AVISO DE PRIVACIDAD CODELCAUCA

De acuerdo con lo dispuesto en la ley No. 1581 de 2012, el decreto No. 1377 de 2013, el decreto único reglamentario 1074 de 2015 y demás normas que las adicionen o modifiquen, la Cooperativa del Departamento del Cauca, Codelcauca, Informa a sus asociados, ex asociados, beneficiarios, usuarios, empleados, personal de apoyo, proveedores, aliados y al público en general, las siguientes disposiciones:

1. Identificación del Responsable del Tratamiento.

A. Razón social: La cooperativa del Departamento del Cauca, en adelante Codelcuaca.

B. Número de identificación tributaria, Nit No. 800.077.665-0

C. Dirección: Calle 3 No. 8 - 22, Barrio Centro.

D. Correo electrónica para la comunicación con los titulares: pqrs@codelcauca.com.co.

E. Teléfono: 602 8241414.

F. Sitio web: https://www.codelcauca.com.co/

2. Tratamiento y finalidad de los datos recolectados. Para conocer las bases de datos que tratamos y las finalidades de estas, usted puede consultar nuestro Manual de Políticas y Procedimientos de Habeas Data, disponible en nuestra página web

https://www.codelcauca.com.co/. De la misma forma, se pondrá en conocimiento a los titulares y al público en general, los cambios sustanciales que se produzcan en ese documento.

3. Derechos de los titulares: Usted puede ejercer en cualquier momento sus derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre sus datos personales, mediante escrito dirigido a CODELCAUCA, a la dirección de correo electrónico pqrs@codelcauca.com.co, indicando en el asunto el derecho que desea ejercitar, o mediante correo ordinario remitido a la dirección: Calle 3 No. 8 - 22, Barrio Centro.

4. Notificación a los titulares: Con el fin de cumplir con las finalidades requeridas para el adecuado funcionamiento del servicio de WhatsApp Corporativo, CODELCAUCA manifiesta que transferirá los datos personales de sus números celulares al operador Claro.

- CODELCAUDA garantiza que su información personal será tratada de acuerdo con los principios de transparencia, veracidad, confidencialidad y seguridad que resulten aplicables, de acuerdo con la naturaleza de los datos personales que recoge.

MANUAL DE POLITICAS Y PROCEDIMIENTO HABEAS DATA

REGISTRO HISTORICO DE MODIFICACIONES

Versión	Fecha	Descripción del cambio	ACTA
1	29-08-2022	Actualización política de protección de datos personales	265 del Consejo de Administración.
2	21-12-2023	Actualización política de protección de datos personales	303 del Consejo de Administración

TABLA DE CONTENIDO.

Contenido

Contenido

1. BASE DE APLICACIÓN Y AMBITO LEGAL.

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en:

1. Los artículos 15 y 20 de la Constitución Política
2. Ley Estatutaria 1266 de 2008
3. Ley 1273 de 2009
4. Ley Estatutaria 1581 de 2012
5. Decreto 1377 de 2013
6. Decreto 886 de 2014
7. Decreto 1074 de 2015
8. Título V de la Circular Única de la Superintendencia de Industria y Comercio

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una institución, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

La presente política, está dirigida a nuestros asociados, usuarios, colaboradores, proveedores, aliados y en general nuestros grupos de interés sobre los cuales CODELCAUCA realiza tratamiento de información personal.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la institución responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la organización; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar con el cumplimiento de sus obligaciones de seguridad, LA COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, nombra al director de Riesgos como encargado de

seguridad para desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad para la protección de datos personales.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo de La COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA.

Todos los usuarios identificados en el presente documento de Seguridad están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

Algunas de las normas aplicables citadas se amplían a continuación:

Tipo de Norma	Número y fecha de exposición	Titulo	Expedida por	Sinopsis Aplicación
Ley Estatutaria	1581 de 2012	*"por la cual se dictan disposiciones generales para la protección de datos personales"*	Congreso de la República	Por medio de la cual desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Ley	1273 de 2009	*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"*	Congreso de la Republica	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley	1377 de 2013	*'Por medio del cual se reglamenta parcialmente la*	Presidente de la República de Colombia.	Mediante la cual se reglamenta parcialmente la Ley 1581 de2012, por la cual se dictan disposiciones

		ley 1581 de 2012'		generales para la protección de datos personales
Decreto	1074 de 2015	*"Por medio del cual se expide el decreto reglamentario del Sector Comercio, Industria y Turismo"*	Presidente de la República de Colombia.	El Ministerio de Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria

2. DEFINICIONES ESTABLECIDAS EN EL ARTICULO 3 DE LA LEPD Y EL CAPITULO 25 SECCION 1 ARTICULO 2.2.2.25.1.3 DEL DECRETO 1074 DE 2015

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.

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. Contraseña: Seña 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. 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.

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.

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.

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.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

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 estos 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.

3. PRINCIPIOS DE LA PROTECCION DE DATOS.

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

Principio de legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos (LEPD): 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.

Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error. Principio de transparencia: En el tratamiento debe garantizarse el derecho del Titular a obtener del Manual de políticas y procedimientos Habeas Data Versión 1 29/08/2022 responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber: - El tratamiento al cual será sometidos sus datos y la finalidad del mismo. - El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes. - Los derechos que le asisten como

Titular. - La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la Ley de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el presente documento, de obligado cumplimiento para todo usuario y personal de CODELCAUCA; Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

4. CATEGORIAS ESPECIALES DE DATOS.

4.1 Datos sensibles:

Los datos sensibles son 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. Según el artículo 6 de la Ley Estatuaria de Protección de datos Personales (LEPD), se prohíbe el tratamiento de datos sensibles, excepto cuando:

El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado.

En estos eventos, los representantes legales deberán otorgar su autorización.

El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.

El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2 Derechos de los niños, niñas y adolescentes:

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.

- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho ala privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1074 de 2015. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos

4.3 Derechos de los titulares.

De acuerdo con el artículo 8 de la LEPD y al capítulo 25 sección 4 del decreto 1074 de 2015, los Titulares de los datos pueden ejercer una serie de derechos en relación con el 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 les 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, rectifique 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 LEPD.

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

5. ATORIZACION DE LA POLITICA DE TRATAMIENTO.

De acuerdo con el artículo 9 de la LEPD, 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 COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, en los

términos y condiciones recogidos en la misma.

La autorización también podrá obtenerse a partir de conductas inequívocas del titular del dato, las cuales permitan concluir de manera razonable que éste otorgó su consentimiento para el tratamiento de su información. Dichas conductas deben exteriorizar de manera clara la voluntad de autorizar el tratamiento.

En virtud de su naturaleza y objeto social, la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA recibe, recolecta, registra, conserva, almacena, modifica, reporta, consulta, entrega, transmite, transfiere, comparte y elimina información personal, para lo cual obtiene la previa autorización del titular.

La autorización que le otorgan los titulares de la información a la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA permite entre otras cosas, la realización de las siguientes finalidades: ofrecer y suministrar información de los productos y servicios, así como consultar, reportar y actualizar sus datos ante los operadores de información y riesgo; actualizar las relaciones contractuales vigentes y dar cumplimiento a las obligaciones pactadas, entre otras (ver finalidades en el presente documento).

la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA conservará prueba de dichas autorizaciones de manera adecuada, velando y respetando los principios de privacidad y confidencialidad de la información.

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 pororden 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.

Los datos personales estarán sujetos a tratamiento por la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA durante el termino contractual en el que el titular de la información tenga el producto, servicio, contrato o relación, más el término que establezca la ley.

6. RESPONSABLE DE TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, cuyos datos de contacto son

Dirección: Calle 3 No. 8 - 22, Barrio Centro

Correo electrónico: pqrs@codelcauca.com.co

Teléfono: 602 8241414

1. Las obligaciones del responsable del tratamiento.

Las obligaciones en materia de seguridad de los datos de la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el presente documento.

- Difundir el referido documento entre el personal afectado.

- Mantener este Manual actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la institución, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.

- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos.

- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.

- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en este Manual, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel y el uso de módemsy las descargas de datos.

- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperaciónde datos.

- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.

- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada dos meses.

- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada año.

7. Tratamiento y finalidades de las bases de datos

CODELCAUCA, en el desarrollo de sus actividades, 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.

De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información, CODELCAUCA realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión, entrega de los datos a terceras entidades a título deencargados o de responsables; esto de acuerdo con el acuerdo al que entre las partes se llegue. Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajolos lineamientos de las políticas de Seguridad de la Información de CODELCAUCA, en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Así mismo y en ejecución del objeto social de CODELCAUCA, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

La siguiente tabla presenta las distintas bases de datos y las finalidades asignadas a cada una de ellas.

TABLA I. BASES DE DATOS Y FINALIDADES

Nombres bases de	**Finalidades bases de datos**

datos	
Base de datos Asociados A-LNX	Dado que toda actividad de tratamiento de datos personales debe obedecer a las finalidades mencionadas en la autorización que otorga el titular del dato, o en los documentos específicos donde se regule cada tipo o proceso de tratamiento de datos personales, a continuación, y de manera general se enumeran y se presentan a título enunciativo y no restrictivo, sin limitar, las principales finalidades del tratamiento de datos personales por parte de CODELCAUCA, como responsable del tratamiento de datos para que, directamente o a través de terceros quienes adquirirán la calidad de encargados, trate mi información personal, financiera, crediticia, comercial, sensible, privada, semiprivada, profesional, laboral y de aportes de seguridad social integral, contenida en medios físicos, electrónicos o digitales, en los siguientes términos: 1. Tramitar la vinculación y servicios financieros del Titular en calidad de asociado, cliente o usuario, según corresponda y transferir de manera total o parcial la información registrada en cualquier formulario de vinculación, de actualización de datos, soportes y/o los resultados de los análisis de SARLAFT efectuados por CODELCAUCA y transmitir a entidades aseguradoras si así lo dispone la entidad. Establecer una relación contractual, así como mantener y terminar una relación contractual. 2. Realizar todas las gestiones necesarias tendientes a confirmar y actualizar la información 3. Validar y verificar la identidad para el ofrecimiento y administración de productos y servicios, así mismo para compartir la información con diversos actores del mercado. 4. Permitir la construcción, el ofrecimiento y venta de servicios y productos derivados del objeto social tanto de CODELCAUCA como de terceros a través de cualquier medio o canal de acuerdo con el perfil del Titular y los avances tecnológicos, efectuar labores de mercadeo, realizar muestreos, encuestas e investigaciones comerciales y de servicio, de riesgos y de mercado, realizar pruebas, generar estadísticas,
Base de datos Asociados F Asociados A-WRM	
Base de datos Ex asociados a-LNX	
Base de datos Usuarios, beneficiarios de asociados y exasociados	

	utilizar o elaborar modelos matemáticos, identificar, recolectar, analizar y asociar información sobre intereses y hábitos de utilización de los productos o servicios y derivar conclusiones o determinar tendencias, permitiendo que la información del Titular se pueda o no armonizar para los fines previstos en este numeral y cuyos resultados podrán ser utilizados por CODELCAUCA y aliados comerciales de esta para los fines previstos en la presente finalidad 5. Recibir mensajes relacionados con la gestión de cobro y recuperación de cartera, ya sea directamente o mediante un tercero contratado para tal función. 6. Realizar una adecuada prestación y administración de los servicios financieros, incluyendo la gestión de cobranza. 7. Implementar programas de fidelización por CODELCAUCA o sus aliados estratégicos, permitiendo el uso de dichos datos comerciales, financieros o crediticios del Titular para procesos comerciales, de mercadeo, publicidad, redención y acumulación de premios contenidos en los reglamentos y demás campañas promocionales actuales o futuras 8. Manejar cualquier información personal, financiera, crediticia, comercial, sensible, privada y semiprivada del Titular o sus beneficiarios informados a CODELCAUCA en una o varias bases de datos para ser transmitida o transferida por CODELCAUCA , hacer perfilamientos o segmentaciones a partir de la utilización de productos o servicios, incluyendo la georreferenciación o ubicación generada por cualquier dispositivo del Titular al momento de utilización de un canal virtual para propósitos de profundizar, optimizar y completar el portafolio de productos y servicios ofrecidos y tomados por el Titular o su grupo familiar. 9. Suministrar al Titular información comercial sobre los productos y servicios ofrecidos por CODELCAUCA, así como recomendaciones de seguridad, y en general cualquier información que se considere necesaria y apropiada para la utilización de los productos o la prestación de los servicios 10. Realizar el análisis de riesgos integral del Titular,

	incluyendo el cumplimiento de la normativa sobre “conocimiento del cliente: asociado/exasociado/usuarios/beneficiarios de los anteriores”, prevención de fraudes, prevención de lavado de activos y la financiación del terrorismo, así como realizar informes de seguridad sobre las transacciones validando registros físicos, auditivos, electrónicos y fílmicos con el propósito de elevar los niveles de eficiencia, evaluar y generar estadísticas para efectos de control y supervisión. En caso que sea requerido o en cumplimiento de los deberes legales y reporte a reguladores, organismos de autorregulación y autoridades competentes, el Titular autoriza compartir los resultados de dichos análisis y de los informes en desarrollo de las finalidades acá establecidas 11. Cumplir con los deberes legales impuestos a CODELCAUCA, como la transmisión de los datos a las entidades que regulan el negocio en temas tributarios, contables, administrativos, financieros y aduaneros. 12. Realizar gestiones de cobranza de todas las obligaciones con CODELCAUCA bien sea directamente o a través de terceros autorizados por ésta, quienes actuarán como encargados, así como la localización e investigación de bienes del Titular. 13. Transmitir, transferir, enviar, procesar, almacenar o enviar a proveedores que presten servicios logísticos, oferta de seguros, administrativos, aliados comerciales o estratégicos, tecnológicos, de distribución, marketing, contact center, ubicados dentro o fuera del territorio nacional que actuarán como encargados del tratamiento 14. Transmitir o transferir a la empresa o entidad ubicada dentro o fuera del territorio nacional que a futuro adquiera o administre a CODELCAUCA, o alguna unidad de negocio o de sus activos, total o parcialmente. 15. Enriquecer cualquiera de las bases de datos de CODELCAUCA utilizando datos de otras bases de entidades o personas que cuenten con la autorización pertinente, así como el cruce de información reportada y existente en las bases de datos de la Registraduría Nacional del Estado Civil, de los

	operadores de información financiera, comercial, de seguridad social y parafiscales, de empresas de servicios públicos o telefonía móvil, y de terceros que tengan autorización para el efecto de establecer, mantener, cumplir o terminar la relación contractual entre el Titular y permitir que la información del Titular sea utilizada como medio de prueba. 16. Estudiar las solicitudes de crédito del Titular, beneficiarios financieros y en general las solicitudes para celebrar cualquier operación activa de crédito y evaluar el riesgo crediticio del Titular, su comportamiento comercial, hábitos de pago, información sobre el cumplimiento de obligaciones y deberes legales, la existencia de multas o sanciones impuestas por cualquier autoridad judicial o administrativa, y compartir los resultados de dichos análisis con otras entidades. 17. Realizar actividades recreativas, deportivas, sociales y culturales que propendan por el bienestar de los asociados y sus beneficiarios. 18. Adelantar los procesos de inscripción a cursos, programas de educación y capacitaciones, tanto a nivel formal, como informal. 19. Adelantar los trámites necesarios en desarrollo de los procesos de exclusión y disciplinarios. 20. Validaciones y análisis relacionadas con el Sistema de Administración de Riesgo de Lavado de Activos y en contra de la Financiación del Terrorismo SARLAFT, la prevención contra el soborno transnacional y las demás que la normatividad colombiana disponga. 21. Gestionar los procesos relacionados con los gastos de transporte requeridos para acudir a los eventos realizados y patrocinados por la Cooperativa. 22. Suministrar, transferir o trasmitir información otorgada a las empresas con las que se tienen convenios empresariales, contratos, ventas o cesiones de cartera.

	23. Llevar un historial de la cooperativa, Conservar registros históricos y los diferentes tipos de archivo. 24. Desarrollar y adelantar programas y campañas de prevención de riesgos de salud y llevar un control de los antecedentes médicos, de los riesgos de salud y de aquellos relacionados con las actividades que realizan. 25. Efectuar la verificación de sus datos personales y de las referencias suministradas por el titular. 26. Gestionar trámites como solicitudes, quejas y/o reclamos, reportes a centrales de riesgo por incumplimiento de las obligaciones financieras derivadas de la relación comercial. 27. Para llevar un historial de consumo, Uso de imágenes fotográficas y videos con fines corporativos, Gestión comercial, conocer información del comportamiento de los asociados y del e - commerce y sus canales de contacto para realizar ofrecimientos ajustados a sus necesidades. 28. Realizar, validar, autorizar o verificar transacciones, incluyendo, cuando sea requerido, la consulta y reproducción de datos sensibles tales como la huella digital, imagen o voz, entre otros. 29. Realizar encuestas de satisfacción concerniente a los servicios prestados por CODELCAUCA 30. Consultar multas y sanciones ante las diferentes autoridades administrativas y judiciales o bases de datos públicas que tengan como función la administración de datos de esta naturaleza. 31. Tramite de auxilios o reconocimiento de beneficios sociales otorgados por CODELCAUCA o aliados estratégicos 32. Constitución de pólizas de seguros de cualquier índole 33. Ejercicio democrático de elección a cargos directivos y de control de CODELCAUCA, así como el cumplimiento de las labores que competan a su rol.

	Para el cumplimiento de las finalidades anteriores, el Titular autoriza que se le contacte por cualquier medio o canal establecido por CODELCAUCA, incluyendo la utilización de correos electrónicos, servicio de mensajes simples (SMS) o de mensajería multimedia (MMS) vía dispositivos móviles, aplicaciones (APP´s) de mensajería telefónica móvil, portales transaccionales, WhatsApp, redes sociales y otros medios electrónicos equivalentes que garanticen el contacto privado con el Titular.

Nombre bases de datos	**Finalidades bases de datos**
Base de datos Empleados F Base de datos Ex Empleados A-LNX, pasantes y personal de apoyo	La información que CODELCAUCA recolecta de aspirantes o candidatos a cargos dentro de la Cooperativa es tratada con la finalidad de realizar la evaluación de ingreso y el proceso de vinculación del aspirante, independientemente de su forma de vinculación sea esta laboral o no, y que el vínculo sea directa o indirectamente con CODELCAUCA (incluidos pasantes, practicantes, aprendices o cualquier otra denominación sea). El tratamiento de la información del personal tiene como finalidad la gestión de las relaciones laborales existentes con éstos, así como el desarrollo de las diferentes actividades establecidas por la Cooperativa. Entre las cuales resaltamos las siguientes: 1. Dar cumplimiento a las obligaciones y derechos derivados de su actividad como empleador, y a las actividades propias de su objeto social principal y conexo, las cuales pueden ser realizadas directamente o con el apoyo de terceros con los que se compartirá su información para los fines relacionados con el objeto del contrato. 2. Compartir sus datos personales con las autoridades (judiciales o administrativas) nacionales o extranjeras cuando la solicitud se base en razones legales, procesales, contables, administrativas y/o tributarias. 3. Acceso y autorización de los beneficios establecidos por el empleador, según los requisitos definidos en cada caso. 4. Consulta de sus datos en las listas internas de control, en cumplimiento de las normas nacionales y políticas internas

	asociadas al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT, así como el cumplimiento con estándares de ética, conducta, buen gobierno e integridad establecidos por CODELCAUCA 5. Para entregar su información a los operadores de libranza, los fondos de empleados y/o fondos mutuos de inversión a los cuales ha autorizado para conocer la misma. 6. Cumplir con todas las actividades de "Conocimiento del Cliente" antes, durante y después de la relación contractual establecida, la cual puede incluir identificación personal, entrevistas programadas, visitas domiciliarias, verificación de referencias laborales, personales, experiencia laboral y trayectoria profesional información de contacto, datos de carácter académico, datos del historial laboral, profesional y financiero para desarrollar adecuadamente el proceso de registro y vinculación laboral 7. Implementar acciones de bienestar laboral 8. Difundir ofertas laborales para participar en procesos internos de selección de personal en la Institución 9. Comunicar información institucional y/o publicitaria de la Cooperativa 10. Ejecutar actividades con fines estadísticos 11. Adelantar la actualización de datos y verificación de identidad de los trabajadores y sus familiares (pareja, padres hijos) 12. Desarrollar los procesos de inscripción en capacitaciones sean estos formales o informales congresos 13. Suministro de información a las empresas con la cuales se tiene convenio 14. Administración de equipos e inventarios asignados al personal 15. Confección de artículos de dotación 16. Elaboración de informes de gestión humana 17. Realizar proceso de validación y afiliación al sistema de seguridad social y cajas de compensación del colaborador y sus beneficiarios 18. Desarrollo de actividades recreativas, culturales y de bienestar a través de la Instituciones o entidades aliadas para el colaborador y su grupo familiar 19. Desarrollo de valuaciones de desempeño 20. Generación de certificaciones laborales, 21. Gestión de ascensos, traslados 22. En procesos de auditoría y control interno y externo

	23. Cumplimiento con informes o reportes legalmente obligatorios 24. Entrevistas de retiro de la Cooperativa 25. Desactivación de sistemas de información 26. Uso de huellas digitales y demás datos de salud y/o datos sensibles para los fines misionales Tratándose de excolaboradores, CODELCAUCA almacenará, aun después de finalizado el contrato de trabajo, la información necesaria para cumplir con las obligaciones que puedan derivarse en virtud de la relación laboral que existió conforme a la legislación colombiana, o en virtud de los servicios que en virtud de la relación puedan llegar a prestarse, al igual que, proporcionar las certificaciones laborales que sean solicitadas por el excolaborador o por terceros frente a quienes aquel adelante un proceso de selección.

Nombre base de datos	**Finalidades base de datos**
Acceso a edificios, vigilancia y seguridad de las instalaciones	1. Contar con información de cada uno de los empleados, del personal Outsourcing que labora al servicio del CODELCAUCA y de los visitantes que ingresen a los edificios donde se encuentren las instalaciones de la Cooperativa. 2. Controlar e identificar el acceso a las sedes administrativas de la Cooperativa. 3. Mantener la seguridad y control de accesos a los edificios, sucursales y otras instalaciones. Los datos recolectados directamente en los puntos de seguridad de las sedes administrativas, edificios, sucursales y otras instalaciones, que sean suministrados en documentos del personal de seguridad, y los datos obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de CODELCAUCA., se utilizan con fines de seguridad de las personas, los bienes e instalaciones.

Nombre Base de datos	**Finalidades Bases de datos**
COVID 19	Los datos serán utilizados con las siguientes finalidades: Reportar

	a la secretaria de salud exigidos por protocolos de Bioseguridad con el fin de realizar cerco epidemiológico; adoptar las acciones preventivas y de seguimiento de las personas infectadas; conocer el estado de salud de las personas que padezcan la enfermedad y realizar campañas para la implementación de las medidas de seguridad que se requieran. Las anteriores finalidades son enunciativas y no taxativas.

Nombre Base de datos	**Finalidades Bases de datos**
Proveedores y Aliados	Las siguientes finalidades son enunciativas y no taxativas. 1. La información solicitada al proveedor o aliado podrá incluir información de la persona natural o jurídica según corresponda. Así mismo, es posible que se solicite información de los empleados del proveedor o aliado que se encuentren dedicados a cumplir alguna función o relación con CODELCAUCA que por la labor desempeñada requieran acceso a las instalaciones, a los aplicativos y/o sistemas u otros de la organización. 2. Registro y seguimiento de proveedores: Mantener un registro actualizado de los proveedores, sus datos de contacto, productos o servicios ofrecidos solicitud de ofertas, propuestas económicas o cotizaciones y su desempeño. 3. Evaluación y selección de proveedores: Utilizar la base de datos para análisis, viabilidad veracidad y evaluar y comparar diferentes proveedores y tomar decisiones fundamentadas en la selección de proveedores. Realizar el proceso de vinculación del proveedor o aliado con la Organización, generando el desarrollo de los procedimientos internos, los cuales son de relacionamiento, contables, financieros, comerciales, logísticos, entre otros. 4. Gestiones pre contractuales y contractuales. Utilizar la base de datos, para realizar las gestiones precontractuales que se requieran para la concreción de acuerdos o contratos comerciales. 5. Gestión de contratos y acuerdos comerciales: Almacenar información sobre los contratos y acuerdos comerciales con los

	proveedores, incluyendo términos y condiciones, fechas de vencimiento y obligaciones contractuales. Gestionar y fortalecer las relaciones contractuales con el proveedor o aliado, permitiendo un mayor control en las obligaciones asumidas por las partes. 6. Gestión de pagos y facturas: Registrar y controlar los pagos realizados a los proveedores, así como el procesamiento y seguimiento de las facturas recibidas. 7. Control de inventario y suministros: Utilizar la base de datos para gestionar el inventario de los productos o suministros provenientes de los proveedores, incluyendo información sobre cantidades, fechas de entrega y reabastecimiento. 8. Evaluación de riesgos y cumplimiento: Utilizar la base de datos para evaluar y gestionar los riesgos asociados a los proveedores, así como asegurar el cumplimiento de regulaciones y normativas aplicables. 9. Gestión de reclamos y devoluciones: Registrar y gestionar los reclamos y devoluciones de productos o servicios provenientes de los proveedores. 10. Análisis de costos y rendimiento: Utilizar la base de datos para realizar análisis de costos, evaluar el rendimiento de los proveedores y tomar decisiones de mejora en la gestión de proveedores. 11. Gestión de relaciones con proveedores: Almacenar información sobre las interacciones y comunicaciones con los proveedores para mantener una relación efectiva y colaborativa. 12. Auditoría y cumplimiento normativo: Utilizar la base de datos para facilitar la auditoría de proveedores, garantizar el cumplimiento normativo y documentar las acciones tomadas. 13. Gestión de asociados y terceros externos: Registrar y gestionar información relevante sobre asociados y terceros externos que tienen relación con los proveedores, como agentes de ventas o distribuidores.

14. Registro y seguimiento de visitantes al auditorio: Mantener un registro de los visitantes que acceden al auditorio, incluyendo información de contacto y propósito de la visita.

15. Gestión de solicitudes de crédito: Almacenar y procesar las solicitudes de crédito presentadas por los proveedores, evaluando su viabilidad y otorgando líneas de crédito cuando corresponda.

16. Postulaciones de hojas de vida: Registrar y gestionar las postulaciones de hojas de vida de potenciales proveedores o colaboradores, facilitando el proceso de reclutamiento y selección.

17. Gestión de trabajadores: Registrar y gestionar la información de los trabajadores de la organización relacionados con el manejo de proveedores, como compradores, negociadores o responsables de la gestión de proveedores.

18. Análisis de proveedores clave: Utilizar la base de datos para realizar análisis de los proveedores clave, identificar oportunidades de mejora y establecer estrategias de colaboración a largo plazo.

19. Gestión de eventos y reuniones con proveedores: Registrar y gestionar la información relacionada con eventos y reuniones con proveedores, como agendas, asistencia y seguimiento de acciones acordadas.

20. Evaluación de proveedores estratégicos: Utilizar la base de datos para evaluar y gestionar los proveedores estratégicos, identificando oportunidades de colaboración y estableciendo relaciones sólidas a largo plazo.

21. Gestión de documentación legal y contractual: Almacenar y gestionar la documentación legal y contractual relacionada con los proveedores, como contratos, acuerdos de confidencialidad y certificaciones.

22. Generación de informes y análisis de proveedores: Utilizar la base de datos para generar informes y análisis de proveedores, facilitando la toma de decisiones basadas en datos y el seguimiento del desempeño de los proveedores.

	23. Ofrecer y prestar productos o servicios a través de cualquier medio o canal de acuerdo con el perfil del proveedor o aliado, y de acuerdo con los avances tecnológicos. 24. Utilizar la información que repose en la base de datos, para la presentación de informes pertinentes a los diferentes entes de control. 25. Utilizar la base de datos para información en procesos de auditoría interna y externa que se realicen al interior de la COOPERATIVA. 26. Utilizar la base de datos para verificar el cumplimiento de obligaciones fiscales y/o contables y/o aduanera y/o Administrativas, y demás que disponga la ley. 27. Utilizar la información contenida en la base de datos para la remisión de contactos a aliados estratégicos 28. Utilizar la información contenida en la base de datos para realizar campañas de Actualización de datos e información de cambios en el tratamiento de datos personales. 29. Utilizar la información contenida en la base de datos para realizar la verificación de requisitos jurídicos, técnicos y/o financieros. 30. Administrar y verificar antecedentes comerciales, reputacionales y los riesgos de lavado de activos y financiación del terrorismo, así como para detectar y/o prevenir el fraude, corrupción y otras actividades ilegales, por parte del proveedor o sus empleados en relación con la operación de CODELCAUCA.

8. PROCEDIMEINTOS PARA EJERCER LOS DERECHOS DEL TITULAR

a. Atención a los titulares de datos

Quien ocupe el cargo de DIRECTOR DE RIESGOS, será el encargado de coordinar la respuesta a la atención de peticiones, consultas y reclamos en relación con los

derechos a conocer, actualizar, rectificar y/o suprimir la información personal de los titulares. Para tal efecto el canal habilitado con el fin de que el titular ejerza sus derechos es el correo electrónico: pqrs@codelcauca.com.co.

Para la actualización de datos personales se cuentan con los siguientes canales:

Agencias físicas: los titulares de la información pueden acercarse a cualquiera de las agencias/Sucursales de CODELCAUCA. y presentar su solicitud dentro de los términos establecidos por la ley.

Página web: mediante el link "CONTACTENOS", diligenciando la información solicitada y remitiendo la solicitud de actualización de datos específica o mediante link de "Actualización de datos" publicado en dicha página.

Otros canales de actualización de datos: canal de radicación por escrito con el personal de la fuerza comercial y cobranza u otros canales que informe la CODELCAUCA para el ejercicio de la actualización de datos.

b. Derecho de acceso o consulta:

Según el capítulo 25 sección 4 del decreto 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

- Al menos una vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información quemotiven nuevas consultas.
- Para consultas cuya periodicidad sea mayor a una por cada mes calendario, la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.
- El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escritodirigidoa CODELCAUCA, enviado mediante correo electrónico pqrs@codelcauca.com.co, indicando en el asunto "ejercicio del derecho de acceso o consulta" 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 comodel documento acreditativo de tal representación.

- Petición clara y concreta 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 lainformación solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo u otros medios electrónicos.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecidopor la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA.

Una vez recibida la solicitud, CODELCAUCA, resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de lafecha 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 delprimer término. Estos plazos están fijados en el artículo 14 de la LEPD.

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

c. DERECHO DE QUEJAS Y RECLAMOS.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA enviado, mediante correo electrónico a pqrs@codelcauca.com.co indicando en el asunto “ejercicio del derecho queja o reclamo”, la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.

- Identificación del titular o de quien está presentando la reclamación, señalando su nombre y número de identificación.

- Acreditar el interés legítimo con el que actúa quien presenta el reclamo y adjuntar, en caso de ser necesarios, los soportes correspondientes. 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 clara y expresa de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación

- 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 delreclamo.

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

CODELCAUCA, 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 dedicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá sureclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

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

<u>Supresión de la información</u>

El Titular de los datos puede ejercitar los derechos de supresión sobre sus datos mediante un escrito dirigido a la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA enviado, mediante correo electrónico a pqrs@codelcauca.com.co indicando en el asunto “ejercicio del derecho de supresión de la información”

En caso de solicitar la supresión de toda o parte de su información personal deberá tener en cuenta que CODELCAUCA analizará el requerimiento realizado. Sin embargo, no procederá la supresión de la información en caso de que el titular tenga algún deber legal o contractual de permanecer en la base de datos que administra CODELCAUCA.

Revocatoria de la autorización

El Titular de los datos puede ejercitar los derechos de revocatoria sobre sus datos mediante un escrito dirigido a la COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA enviado, mediante correo electrónico a pqrs@codelcauca.com.co indicando en el asunto "Ejercicio del derecho de Revocatoria de la información"

En caso de solicitar la revocatoria de la autorización de sus datos personales, CODELCUACA analizará el requerimiento realizado y comunicará al titular si esta revocatoria procede.

No obstante, no procederá la revocatoria de la autorización en caso de que el titular tenga algún deber legal o contractual de permanecer en la base de datos que administra CODELCAUCA

Las consultas y reclamaciones presentadas se tramitarán de acuerdo con los procesos y procedimientos internos.

9. MEDIAS DE SEGURIDAD

COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, 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, COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, 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.

9.1 Encargados de seguridad

Los encargados de seguridad tienen las siguientes funciones:

Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del manual de Políticas y Procedimientos Habeas Data.

Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases dedatos y elaborar un informe periódico sobre dicho control.

Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en estemanual.

Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.

Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización en este manual y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

Definir los tiempos dentro de los cuales se realizarán las auditorias, los cuales NO podrán ser superiores aun año.

Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.

Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

9.2 Usuarios de la información

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

CODELCAUCA, 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 sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de CODELCAUCA se definen, con carácter general, según el tipo de actividad que desarrollan de acuerdocon sus funciones dentro de la institución y, específicamente, por el contenido de este Manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en este documento.

Con carácter general, 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 de Políticas y Procedimientos Habeas Data. por parte del personal al servicio CODELCAUCA, es sancionable de acuerdo con la normativa aplicablea la relación jurídica existente entre el usuario y la organización.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad deCODELCAUCA 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 CODELCAUCA no pueden comunicar o relevar a terceras personas, datos que manejen o de los quetengan 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.

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.

10. MODIFICACIONES A LA PRESENTE POLITICA

Esta política puede ser modificada en cualquier momento con el objeto de adaptarla a nuevas prácticas que se desarrollen o a novedades legislativas o jurisprudenciales en la materia. Cualquier actualización se pondrá a disposición de los titulares de la información personal en la página web https://www.codelcauca.com.co, o en cualquier otro medio que se considere pertinente, indicando la fecha de entrada en vigencia de la correspondiente modificación o actualización, según sea el caso.

11. VIGENCIA.

El presente documento entra en vigencia el 21 de diciembre de 2023 Publíquese y cúmplase

Manual de Medidas de Seguridad de Habeas Data

REGISTRO HISTORICO DE MODIFICACIONES

Versión	Fecha	Descripción del cambio	ACTA
1	21-12-2023	Creación del documento según reorganización Manual de Políticas y Procedimiento de habeas Data del 29-08-2022.	303 del Consejo de Administración

Manual de Medidas de Seguridad de Habeas Data

1. Cumplimiento y actualización.

Este es un documento interno de obligatorio cumplimiento para todo el personal CODELCAUCA, con acceso a los sistemas de información que contengan datos personales. Este manual de Políticas y Procedimientos Habeas Data, 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. Así mismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

2. Medidas de seguridad.

Las bases de datos son accesibles únicamente por las personas designadas por COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA.

El Coordinador de Sistemas de CODELCAUCA[1], se encarga 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 que podrá implementar CODELCAUCA.

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

2.1 Tabla I. 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, tales como, destructora de papel. • Acceso restringido al lugar donde se almacenan los datos • Sistema de etiquetado o identificación del tipo de información. • Inventario de los soportes en los que se almacenan bases de datos. • Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico
Generalidades	Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes. 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 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 estos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos y en este manual. La identificación de los documentos y soportes de 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 las personas. La salida de documentos y soportes que contengan datos personales fuera de los locales 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. El personal de CODELCAUCA 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.

[1] O quien haga sus veces según designe la Gerencia

	CODELCAUCA se ocupa del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. 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 por CODELCAUCA de manera expresa. Cualquier personal ajeno a CODELCAUCA, 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.
Archivo de documentos	CODELCAUCA, 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 y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares. 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 y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la institución. 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 CODELCAUCA, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas. Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de estos 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, CODELCAUCA, podrá adoptar medidas alternativas debidamente motivadas que se incluirán en el presente documento.
Entrada y salida de documentos o	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

soportes	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. Las instalaciones de CODELCAUCA son sede 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 incluyen los datos. CODELCAUCA, 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 en el presente manual. Los locales e instalaciones donde se ubican las bases de datos, especificando sus características físicas y las medidas de seguridad física existentes. 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.
Control de acceso	Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones, de acuerdo con el rol que desempeña. Lista actualizada de usuarios y accesos autorizados. 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. Concesión, alteración o anulación de permisos por el personal autorizado
Ejecución del tratamiento fuera de la institución.	El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera del lugar natural de trabajo, requiere una autorización previa por parte de CODELCAUCA, y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.
Bases de datos temporales, copias y reproducciones	Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares podrán 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 con dicha función puede realizar copias o reproducir los documentos.
Responsable de seguridad	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.

	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 tal y como se refleja en el numeral referido anteriormente. 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 en cuestión de CODELCAUCA.
Responsable de seguridad	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. 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 tal y como se refleja en el numeral referido anteriormente. 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 en cuestión de CODELCAUCA.
Registro de acceso.	De los intentos de acceso a los sistemas de información de CODELCAUCA, deberá guarda, 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 mensual 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. 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. 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.
Auditoría	Auditoría ordinaria (interna o externa) cada año. • Eventuales Auditorías 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 competente Las bases de datos que contengan datos personales, objeto de tratamiento por CODELCAUCA, clasificadas con nivel de seguridad sensible o privado, se han de someter, a una auditoria cada año, esta puede ser 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. CODELCAUCA, 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 estas. 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 encontradas y la sugerencia de medidas correctoras 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 correctoras. Los informes de auditoría serán adjuntados a este manual y quedarán a disposición de la Autoridad de Control.
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 estas.
Políticas y Procedimientos	Elaboración e implementación del presente Manual, de obligatorio cumplimiento para el personal, así como del Manual de políticas de seguridad de la información.
Copias de respaldo y recuperación de datos.	CODELCAUCA, ha llevado a cabo los procedimientos de actuación necesarios para realizar copias de respaldo. 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 podrán grabar manualmente los datos dejando constancia de ello en este manual. CODELCAUCA, se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos. Los procedimientos de copia y respaldo se recogen en el Manual de políticas de seguridad de la información y/o documentos separados. CODELCAUCA, debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de estos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar podrá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

3. Control de acceso.

Tabla II. 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**
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.	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.	1. Acceso a datos mediante redes seguras.

3.1 Identificación y autenticación.

CODELCAUCA, 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.

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 recomiendan que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y letras.

Por otra parte, CODELCAUCA debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días.

CODELCAUCA, también garantiza el almacenamiento automatizado, interno (preferiblemente cifrado), de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados.

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

Bases de datos automatizadas y no automatizadas		
Auditoría	**Responsable de seguridad**	**Políticas y Procedimientos Habeas Data**
- Auditoría ordinaria (interna o externa) cada año. - Eventuales Auditorías 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.	- Designación de uno o varios responsables de seguridad. - Designación de uno o varios encargados del control y la coordinación de las medidas del Manual políticas y procedimientos. - Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.	- Controles al menos una vez al año de cumplimiento, consistente en la auditoriaanual, así como la capacitación al personal mínimo una vez al año.

Bases de datos automatizadas			
Gestión de documentos y soportes	**Control de acceso**	**Identificación y autenticación**	**Incidencias**
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 al lugar o lugares donde se ubican los sistemas de información.	Mecanismo que limite el número de intentos reiterados de acceso no autorizados.	Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. Autorización del responsabledel tratamiento para laejecución de los procedimientos de recuperación.

Bases de datos no automatizadas			
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**
- Acceso solo para personal autorizado. - Mecanismo de identificación de acceso. - Registro de accesos de usuarios no autorizados.	- Archivadores, armarios u otros ubicados en áreas de acceso protegidascon llaves u otras medidas.	- Solo por usuarios autorizados. - Destrucción que impida el acceso o recuperación de los datos.	- Medidas que impidan el acceso o manipulación de documentos.

5. Medidas de seguridad para datos sensibles según el tipo de base de datos. Tabla IV.

Bases de datos no automatizadas			
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**
- Acceso solo para personal autorizado. - Mecanismo de identificación de acceso. - Registro de accesos de usuarios no autorizados.	- Archivadores, armarios u otros ubicados en áreas de acceso protegidascon llaves u otras medidas.	- Solo por usuarios autorizados. - Destrucción que impida el acceso o recuperación de los datos.	- Medidas que impidan el acceso o manipulación de documentos.

Bases de datos automatizadas		
Gestión de documentos y soportes	**Control de acceso**	**Telecomunicaciones**
- Sistema de etiquetado confidencial. - Cifrado de datos. - Cifrado de dispositivos portátiles cuando sean retirados.	- 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: por el periodo que las leyes impongan.	- Transmisión de datos mediante redes electrónicas cifradas.

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, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

6.1 Encargados de seguridad

Los encargados de seguridad tienen las siguientes funciones:

Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del manual de Políticas y Procedimientos Habeas Data.

Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe periódico sobre dicho control.

Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en este manual.

Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.

Comprobar periódicamente, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización en este manual y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

Cumplir y/o velar por el cumplimiento del registro Nacional de bases de datos en y dentro de los términos legales

Realizar y/o velar por el cumplimiento del registro de novedades en y dentro de los términos legales: reclamos presentados por los titulares, registro de eliminación de bases de datos, reportes de incidentes de seguridad en caso de aplicar.

6.2 Usuarios.

CODELCAUCA, 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, plataformas digitales, etc.). De igual modo, debe poner a disposición del personal el presente manual de Políticas y Procedimientos Habeas Data para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.

CODELCAUCA, 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 y mediante posibles circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de CODELCAUCA se definen, con carácter general, según el tipo de actividad que desarrollan al interior de la institución, específicamente, por el contenido de este manual. La lista de usuarios y perfiles con acceso a los recursos protegidos generalmente están recogidos en el Core Bancario.

Con carácter general, 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 el presente manual por parte del personal al servicio de CODELCAUCA es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre las partes.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de CODELCAUCA 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 organización no pueden comunicar o relevar 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 estos.

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.

- Las 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 estos.

- 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 pérfida 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 al interior de CODELCAUCA.

- 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.

- Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales propiedad de CODELCAUCA

- 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 capitulo.

7. Bases de datos y sistemas de información.

Las bases de datos almacenadas y tratadas por CODELCAUCA 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**
Asociados A-LNX	Alto
Asociados F	Alto
Asociados A-WRM	Alto
Ex asociados a-lnx	Alto
Usuarios/beneficiarios de asociados y exasociados	Alto
Empleados F	Alto
Ex Empleados A-LNX, pasantes y personal de apoyo	Alto

Acceso a edificios, vigilancia y seguridad de las instalaciones	Alto
Proveedores y Aliados	Alto
COVID 19	Alto

Se contará con tabla que recoja la estructura de las bases de datos de CODELCAUCA, mínimo con la siguiente información: Datos del responsable del tratamiento; Usuarios externos en calidad de encargado (transmisión/ transferencia), y datos de transferencia o transmisión (nombre y razón social, Tipo de documento, numero de documento, dirección, ciudad, correo electrónico, Teléfono móvil, Teléfono fijo, sitio web); Tipos de datos; control de acceso físico; control de acceso lógico; copias de respaldo, ubicación.

Hará parte anexa a este documento el registro nacional de las bases de datos vigente.

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

CODELCAUCA, identifica en este manual, a los encargados del tratamiento, así como las condiciones del encargo. Cuando exista contrato de transmisión de datos, los encargados del tratamiento se identifican en el anexo sobre transmisión de datos de este documento. Los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente manual.

8. Procedimiento de notificación, gestión y respuesta ante incidencias

COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA, 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.

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 institución 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. La incidencia se reporta al correo electrónico del responsable de Seguridad o mediante plataforma de gestión documental en caso de tenerlo implementado.

CODELCAUCA, crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de esta, 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 y debe incluirse como anexo en el presente manual.

Asimismo, de ser necesario 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.

8.1 Procedimiento de notificación, gestión y respuesta ante incidencias

CODELCAUCA, 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. 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 institución 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. CODELCAUCA, crea un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de esta, 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 y debe incluirse como anexo en el presente manual. 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.

8.2 Reporte

Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por COOPERATIVA DEL DEPARTAMENTO DE CAUCA, CODELCAUCA. Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el responsable de la información debe ser notificado de forma inmediata. Los funcionarios deben reportar a su jefe directo y/o al Oficial de Protección de Datos Personales cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de la Entidad. A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de orden de autoridad competente deberá requerirse la Asesoría Jurídica contratada por la entidad con el fin de prestar el asesoramiento adecuado.

El responsable de la información debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado, apoyado con Oficina de Tecnologías e Informática.

Se toman como referentes para el reporte los siguientes conceptos contenidos en ANEXO 5. CONCEPTOS PARA EL REPORTE DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES Manual de Usuario del Registro Nacional de Bases de Datos – RNBD:

Un Incidente de seguridad de datos personales se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de datos personales que sean tratados bien sea por el responsable del Tratamiento o por su Encargado.

La gestión de incidentes de seguridad, se refiere a la documentación de los pasos a seguir una vez se detecte la comisión del incidente, tanto a nivel correctivo como preventivo. Dentro de los cuales se deben determinar tiempos, roles y responsabilidades.

8.2.1 Causales de los incidentes

Fraude interno Delito no violento efectuado con la participación de los empleados o personas de confianza del responsable o Encargado del Tratamiento, bien sea en forma directa o indirecta.

Ejemplo Cualquier apropiación, acceso o uso indebido o no lícito de los datos personales a los cuales el Responsable o Encargado les realice tratamiento, a través de engaños, gestiones no reales, falsificación o adulteración de documentos,

administración mal intencionada, cometido por los empleados o personas de confianza dentro de la organización; quienes valiéndose de su posición o de la información privilegiada de la que disponen, realizan un manejo indebido de los datos personales o cualquier tipo de infraestructura que pueda incidir o representar un riesgo en el tratamiento de los mismos.

Fraude externo Cualquier acto efectuado por una persona ajena al responsable o Encargado del tratamiento, buscando acceder, apropiarse, causar adulteración o eliminación a los datos personales a los cuales estos les realizan tratamiento.

Ejemplo Cualquier apropiación, acceso o uso indebido o no lícito de los datos personales a los cuales el responsable o Encargado les realice tratamiento, a través de los sistemas informáticos, robo, atraco, engaños, falsificación o adulteración de documentos, cometido por personas que no pertenecen a la organización.

Daños a activos físicos Pérdida, deterioro o cualquier afectación de los datos personales a los cuales el responsable o Encargado realicen tratamiento, causados por daños a los activos físicos de los mismos.

Ejemplo Daño físico en los computadores de la empresa, archivos físicos como papel, cintas, discos, etc. Causados por cualquier tipo de incidencia como fenómenos naturales, accidentales o por problemas de orden público.

Falla de tecnología informática Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o Encargado realicen tratamiento, causados por fallas en la infraestructura tecnológica de uno u otro.

Ejemplo Daño en el funcionamiento de los sistemas de información, daño en las redes de datos, problemas con los canales de transmisión de información, VPN, aplicaciones, etc.

Ejecución y/o administración de procesos Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o Encargado realicen tratamiento, causados por fallas en la ejecución, aplicación y/o administración de procesos, procedimientos, protocolos, políticas de uno u otro.

Ejemplo Toda vulneración que se detecte por la mala aplicación o ejecución de un procedimiento ya establecido, el cual debe estar documentado y llevar una trazabilidad de su correcta ejecución.

Falla por negligencia o actos involuntarios de los titulares Pérdida, indisponibilidad, adulteración o cualquier afectación de los datos personales a los cuales el responsable o Encargado realicen tratamiento, causados por negligencia o actos involuntarios del mismo titular, que puede ver afectados tanto sus propios datos como los de otros titulares.

Ejemplo Por lo general, este riesgo se materializa cuando el titular no acata las recomendaciones de seguridad frente al manejo de sus propios datos personales,

como el uso de contraseñas de acceso a sistemas de información o cuentas bancarias, cuentas de correo electrónico, números de tarjetas bancarias, utilización de éstos en medios no seguros o excesiva confianza en la entrega de sus datos personales o de otros titulares a personas no autorizadas.

8.2.2 Tipo de incidente de seguridad

Afecta la Confidencialidad de los datos personales Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Confidencialidad de los datos personales, siendo ésta, la característica que evita la divulgación de la información a personas o procesos que no estén debidamente autorizados.

Ejemplo Cualquier acceso no autorizado a los datos personales.

Afecta la Disponibilidad de los datos personales Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Disponibilidad de los datos personales, que es la característica que garantiza el acceso a la información por las personas o procesos autorizados, siempre que sea requerida.

Ejemplo Caída en los sistemas de información, ataques de denegación de servicio

Afecta la Integridad de los datos personales Todos aquellos incidentes que afecten el principio de seguridad relacionado con la Integridad de los datos personales que es aquél que garantiza que la información se mantenga, tal como fue recolectada o generada, sin alteraciones o modificaciones no solicitadas o autorizadas.

Ejemplo Alteración en los datos personales frente a los datos entregados por el titular, sin trazabilidad de solicitud de actualización.

Afecta Confidencialidad y disponibilidad de los datos personales Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad y disponibilidad de los datos personales.

Ejemplo Acceso no autorizado a la base de datos personales y eliminación de algunos o todos los datos personales encontrados en la misma.

Afecta Confidencialidad e Integridad de los datos personales Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad e Integridad de los datos personales.

Ejemplo Acceso no autorizado a la base de datos personales y adulteración de algunos o todos los datos personales encontrados en la misma.

Afecta Disponibilidad e Integridad de los datos personales Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la disponibilidad e Integridad de los datos personales.

Ejemplo Acceso autorizado a la base de datos personales con adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

Afecta la Confidencialidad, Disponibilidad e Integridad de los datos personales Son aquellos incidentes en los cuales se afecta al mismo tiempo y de acuerdo con las definiciones anteriores los pilares de la seguridad de la información relacionados con la confidencialidad, disponibilidad e integridad de los datos personales

Ejemplo Acceso no autorizado a la base de datos con información personal y adulteración de algunos o todos los datos personales encontrados en la misma y que para perpetrar el hecho, se realice cualquier acción en forma temporal o definitiva en la que se evite el acceso a la información del (los) titular (es) por parte de personas o procesos autorizados.

9. Control de acceso y video vigilancia

Control acceso: Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados y que permita guardar la trazabilidad de los ingresos y salidas.

Video Vigilancia: La Entidad cuenta con cámaras de video vigilancia que tienen como finalidad dar cumplimiento a las políticas de seguridad física, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control. Las imágenes deberán ser conservadas por lo menos 30 días. En caso que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

10. 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 a notación 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 CODELCAUCA. 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 e incluyéndolas en el presente manual.

11. Infracciones y sanciones

De acuerdo con el Capítulo II de la Ley Estatutaria 1581 de 2012 de Protección de Datos, la Superintendencia de Industria y Comercio puede imponer sanciones por el incumplimiento de la normativa sobre protección de datos al responsable del tratamiento o al encargado del tratamiento. Las posibles sanciones son:

Multas de carácter personal e institucional hasta por el equivalente a dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción.

Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

Suspensión de las actividades relacionadas con el tratamiento hasta por un término de seis (6) meses.

En el acto de suspensión se indicarán los correctivos que se deberán adoptar.

Cierre temporal de las operaciones relacionadas con el tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio.

Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

12. Vigencia

El presente documento entra en vigencia el 21 diciembre de 2023.