TABLA DE CONTENIDO

COPIA CONTROLADA

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN

La CAJA DE COMPENSACIÓN FAMILIAR DE BOYACÁ - COMFABOY, con objeto de garantizar el adecuado cumplimiento de la Ley Estatutaria 1581 de 2012 de Protección de Datos (LEPD) y del Decreto 1377 de 2013, adopta este Manual Interno de Seguridad donde se recogen las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en el artículo 4 literal g) de la LEPD.

El presente manual pertenece a: CAJA DE COMPENSACIÓN FAMILIAR DE BOYACÁ - COMFABOY.

. Dirección: CARRERA 10 # 16- 81
. Correo electrónico: protecciondedatos@comfaboy.com.co
. Teléfono:7441515 Extensión 1220

2. ALCANCE

Las disposiciones de este documento se aplican a las bases de datos objeto de responsabilidad de la COMFABOY, así como a los sistemas de información, soportes y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa vigente, a las personas que participan en el tratamiento y a los locales donde se ubican dichas bases de datos.

3. DEFINICIONES DE CONCEPTOS EN MATERIA DE SEGURIDAD

. Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es

el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.
. Autenticación: Procedimiento de verificación de la identidad de un usuario.
. Contraseña: Contraseña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.
. Control de acceso: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.
. Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.
. Identificación: Proceso de reconocimiento de la identidad de los usuarios.
. Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.
. Perfil de usuario: Grupo de usuarios a los que se da acceso.
. Recurso protegido: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.
. Responsable de seguridad: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.
. Sistema de información: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.
. Soporte: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
. Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

4. CUMPLIMIENTO Y ACTUALIZACIÓN

El Manual Interno de Seguridad es un documento interno de la empresa de obligatorio cumplimiento para todo el personal de COMFABOY, con acceso a los sistemas de información que contengan datos personales.

Este manual debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

5. MEDIDAS DE SEGURIDAD

Las bases de datos son accesibles únicamente por las personas designadas por COMFABOY, y referidas en el numeral 6 de este documento.
Los responsables de seguridad de COMFABOY señalados en numeral 6 del presente manual, se encargan de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.
A continuación, se enumeran y detallan las medidas de seguridad implementadas por COMFABOY.

COPIA CONTROLADA

5.1. MEDIDAS DE SEGURIDAD COMUNES

5.1.1. Gestión de documentos y soportes

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el listado maestro de documentos del Sistema Gestión de Calidad de COMFABOY.

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados están referidos en el numeral 6 sobre bases de datos y sistemas de información del presente manual.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos del archivo y de Gestión de Calidad.

La identificación de los documentos y soportes que contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de las sedes que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

5.1.2. Control de acceso

El personal de COMFABOY solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento en este manual.

COMFABOY se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos de acuerdo a los procedimientos de Gestión Tecnológica. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a COMFABOY, que de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

Los usuarios autorizados para el acceso a las bases de datos se establecen en el numeral 6 de este manual.

5.1.3. Ejecución del tratamiento fuera de las sedes.

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de las sedes requiere una autorización previa por parte de COMFABOY, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

5.1.4. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias son borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.
Solamente el personal autorizado en el numeral 6 puede realizar copias o reproducir los documentos.

COPIA CONTROLADA

5.1.5. Responsable de seguridad

COMFABOY, ha designado a los respectivos responsables de seguridad que serán los encargados de coordinar y controlar las medidas de seguridad contenidas en el presente manual.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

5.1.6. Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento de COMFABOY, clasificadas con nivel de seguridad sensible o privado, se han de someter, al menos una vez cada año, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.
COMFABOY, realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

Las auditorías concluirán con un informe de auditoría que contendrá:

. El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
. La identificación de las deficiencias halladas y la sugerencia de medidas correctivas o complementarias necesarias.
. La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

El responsable de seguridad que corresponda estudiará el informe y trasladará las conclusiones al responsable del tratamiento para que implemente las medidas correctivas.

5.2. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS NO AUTOMATIZADAS

5.2.1. Archivo de documentos

COMFABOY, fija los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización, consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. Estos criterios y procedimientos se recogen en el numeral 6 de este manual.

Se recomienda que los documentos sean archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión, tratamiento y la diferenciación entre bases de datos históricas, de administración o gestión de la empresa.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso la COMFABOY, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Los dispositivos se identifican y describen en el numeral 6 del presente manual.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible, deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, COMFABOY, podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente manual.

La descripción de las medidas de seguridad de almacenamiento se encuentra recogidas en el numeral 6 de este documento.

5.2.2. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas.
El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido.
El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad de COMFABOY.

5.2.3. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envío.

COPIA CONTROLADA

5.3. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS AUTOMATIZADAS

5.3.1. Identificación y autenticación.

COMFABOY, debe instalar un sistema de seguridad informática que permita identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecer un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento, etc. La nomenclatura utilizada para la asignación de nombres de usuario para acceder al sistema de información y el sistema de autenticación de los usuarios se recogen en el numeral 6 de este documento.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomienda que tengan un mínimo de nueve caracteres y contengan mayúsculas, minúsculas, números y letras. La política de contraseñas de la COMFABOY, se encuentra en el numeral 6 del presente manual.
Por otra parte, COMFABOY, debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días. El periodo de vigencia de las contraseñas se recoge en el ya referido numeral 6.

COMFABOY, también garantiza el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados, también detallado en el numeral 6 del manual.

5.3.2. Control de acceso físico

Las sedes de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; así mismo, han de cumplir con las medidas de seguridad físicas correspondientes al documento o soporte donde se incluyen los datos.

COMFABOY, tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas. Las sedes e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad se señalan en el numeral 6 del presente documento.

Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.

5.3.3. Copias de respaldo y recuperación de datos

COMFABOY, ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez a la semana, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello.
COMFABOY, se encargará de controlar y verificar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses mediante.
Los procedimientos de copia y respaldo se recogen en numeral 6 de este manual.

COMFABOY, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

5.3.4. Registro de acceso

De los intentos de acceso a los sistemas de información de COMFABOY, deberá guardar, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.
Los responsables de seguridad de las bases de datos automatizadas, se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter trimestral la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

COPIA CONTROLADA

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente en el presente documento.

5.3.5. Redes de comunicaciones

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.
La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

6. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de COMFABOY, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

COMFABOY, debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, carteleras, etc.). De igual modo, debe poner a disposición del personal el presente manual para que puedan conocer la normativa de seguridad de la empresa y sus obligaciones en esta materia en función del cargo que ocupan.

COMFABOY, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación referidos en el numeral 6 sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de COMFABOY, se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la empresa y, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el numeral 6 sobre bases de datos y sistemas de información. Cuando un usuario trate

documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.
El incumplimiento de las obligaciones y medidas de seguridad establecidas en este manual por parte del personal al servicio de COMFABOY, es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la empresa.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de COMFABOY, son las siguientes:

. Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la empresa u organización no pueden comunicar o revelar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.
. Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos. Cuando se firmen contratos de transmisión de datos a estos se les dará el procedimiento de custodia de archivo definida.
. Obligaciones relacionadas con las medidas de seguridad implantadas:
- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
- No revelar información a terceras personas ni a usuarios no autorizados.
- Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.
- No sacar información de las instalaciones de la organización sin la debida autorización.
. Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse a los responsables de seguridad que podrán autorizarla y en su caso, registrarla.
. Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.
. Obligación de notificar incidencias: Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.
. Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
. Responsabilidad sobre los terminales de trabajo y portátiles: Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.
. Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la empresa.
. Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
. Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.
. Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el presente manual.

COPIA CONTROLADA

6.1. Bases de datos y sistemas de información

Las bases de datos almacenadas y tratadas por COMFABOY, se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

Tabla I. Bases de datos y nivel de seguridad

BASE DE DATOS	NIVEL DE SEGURIDAD	SISTEMA DE TRATAMIENTO
Comfaboy	SENSIBLE	MIXTO
Fovis	SENSIBLE	MIXTO
Finan_cont	SENSIBLE	MIXTO
New Hotel Hotel Panorama	SENSIBLE	MIXTO
New Hotel Centro Vacacional de Moniquirá	SENSIBLE	MIXTO
New Hotel Centro Recreacional y de Convenciones Sogamoso	SENSIBLE	MIXTO
dbfonede	SENSIBLE	MIXTO
dbcygnus	SENSIBLE	MIXTO
Lsi_ctlhw	SENSIBLE	MIXTO
Lsi_Acs	SENSIBLE	MIXTO
Sihos	SENSIBLE	MIXTO
SGA	SENSIBLE	MIXTO
Sevenet	SENSIBLE	MIXTO

COPIA CONTROLADA

Adulto mayor	SENSIBLE	MIXTO
Arcabuco	SENSIBLE	MIXTO
Caldas	SENSIBLE	MIXTO
Chiquinquirá	SENSIBLE	MIXTO
Deportes	SENSIBLE	MIXTO
Educación adultos	SENSIBLE	MIXTO
Educación especial	SENSIBLE	MIXTO
EdthInfinite	SENSIBLE	MIXTO
Garagoa	SENSIBLE	MIXTO
Maripi	SENSIBLE	MIXTO
Miraflores	SENSIBLE	MIXTO
Nobsa	SENSIBLE	MIXTO
Paipa	SENSIBLE	MIXTO
Pree Chiquinquirá	SENSIBLE	MIXTO
Pree Duitama	SENSIBLE	MIXTO
Pree Sogamoso	SENSIBLE	MIXTO
Preetunja	SENSIBLE	MIXTO
Soracá	SENSIBLE	MIXTO
Sutamarchán	SENSIBLE	MIXTO
Tasco	SENSIBLE	MIXTO
Tibasosa	SENSIBLE	MIXTO
Toca	SENSIBLE	MIXTO
Villa	SENSIBLE	MIXTO
Zetaquira	SENSIBLE	MIXTO
Fosfec	SENSIBLE	MIXTO
Janium	SENSIBLE	MIXTO
DBContrat	SENSIBLE	MIXTO

COPIA CONTROLADA

No se permite el registro de bases de datos personales que no reúnan las condiciones mínimas de seguridad expuestas en el presente manual.

Las medidas de seguridad se clasifican en tres niveles de seguridad según el tipo de datos: público-semiprivado, privado y sensible. Los niveles de seguridad son acumulativos, de forma que las medidas de seguridad para datos sensibles incluyen también las

medidas de seguridad para los niveles, privado y público-semiprivado; y las medidas de seguridad para datos privados incluyen, a su vez, las del nivel público-semiprivado. La clasificación de los niveles de seguridad se realiza atendiendo a la tipología de los datos, la finalidad del tratamiento y la actividad del responsable del tratamiento (Tabla II).

Tabla II. Tipos de datos y el nivel de seguridad

TIPOS DE DATOS	DESCRIPCIÓN	NIVEL DE SEGURIDAD
Público	Datos contenidos en documentos públicos, en sentencias judiciales debidamente ejecutoriadas no sometidas a reserva y los relativos al estado civil de las personas	Público-semiprivado
Semiprivado	Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países (reportes positivos y negativos)	Público-semiprivado
Privado	Números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica	Privado
Sensible	Datos de salud, ideología, afiliación sindical, creencias, religión, origen racial o étnico, vida sexual, datos recabados sin consentimiento para fines policiales, datos biométricos (huellas, iris, etc.), datos derivados de la violencia de género	Sensible

La siguiente tabla recoge la estructura de las bases de datos de COMFABOY.

Tabla III. Estructura de las Bases de datos

COPIA CONTROLADA

RESPONSABLE DEL TRATAMIENTO	CAJA DE COMPENSACIÓN FAMILIAR DE BOYACÁ - COMFABOY, Nit: 891800213-8, dirección: CARRERA 10 # 16- 81, teléfono: 7441515 correo electrónico: protecciondedatos@comfaboy.com.co	
ENCARGADO DE CONSULTAS Y RECLAMOS	Oficina de servicio al cliente identificado con teléfono: 7441515, extensión 1220 correo electrónico: protecciondedatos@comfaboy.com.co	
ORIGEN Y PROCEDENCIA DE LOS DATOS	Recogidos por el responsable	
BASE DE DATOS	**TIPOS DE DATOS**	**SISTEMA DE TRATAMIENTO**
Comfaboy	SENSIBLE	MIXTO
Fovis	SENSIBLE	MIXTO
Finan_cont	SENSIBLE	MIXTO
New Hotel Hotel Panorama	SENSIBLE	MIXTO
New Hotel Centro Vacacional de Moniquirá	SENSIBLE	MIXTO
New Hotel Centro Recreacional y de Convenciones Sogamoso	SENSIBLE	MIXTO
Dbfonede	SENSIBLE	MIXTO
Dbcygnus	SENSIBLE	MIXTO
Lsi_ctlhw	SENSIBLE	MIXTO
Lsi_Acs	SENSIBLE	MIXTO

Sihos	SENSIBLE	MIXTO
SGA	SENSIBLE	MIXTO
Sevenet	SENSIBLE	MIXTO
Adulto mayor	SENSIBLE	MIXTO
Arcabuco	SENSIBLE	MIXTO
Caldas	SENSIBLE	MIXTO
Chiquinquirá	SENSIBLE	MIXTO
Deportes	SENSIBLE	MIXTO
Educación adultos	SENSIBLE	MIXTO
Educación especial	SENSIBLE	MIXTO
EdthInfinite	SENSIBLE	MIXTO
Garagoa	SENSIBLE	MIXTO
Maripí	SENSIBLE	MIXTO
Miraflores	SENSIBLE	MIXTO
Nobsa	SENSIBLE	MIXTO
Paipa	SENSIBLE	MIXTO
Preechiquinquirá	SENSIBLE	MIXTO
Preeduitama	SENSIBLE	MIXTO
Preesogamoso	SENSIBLE	MIXTO
Preetunja	SENSIBLE	MIXTO
Soracá	SENSIBLE	MIXTO
Sutamarchán	SENSIBLE	MIXTO
Tasco	SENSIBLE	MIXTO
Tibasosa	SENSIBLE	MIXTO
Toca	SENSIBLE	MIXTO
Villa	SENSIBLE	MIXTO
Zetaquira	SENSIBLE	MIXTO
Fosfec	SENSIBLE	MIXTO
Janium	SENSIBLE	MIXTO
DBContrat	SENSIBLE	MIXTO

COPIA CONTROLADA

A continuación, se exponen y describen las medidas de seguridad mínimas implantadas por COMFABOY, que están recogidas y desarrolladas en las Tablas IV, V VI, VII.

Tabla IV. 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	CONTROL DE ACCESO	INCIDENCIAS	PERSONAL	MANUAL INTERNO DE SEGURIDAD
1. Medidas tales como, destrucción de papel que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de los soportes en los que se almacenan bases de datos.	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo al rol que desempeña. 2. Lista actualizada de usuarios y accesos autorizados. 3. Autorización escrita del titular de la información para la entrega de sus datos a terceras personas, para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas	1. Elaboración e implementación del Manual de obligatorio cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

COPIA CONTROLADA

Tabla V. 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			BASES DE DATOS AUTOMATIZADAS	
ARCHIVO	ALMACENAMIENTO DE DOCUMENTOS	CUSTODIA DE DOCUMENTOS	IDENTIFICACIÓN Y AUTENTICACIÓN	TELECOMUNICACIONES
Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.	Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	Acceso a datos mediante redes seguras.

Tabla VI. Medidas de seguridad para datos privados según el tipo de bases de datos

BASES DE DATOS AUTOMATIZADAS Y NO AUTOMATIZADAS			BASES DE DATOS AUTOMATIZADAS			
Auditoría	**Responsable de seguridad**	**Manual interno de seguridad**	**Gestión de documentos y soportes**	**Control de acceso**	**Identificación y autenticación**	**Incidencias**
1. Auditoría ordinaria (interna o externa) cada año. 2. eventuales Auditorías extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. 5. Conservación del Informe a disposición de la autoridad.	1. Designación de uno o varios responsables de seguridad. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno políticas de Seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.	1. Controles al menos una vez al año de cumplimiento	1. 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.	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

COPIA CONTROLADA

Tabla VII. Medidas de seguridad para datos sensibles según el tipo de bases de datos

BASES DE DATOS NO AUTOMATIZADAS				BASES DE DATOS AUTOMATIZADAS		
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**	**Gestión de documentos y soportes**	**Control de acceso**	**Telecomunicaciones**
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos.	1. Sistema de etiquetado confidencial. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando salgan.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control del registro de accesos por el responsable de seguridad. Informe mensual. 3. Conservación de los datos: por el periodo que las leyes impongan.	1. Transmisión de datos mediante redes electrónicas cifradas.

COMFABOY nombra a los respectivos responsables de seguridad y desarrolla medidas de seguridad específicas para cada base de datos. Todo ello se recoge en la siguiente tabla.

El nombramiento de los responsables de seguridad no exonera al responsable del tratamiento o encargado del tratamiento de sus

obligaciones.

Tabla VIII. Responsables de seguridad y medidas de seguridad de las bases de datos

Registro de acceso a los documentos	Usuarios autorizados
Sistema de identificación y autenticación	Usuario y contraseña, contraseña: longitud mínima: nueve caracteres, números y letras; cambio de contraseña al menos una vez al año, tres intentos de entrada, almacenamiento cifrado.
Copias de respaldo y procedimiento de recuperación	Copias de respaldo cada 30 días; procedimiento de recuperación.
Control de acceso lógico	Usuario y contraseña, registro de entradas, cambio de contraseñas una vez al año, bloqueo de acceso tras tres intentos
Gestión documental	Archivo en carpetas AZ; almacenamiento en armarios; no se realiza transporte de documentos; destrucción de documentos mediante destructora de papel.
Control de acceso físico	Usuarios autorizados, doble llave

BASE DE DATOS	TIPOS DE DATOS	RESPONSABLE DEL TRATAMIENTO
Comfaboy	SENSIBLE	Jefe División Financiera
Fovis	SENSIBLE	Jefe División Financiera
Finan_cont	SENSIBLE	Jefe Departamento de Contabilidad y Presupuesto
New Hotel Hotel Panorama	SENSIBLE	Jefe Departamento Social
New Hotel Centro Vacacional de Moniquirá	SENSIBLE	Jefe Departamento Social
New Hotel Centro Recreacional y de Convenciones Sogamoso	SENSIBLE	Jefe Departamento Social

COPIA CONTROLADA

dbfonede	SENSIBLE	Jefe División Financiera
dbcygnus	SENSIBLE	Jefe Grupo Crédito y Cartera
Lsi_ctlhw	SENSIBLE	Jefe Grupo Gestión Humana
Lsi_Acs	SENSIBLE	Jefe Grupo Logístico
Sihos	SENSIBLE	Gerente I.P.S
SGA	SENSIBLE	Gerente E.P. S
Sevenet	SENSIBLE	Jefe Grupo Logístico
Adulto mayor	SENSIBLE	Jefe Departamento de Educación
Arcabuco	SENSIBLE	Jefe Departamento de Educación
Caldas	SENSIBLE	Jefe Departamento de Educación
Chiquinquirá	SENSIBLE	Jefe Departamento de Educación
Deportes	SENSIBLE	Jefe Departamento Social
Educación adultos	SENSIBLE	Jefe Departamento de Educación
Educación especial	SENSIBLE	Jefe Departamento de Educación
EdthInfinite	SENSIBLE	Jefe Departamento de Educación
Garagoa	SENSIBLE	Jefe Departamento de Educación
Maripí	SENSIBLE	Jefe Departamento de Educación
Miraflores	SENSIBLE	Jefe Departamento de Educación
Nobsa	SENSIBLE	Jefe Departamento de Educación
Paipa	SENSIBLE	Jefe Departamento de Educación
Preechiquinquirá	SENSIBLE	Jefe Departamento de Educación
Preeduitama	SENSIBLE	Jefe Departamento de Educación
Preesogamoso	SENSIBLE	Jefe Departamento de Educación
Preetunja	SENSIBLE	Jefe Departamento de Educación
Soracá	SENSIBLE	Jefe Departamento de Educación
Sutamarchán	SENSIBLE	Jefe Departamento de Educación
Tasco	SENSIBLE	Jefe Departamento de Educación
Tibasosa	SENSIBLE	Jefe Departamento de Educación

COPIA CONTROLADA

Toca	SENSIBLE	Jefe Departamento de Educación
Villa	SENSIBLE	Jefe Departamento de Educación
Zetaquira	SENSIBLE	Jefe Departamento de Educación
Fosfec	SENSIBLE	Jefe División Financiera
Janium	SENSIBLE	Jefe Departamento de Educación
DBContrat	SENSIBLE	Jefe Departamento Jurídico

Los encargados del tratamiento y las condiciones se establecen en los documentos de cada proceso aprobados en el Sistema Gestión de Calidad, en los cuales se determinan las actividades que se deben realizar con los datos personales y el responsable de cada una, especificando si se realiza en sistemas de información, de forma física, digitalización de documentos, etc.

Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente manual.

7. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

COMFABOY, establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

COPIA CONTROLADA

El procedimiento de notificación, gestión y respuesta ante incidencias es el siguiente:

. Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa deberá comunicarlo, de manera inmediata, a los responsables de seguridad, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.
. Una vez comunicada la incidencia ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
COMFABOY, crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos.

Asimismo, debe implementar los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

8. MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN Y REUTILIZACIÓN DE DOCUMENTOS Y SOPORTES

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Antes de iniciar la destrucción se realizará un acta o se llevará el registro en un libro o agenda, en dicha anotación se describirá el documento objeto de destrucción, la fecha, hora y firma de las dos personas que evidencian la destrucción.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de COMFABOY. Cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos y se incluirán en el presente manual.

8.1. Disposición Final

El presente manual ha sido aprobado por COMFABOY, como responsable del tratamiento de datos, aceptando su contenido, ordenando su ejecución y cumplimiento, con carácter general por todo el personal de la empresa, y en particular, por aquellos a los referidos en este documento.
Los siguientes anexos se encuentran codificados como formatos en el Sistema Gestión de Calidad de COMFABOY.

9. ANEXOS

- ATENCIÓN AL RECLAMO POR INFRACCIÓN
- PROTECCIÓN DE DATOS PERSONALES
- EJERCICIO DEL DERECHO DE ACCESO O CONSULTA
- ATENCIÓN AL DERECHO DE CONSULTA SI NO EXISTE INFORMACIÓN
- ATENCIÓN AL DERECHO DE CONSULTA SI EXISTE INFORMACIÓN
- ATENCIÓN AL RECLAMO POR INFRACCIÓN PROTECCIÓN DE DATOS PERSONALES
- EJERCICIO DEL RECLAMO DE CORRECCIÓN
- EJERCICIO DEL RECLAMO DE SUPRESIÓN
- EJERCICIO DEL RECLAMO POR INFRACCIÓN
- REGISTRO DE INCIDENCIAS"SOLICITUDES DE ACCESO Y RECLAMOS POR PARTE DE LOS TITULARES
- TRANSMISIONES DE DATOS
- ATENCIÓN A LA SOLICITUD DE PRUEBA DE AUTORIZACIÓN
- ATENCIÓN AL RECLAMO DE CORRECCIÓN
- SOLICITUD DE PRUEBA DE AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS
- REVOCACIÓN DE LA AUTORIZACIÓN
- ACUERDO DE CONFIDENCIALIDAD Y DEBER SECRETO CON ACCESO A DATOS - TRABAJADORES
- ACUERDO DE PRESTACIÓN DE SERVICIOS SIN ACCESO A DATOS - TRABAJADORES
- ACUERDO DE CONFIDENCIALIDAD Y DEBER SECRETO CON ACCESO A DATOS - CONTRATISTAS
- ACUERDO DE PRESTACIÓN DE SERVICIOS SIN ACCESO A DATOS - CONTRATISTAS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	24/May/2021	Se actualiza todo el documento

ELABORÓ	REVISÓ	APROBÓ
Nombre: Lady Carolina Gonzalez Moreno **Cargo:** Contratista **Fecha:** 24/May/2021	**Nombre:** Jaime Fernando Diaz Molina **Cargo:** Jefe Departamento de Planeación e Informática **Fecha:** 24/May/2021	**Nombre:** Jaime Fernando Diaz Molina **Cargo:** Jefe Departamento de Planeación e Informática **Fecha:** 24/May/2021

COPIA CONTROLADA