

POLÍTICA DE TRATAMIENTO DE DATOS

Francisco Murillo S.A.S.



Número único: (57) (4) 604 22 92
Aguacatala: Cra. 50C No. 10 Sur 161
Centro: Cra. 52 No. 53 55
Medellín – Colombia.



Contenido:

Base legal y ámbito de aplicación.....	3
Definiciones	3
Autorización de la política de tratamiento.	4
Responsable del tratamiento	4
Tratamiento y finalidades de las bases de datos.	5
Derechos de los Titulares.	5
Atención a los Titulares de datos.	6
Procedimientos para ejercer los derechos del Titular.	6
Derecho de acceso o consulta.	6
Derechos de quejas y reclamos.....	7
Medidas de seguridad.....	8
Transferencia de datos a terceros países.....	8
Vigencia.....	9
ANEXO 1.	10
INFORMACIÓN DE BASES DE DATOS.	10
ANEXO 2.	17
MEDIDAS DE SEGURIDAD PARA CUMPLIR CON EL PRINCIPIO DE SEGURIDAD. 17	
Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas).	17
Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos.....	17
Medidas de seguridad para datos privados para Bases de Datos Automatizadas y No Automatizadas.	18
Medidas de seguridad para datos privados para Bases de Datos Automatizadas.	19
Medidas de seguridad para datos sensibles para Bases de Datos automatizadas y no automatizadas.....	19



Base legal y ámbito de aplicación.

La política de tratamiento de la Información se desarrolla en cumplimiento de los artículos 15 y 20 de la Constitución Política; de los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2.012, por la cual se dictan disposiciones generales para la Protección de Datos Personales y del artículo 13 del Decreto 1377 de 2.013, por el cual se reglamenta parcialmente la Ley anterior.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

Definiciones

Establecidas en el artículo 3 de la Ley Estatutaria 1581 de 2012 y el artículo 3 del Decreto 1377 de 2013.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos sensibles:** Se entiende por datos sensible aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.
- **Transferencia:** La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Autorización de la política de tratamiento.

De acuerdo al artículo 9 de la Ley Estatutaria de Protección de Datos Personales, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de FRANCISCO MURILLO S.A.S en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

Responsable del tratamiento

El responsable del tratamiento de las bases de datos objeto de esta política es FRANCISCO MURILLO S.A.S., cuyos datos de contacto son los siguientes:

Dirección: CRA. 50 C Nro. 10 Sur 161. Medellín, Antioquia – Colombia.
Correo electrónico: protecciondatos@franciscomurillo.com.co
Teléfono: (57) (4) 6042292. Ext. 28

Tratamiento y finalidades de las bases de datos.

FRANCISCO MURILLO S.A.S., en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

En el documento “Anexo 1. Información de Bases de datos” se presenta las distintas bases de datos que manejan la empresa, la información y características de cada una de ellas.

Derechos de los Titulares.

De acuerdo con el artículo 8 de la Ley Estatutaria de Protección de Datos Personales y a los artículos 21 y 22 del Decreto 1377 de 2.013, los Titulares de los datos pueden ejercer una serie de derechos en relación al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas:

- Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus datos personales.
- **Derechos de quejas y reclamos.** La Ley distingue cuatro tipos de reclamos:
 - **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
 - **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
 - **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
 - **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.
- **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** salvo cuando expresamente se exceptúe como requisito para el

tratamiento de conformidad con lo previsto en el artículo 10 de la Ley Estatutaria de Protección de Datos Personales.

- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

Atención a los Titulares de datos.

El encargado de la atención a las consultas, peticiones y reclamos FRANCISCO MURILLO S.A.S. será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos., de acuerdo con el documento "Anexo 3. Roles y Responsabilidades".

Correo electrónico: protecciondatos@franciscomurillo.com.co

Teléfono: (57) (4) 6042292. Ext. 28

Procedimientos para ejercer los derechos del Titular.

Derecho de acceso o consulta.

Según el artículo 21 del Decreto 1377 de 2.013, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a FRANCISCO MURILLO S.A.S. enviado, mediante correo electrónico a: protecciondatos@franciscomurillo.com.co, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a Cra. 50 C Nro. 10 Sur 162. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.

- Telecopia.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por FRANCISCO MURILLO S.A.S.

Una vez recibida la solicitud FRANCISCO MURILLO S.A.S. resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la Ley Estatutaria de Protección de Datos Personales.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

Derechos de quejas y reclamos.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a FRANCISCO MURILLO S.A.S. Enviado, mediante correo electrónico protecciondatos@franciscomurillo.com.co indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a CRA. 50 C Nro. 10 Sur 161. Medellín, Antioquia – Colombia. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

FRANCISCO MURILLO S.A.S. resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se 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.

Número único: (57) (4) 604 22 92
Aguacatala: Cra. 50C No. 10 Sur 161
Centro: Cra. 52 No. 53 55
Medellín – Colombia.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

Medidas de seguridad.

FRANCISCO MURILLO S.A.S., con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley Estatutaria de Protección de Datos Personales, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, FRANCISCO MURILLO S.A.S., mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

En el **Anexo 2**, se exponen las medidas de seguridad implantadas por FRANCISCO MURILLO S.A.S., con el fin de cumplir con el principio de seguridad.

Transferencia de datos a terceros países.

De acuerdo con el Título VIII de la Ley Estatutaria de Protección de Datos Personales, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- “Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.”

"En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales."

Vigencia.

"Las bases de datos responsabilidad de FRANCISCO MURILLO S.A.S., serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. FRANCISCO MURILLO S.A.S., procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, dicha base de datos ha sido creada sin un periodo de vigencia definido.

La presente política de tratamiento permanece vigente desde 14 de octubre de 2016"



Número único: (57) (4) 604 22 92
Aguacatala: Cra. 50C No. 10 Sur 161
Centro: Cra. 52 No. 53 55
Medellín – Colombia.



ANEXO 1.

INFORMACIÓN DE BASES DE DATOS.

RESPONSABLE DEL TRATAMIENTO.

Nombre: FRANCISCO MURILLO S.A.S.
NIT: 890.941.794-6
Dirección: CRA. 50 C Nro. 10 Sur 161, Medellín, Antioquia – Colombia.
Teléfono: (57) (4) 604 22 92.

ENCARGADO DE CONSULTAS Y RECLAMOS.

Correo electrónico: protecciondatos@franciscomurillo.com.co
Cargo: Jefe de Sistemas

BASE DE DATOS: CLIENTES.

Finalidades.

Gestión administrativa, Gestión de cobros y pagos, Gestión de facturación, Gestión económica y contable, Gestión fiscal, Históricos de relaciones comerciales, Prospección comercial, Gestión de clientes.

Información contenida.

Razón social, cámara de comercio, Rut, Nit, Documentos de identificación, teléfonos, direcciones, contratos, correo electrónico.

Tipo de dato.

Privado.

Sistema de tratamiento.

Automatizada.

Cantidad de Titulares.

205.617

Origen y procedencia de los datos.

Recogidos por el responsable.

Encargados del Tratamiento.

FRANCISCO MURILLO S.A.S.

Responsables de Seguridad.

Jefe de Sistemas.

Control de Acceso Físico.

Usuarios autorizados. Llave.

Gestión Documental.

Archivos en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.

Control de Acceso Lógico.

Archivos no públicos; usuario y contraseña; registro de entradas; cambio de contraseñas dos veces al año; bloqueo de acceso tras dos intentos; control de cambio de contraseñas por la empresa.

Copias de Respaldo y Procedimiento de Recuperación.

Copias de respaldo diarias; Procedimiento de recuperación estándar.

Sistema de Identificación y Autenticación.

Usuario y contraseña, contraseña: longitud mínima: ocho caracteres, números y letras; Cambio de contraseña al menos dos veces al año, tres intentos de entrada, almacenamiento cifrado.

Registro de Acceso a los Documentos.

Usuarios autorizados.

BASE DE DATOS: PROVEEDORES.**Finalidades.**

Gestión administrativa, Gestión fiscal, Gestión de cobros y pagos, Gestión económica y contable, Históricos de relaciones comerciales, Gestión de proveedores.

Información contenida.

Razón social, cámara de comercio, Rut, Nit, documentos de identificación, teléfonos, direcciones, contratos, correo electrónico.

Tipo de dato.

Privado.

Sistema de tratamiento.

Automatizada.

Cantidad de Titulares.

835

Origen y procedencia de los datos.

Recogidos por el responsable.

Encargados del Tratamiento.

FRANCISCO MURILLO S.A.S.

Responsables de Seguridad.

Jefe de Sistemas.

Control de Acceso Físico.

Usuarios autorizados. Llave.

Control de Acceso Lógico.

Archivos no públicos; usuario y contraseña; registro de entradas; cambio de contraseñas dos veces al año; bloqueo de acceso tras dos intentos; control de cambio de contraseñas por la empresa.

Copias de Respaldo y Procedimiento de Recuperación.

Copias de respaldo diarias; Procedimiento de recuperación estándar.

Sistema de Identificación y Autenticación.

Usuario y contraseña, contraseña: longitud mínima: ocho caracteres, números y letras; Cambio de contraseña al menos dos veces al año, tres intentos de entrada, almacenamiento cifrado.

Registro de Acceso a los Documentos.

Usuarios autorizados.

BASE DE DATOS: EMPLEADOS.**Finalidades.**

Gestión administrativa, Gestión de cobros y pagos, Gestión fiscal, Gestión económica y contable, Históricos de relaciones comerciales, Gestión de nómina, Gestión de

personal, Gestión de trabajo temporal, Prestaciones sociales, Prevención de riesgos laborales, Promoción y selección de personal.

Información contenida.

Hoja de vida, cédula, certificaciones académicas, laborales, procuraduría, pasado judicial, afiliación seguridad social, contrato, incapacidades. permisos, memorándums.

Tipo de dato.

Sensible.

Sistema de tratamiento.

Automatizada.

Cantidad de Titulares.

94

Origen y procedencia de los datos.

Recogidos por el responsable.

Encargados del Tratamiento.

Francisco Murillo S.A.S., ARL Sura, EPS Sura, Salud Total, Savia Salud, Coomeva, Nueva EPS, Cafesalud, EPS Sanitas, Cruz Blanca, SaludVida, Colpensiones, AFP Provenir, Colfondos, Protección, Sistema de Gestión Humana S.A.S. (SIGH).

Responsables de Seguridad.

Jefe de Sistemas.

Control de Acceso Físico.

Usuarios autorizados. Doble Llave.

Gestión Documental.

Archivos en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.

Control de Acceso Lógico.

Archivos no públicos; usuario y contraseña; registro de entradas; cambio de contraseñas dos veces al año; bloqueo de acceso tras dos intentos; control de cambio de contraseñas por la empresa.

Copias de Respaldo y Procedimiento de Recuperación.

Copias de respaldo diarias; Procedimiento de recuperación estándar.

Sistema de Identificación y Autenticación.

Usuario y contraseña, contraseña: longitud mínima: ocho caracteres, números y letras; Cambio de contraseña al menos dos veces al año, tres intentos de entrada, almacenamiento cifrado.

Registro de Acceso a los Documentos.

Usuarios autorizados.

BASE DE DATOS: EMPLEADOS FÍSICA.**Finalidades.**

Gestión administrativa, Gestión de cobros y pagos, Gestión fiscal, Gestión económica y contable, Históricos de relaciones comerciales, Gestión de nómina, Gestión de personal, Gestión de trabajo temporal, Prestaciones sociales, Prevención de riesgos laborales, Promoción y selección de personal.

Información contenida.

Hoja de vida, cédula, certificaciones académicas, laborales, procuraduría, pasado judicial, afiliación seguridad social, contrato, incapacidades, permisos, memorándums.

Tipo de dato.

Sensible.

Sistema de tratamiento.

Física.

Cantidad de Titulares.

97

Origen y procedencia de los datos.

Recogidos por el responsable.

Encargados del Tratamiento.

Francisco Murillo S.A.S., ARL Sura, EPS Sura, Salud Total, Savia Salud, Coomeva, Nueva EPS, Cafesalud, EPS Sanitas, Cruz Blanca, SaludVida, Colpensiones, AFP Provenir, Colfondos, Protección, Sistema de Gestión Humana S.A.S. (SIGH).

Responsables de Seguridad.

Jefe de Sistemas.

Control de Acceso Físico.

Usuarios autorizados. Doble Llave.

Gestión Documental.

Archivos en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.

Control de Acceso Lógico.

Archivos no públicos; usuario y contraseña; registro de entradas; cambio de contraseñas dos veces al año; bloqueo de acceso tras dos intentos; control de cambio de contraseñas por la empresa.

Copias de Respaldo y Procedimiento de Recuperación.

Copias de respaldo diarias; Procedimiento de recuperación estándar.

Sistema de Identificación y Autenticación.

Usuario y contraseña, contraseña: longitud mínima: ocho caracteres, números y letras; Cambio de contraseña al menos dos veces al año, tres intentos de entrada, almacenamiento cifrado.

Registro de Acceso a los Documentos.

Usuarios autorizados.

BASE DE DATOS: SOCIOS.**Finalidades.**

Gestión administrativa.

Información contenida.

Nombre, documento de identificación, cámara de comercio, Nit, Rut, acta socio.

Tipo de dato.

Privado.

Sistema de tratamiento.

Física.

Cantidad de Titulares.

5

Origen y procedencia de los datos.

Recogidos por el responsable.

Encargados del Tratamiento.

Luis Carlos Cuartas Cuartas
Gerente

Responsables de Seguridad.

Representante Legal

Control de Acceso Físico.

Usuarios autorizados. Doble Llave.

Gestión Documental.

Archivos en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.

Control de Acceso Lógico.

Archivos no públicos; usuario y contraseña; registro de entradas; cambio de contraseñas dos veces al año; bloqueo de acceso tras dos intentos; control de cambio de contraseñas por la empresa.

Copias de Respaldo y Procedimiento de Recuperación.

Copias de respaldo diarias; Procedimiento de recuperación estándar.

Sistema de Identificación y Autenticación.

Usuario y contraseña, contraseña: longitud mínima: ocho caracteres, números y letras; Cambio de contraseña al menos dos veces al año, tres intentos de entrada, almacenamiento cifrado.

Registro de Acceso a los Documentos.

Usuarios autorizados.

ANEXO 2.

MEDIDAS DE SEGURIDAD PARA CUMPLIR CON EL PRINCIPIO DE SEGURIDAD.

Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas).

Gestión de documentos y soportes.

- Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos.
- Acceso restringido al lugar donde se almacenan los datos.
- Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico.
- Sistema de etiquetado o identificación del tipo de información.
- Inventario de soportes.

Control de acceso.

- Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones.
- Lista actualizada de usuarios y accesos autorizados.
- Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados.
- Concesión, alteración o anulación de permisos por el personal autorizado.

Incidencias.

- Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras.
- Procedimiento de notificación y gestión de incidencias.

Personal.

- Definición de las funciones y obligaciones de los usuarios con acceso a los datos.
- Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento.
- Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.

Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos.

Bases de datos no automatizadas.

Archivo.



Número único: (57) (4) 604 22 92
Aguacatala: Cra. 50C No. 10 Sur 161
Centro: Cra. 52 No. 53 55
Medellín – Colombia.



Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares.

Almacenamiento de documentos.

Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.

Custodia de documentos.

Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.

Bases de datos automatizadas.

Identificación y autenticación.

- Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización.
- Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.

Telecomunicaciones.

Acceso a datos mediante redes seguras.

Medidas de seguridad para datos privados para Bases de Datos Automatizadas y No Automatizadas.

Bases de datos automatizadas y no automatizadas.

Auditoría.

- Auditoría ordinaria (interna o externa) cada dos meses.
- Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información.
- Informe de detección de deficiencias y propuesta de correcciones.
- Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
- Conservación del Informe a disposición de la autoridad.

Responsable de seguridad.

- Designación de uno o varios responsables de seguridad.
- Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.

Medidas de seguridad para datos privados para Bases de Datos Automatizadas.

Bases de datos automatizadas.

Gestión de documentos y soportes.

Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.

Control de acceso.

Control de acceso al lugar o lugares donde se ubican los sistemas de información.

Identificación y autenticación.

Mecanismo que limite el número de intentos reiterados de acceso no autorizados.

Incidencias.

- Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente.
- Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

Medidas de seguridad para datos sensibles para Bases de Datos automatizadas y no automatizadas.

Bases de datos automatizadas.

Gestión de documentos y soportes.

- Sistema de etiquetado confidencial.
- Cifrado de datos.
- Cifrado de dispositivos portátiles cuando se encuentren fuera.

Control de acceso.

- Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede.
- Control del registro de accesos por el responsable de seguridad. Informe mensual.
- Conservación de los datos: 2 años.

Telecomunicaciones.

- Transmisión de datos mediante redes electrónicas cifradas.

Bases de datos no automatizadas.

Control de acceso.

- Acceso solo para personal autorizado.
- Mecanismo de identificación de acceso.
- Registro de accesos de usuarios no autorizados.

Almacenamiento de documentos.

- Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.

Copia o reproducción.

- Solo por usuarios autorizados.
- Destrucción que impida el acceso o recuperación de los datos.

Traslado de documentación.

- Medidas que impidan el acceso o manipulación de documentos.