de quince (15) días hábiles, contado a partir del día siguiente a la fecha de su recibo.

Cuando no fuere posible atender el reclamo dentro de dicho término, ACPEIM informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término. Una vez cumplidos los términos señalados por la Ley 1581 de 2012 y las demás normas que la reglamenten o complementen, el Titular al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, actualización, rectificación, supresión y revocación, podrá poner su caso en conocimiento de la Superintendencia de Industria y Comercio –Delegatura para la Protección de Datos Personales-.

1. **Medidas de seguridad**

ACPEIM tiene implantadas en sus sistemas de información las medidas de seguridad necesarias para proteger los datos personales y garantizar la confidencialidad, integridad, disponibilidad y resiliencias de los servicios y sistemas de información.

Tratamientos automatizados

- **Ordenadores y dispositivos**

- **Actualización**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- **Antivirus**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
- **Firewall**: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

- **Control de acceso físico y lógico**

El acceso a datos personales queda absolutamente restringido a las personas debidamente autorizadas.

- **Control de accesos**: La autorización de los usuarios para acceder a los locales donde se encuentren ubicados los sistemas de información, así como a los propios sistemas, equipos, aplicaciones y, en general, a datos personales, dependerá de las funciones que desarrollen en cada momento. Los usuarios solo tendrán acceso a aquellos datos estrictamente necesarios para el desarrollo de las funciones que la Sociedad les haya encomendado.

- **Identificación y autenticación**: Un objetivo prioritario para la normativa aplicable en materia de protección de datos es evitar cualquier tipo de uso indebido o no autorizado a datos personales. Por ello, se deben implantar una serie de procedimientos de identificación y autenticación que permitan obtener y verificar puntualmente la identidad del usuario de forma inequívoca.
    - Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
    - Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
    - Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
    - Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
    - Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.
    - Previamente a la asignación de nombres de usuario y contraseña, se definirán las pantallas, módulos y procesos a los que tendrán acceso autorizado cada uno de los usuarios que prestan servicios para la Sociedad.
    - Todas las aplicaciones estándar bajo Sistema Operativo, hojas de cálculo, bases de datos, documentos de texto, etc. que contengan datos personales, se configurarán de tal modo que al ejecutarse alguna de ellas se deba introducir una contraseña. Se exceptuará esta obligación en caso de existencia de aplicativos de gestión de identidades.
    - Igualmente, las aplicaciones a medida o de terceros también deberán configurarse de modo que los usuarios deban introducir una contraseña.
    - Se limitará el número de intentos de acceso tanto al Sistema Operativo como a las aplicaciones a medida o de terceros, de forma que tras tres intentos fallidos, se inhabilitaría el acceso del usuario de forma permanente, hasta que el administrador vuelva a permitir el acceso.
    - Las contraseñas deben cambiarse periódicamente, preferiblemente cada 2 ó 3 meses.

  - Las contraseñas deben almacenarse de forma cifrada, de forma que únicamente los usuarios conozcan sus propias contraseñas.
- **Registro de accesos**: se llevarán a cabo registros de accesos, especialmente si se trata de **datos sensibles**. Estos accesos pueden ser controlados a través de una aplicación de gestión de identidades. En los casos en que acceda más de un usuario a los datos personales, se guardará un registro de cada acceso en el que conste la identificación del usuario, la fecha y hora del acceso, los datos a los que accede, el tipo de acceso y si fue autorizado o denegado. Si el acceso se autoriza, se guardará además la información que permita identificar el registro accedido y, si es posible, qué acción ha realizado, durante, al menos, dos años. El **Responsable de Seguridad Técnico** revisará periódicamente la información registrada.

- **Gestión de soportes**

Todos los soportes que contengan datos personales deben estar identificados, etiquetados, inventariados y almacenados en un lugar con acceso restringido.

- **Control de entrada y salida de soportes**: ACPEIM cada Actividad de Tratamiento, deberá autorizar la entrada y salida de soportes con datos personales fuera de los locales en los que están ubicados, y llevar un Registro en el que conste el tipo y cantidad de soportes que entran o salen; la referencia genérica del tipo de datos contenidos; la fecha y hora de salida o entrada; la forma de envío o recepción; y la identificación detallada de los datos del receptor, o en su caso emisor.
- **Reutilización y destrucción de soportes**: cuando un soporte con datos personales vaya a ser reutilizado o destruido, previamente deberá ser borrada toda la información que contiene mediante un sistema que no permita su aprovechamiento posterior. En primer caso, se procederá al borrado lógico de la información de los soportes, de tal forma que no se permita el recuperado de la información. En el segundo caso, se procederá además a la destrucción completa del soporte.
- **Distribución de soportes**: en caso de producirse una salida de soportes con datos personales fuera de los sistemas de información de la Sociedad, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información, especialmente si se trata de **datos sensibles**.

- **Brechas de seguridad**

ACPEIM notificará al responsable del tratamiento, en la mayor brevedad posible, las violaciones de seguridad de los datos a su cargo, de forma que el responsable del tratamiento tenga tiempo suficiente para informar, en su caso, a la AEPD o a los interesados.

- **Copias de seguridad**

La posibilidad de que en una incidencia puedan perderse datos personales que constan en los sistemas informáticos de ACMEIM, obliga a que se conserven copias de seguridad de todos los archivos, programas, etc. que contengan datos personales.
Todo programa, aplicación o base de datos utilizado para el tratamiento de datos personales deberá proveer la función de realización de copias de seguridad, o bien, permitir la realización de copias de seguridad de tal forma que se garantice la recuperación de datos.
Periódicamente, como mínimo una vez a la semana, se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador o servidor con los archivos, programas, etc. originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.
Antes de proceder al almacenamiento de la copia de seguridad se verificará que ésta se ha realizado correctamente y sin ninguna incidencia.

- Deber de confidencialidad sobre el modo o sistema de realización de las mencionadas copias, salvo a las personas autorizadas.
- Prohibición de entregar las copias de seguridad a persona distinta de aquellas que hayan sido debidamente autorizadas.
- Prohibición de manipular, alterar o deteriorar los soportes (cintas, disquetes, etc.) en los que se realizan las copias de seguridad.

Tratamientos no automatizados

- **Control de acceso físico**

El acceso a los locales donde se encuentren ubicados los soportes no automatizados con datos personales y el acceso a los propios datos personales queda absolutamente restringido a las personas debidamente autorizadas.
La presencia de terceros en los citados locales sólo podrá tener lugar cuando se encuentren acompañados de un usuario autorizado, bajo la completa responsabilidad de éste y con la autorización expresa del **ACPEIM** En ningún caso la presencia de terceros podrá suponer que estos accedan a los sistemas de información o a datos personales.
Por ello, únicamente las personas autorizadas, dependiendo de las funciones que desarrollen en cada momento, podrán tener acceso a la información en soporte papel. Los usuarios solo tendrán acceso a aquellos datos estrictamente necesarios para el desarrollo de las funciones que la Sociedad les haya encomendado.
En caso de acceder a **datos sensibles**, se deberá identificar al usuario con acceso a este tipo de tratamiento, la Actividad de Tratamiento correspondiente, la fecha y hora del acceso, y la documentación o datos a los que tiene acceso. El acceso realizado a esta documentación por personas no autorizadas también deberá anotarse en este Registro.

- **Gestión de incidencias**

Las incidencias de seguridad a datos personales en soportes no automatizados serán notificadas, registradas y gestionadas para asegurar que se toman las medidas adecuadas para su resolución. Todo aquello acontecido que se considere una incidencia debe quedar debidamente reflejado en un Registro habilitado al efecto.
Este procedimiento de incidencias deberá ser conocido por todos los empleados y colaboradores de **ACPEIM**, que, por sus funciones en la misma, traten datos personales. Dicho plan consta de tres fases:

- **Notificación**: Cualquier persona que preste servicios para **ACPEIM** y detecte alguna anomalía en los datos personales contenidos en soportes no automatizados, deberá ponerlo en conocimiento inmediato. De esta forma tratará de evitarse que la posible incidencia repercuta negativamente en la seguridad con la que son tratados y mantenidos los datos personales. Esta comunicación con el **Responsable Funcional** correspondiente debe realizarse a través del medio más rápido y fiable posible para que se mantenga la seguridad y confidencialidad de los datos personales. La persona que se ponga en contacto con el **ACPEIM** correspondiente a fin de notificarle la incidencia debe facilitarle la información necesaria para que se proceda a su registro y control, así como para poner en marcha, si fuera posible, un plan de respuesta para interrumpir y eliminar la incidencia.
- **Gestión**: **ACPEIM** comunicará la incidencia a su personal, se asegurará que, con la mayor brevedad posible, se dé una respuesta a las incidencias detectadas y supervisará personalmente la subsanación de la anomalía. **ACPEIM** comunicará al Delegado de Protección de Datos (DPO) las incidencias que puedan afectar a los derechos y libertades de los individuos. Finalizada la incidencia, **ACPEIM** correspondiente adoptará las medidas necesarias para que no vuelva a producirse una situación similar en la que pueda peligrar la integridad de los datos personales en soporte no automatizado.

- **Brechas de seguridad**

ACPEIM notificará al responsable del tratamiento, en la mayor brevedad posible, las violaciones de seguridad de los datos a su cargo, de forma que el responsable del tratamiento tenga tiempo suficiente para informar, en su caso, a la AEPD o a los interesados.

- **Gestión de soportes**

Los soportes extraíbles y los documentos en papel serán identificados, etiquetados, inventariados y almacenados en armarios u otro tipo de mobiliario con sistemas de cierre, de forma que se obstaculice su apertura.
En caso de que esto no sea posible, deben adoptarse las medidas necesarias para impedir el acceso a la documentación en papel por personas no autorizadas.

Mientras la documentación con datos personales no se encuentre archivada en los dispositivos de almacenamiento establecido en el punto anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.
La documentación que contenga **datos sensibles** se almacenará en locales con sistemas de cierre y permanecerán cerrados cuando no sea preciso el acceso a esta documentación.
Siempre que se proceda al traslado físico de la documentación con **datos sensibles**, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

- **Copias o reproducción de documentos con datos sensibles**

Las copias o reproducciones de documentos con datos sensibles deberán ser controlada y debidamente autorizada.
Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

VIGENCIA: La presente Política para el Tratamiento de Datos Personales rige desde el 2025 Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en esta política. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar la información, los datos serán eliminados de nuestras bases de datos.

Los datos personales proporcionados se conservarán mientras se mantenga la relación contractual con el Titular de la información.

Los datos personales proporcionados se conservarán mientras no se solicite su supresión por el interesado y siempre que no exista un deber legal de conservarlos.

Los datos personales proporcionados se conservarán durante un plazo de 4 años a partir de la última confirmación de interés de parte del Titular.