PROYECTO "FORTALECIMIENTO DEL CENTRO DE DESARROLLO TECNOLÓGICO PARA LA TRANSFORMACIÓN DIGITAL Y LA INDUSTRIA 4.0, EN EL MARCO DEL ECOSISTEMA DE INNOVACIÓN DIGITAL DEL VALLE DEL CAUCA" - CÓDIGO BPIN 2017000100053.

Política De Tratamiento y Protección de Datos Personales

DEL CENTRO DE DESARROLLO TECNOLÓGICO PARA LA TRANSFORMACIÓN DIGITAL Y LA INDUSTRIA 4.0 DEL VALLE DEL CAUCA - CIDTI 4.0

Cali – Valle Del Cauca.
2020

TABLA DE CONTENIDO

Introducción

El **Centro de Desarrollo tecnológico para la transformación digital y la industria 4.0 - CDT 4.0** – es el centro tecnológico de pensamiento, innovación y desarrollo, del Valle del Cauca, que tiene como meta, acompañar a las empresas en su proceso de transformación digital, ruta hacia la industria 4.0 y así contribuir a la construcción de territorios inteligentes, *más amigables con el medio ambiente,* que *garantizan una mejor calidad de vida a sus habitantes.*

Fue creado en diciembre de 2018, por medio de la **Resolución 166 del 13 de diciembre de 2018,** de la Secretaría de las Tecnologías de la Información y Comunicación de la Gobernación del Valle del Cauca.

En cumplimiento de las disposiciones Legales y Constitucionales establecidas en Colombia, en materia de Protección de Datos Personales, Ley estatutaria 1581 de 2012 “Por la cual se dictan las disposiciones generales para la protección de datos personales”, su Decreto Reglamentario 1377 de 2013, y con el fin de garantizar el respeto y protección del 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, el **CENTRO DE DESARROLLO TECNOLÓGICO PARA LA TRANSFORMACIÓN DIGITAL Y LA INDUSTRIA 4.0, DEL ECOSISTEMA DE INNOVACIÓN DIGITAL DEL VALLE DEL CAUCA**, en el marco de la ejecución del Proyecto identificado con CÓDIGO BPIN 2017000100053, adopta mediante el presente documento, su propia Política de tratamiento y protección de datos personales - CDT 4.0.

1. Adopción de los Principios de la Protección de Datos Personales

La Ley Estatutaria 1581 de 2012, del Régimen General de Protección de Datos Personales en su artículo 4, establece como lineamiento para el tratamiento de datos personales ocho Principios Rectores Generales, con el fin de desarrollar 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; dichos principios son adoptados por medio de la presente Política De Tratamiento De Datos Personales del CDT 4.0, estableciendo como premisa obligatoria su aplicación de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley 1581, su Decreto Reglamentario 1377 de 2013 y lo consignado en el artículo 15 de nuestra Constitución Política, garantizando que el interés y finalidad superior de cada una de sus actuaciones sea el bienestar de la comunidad beneficiaria del Proyecto identificado con CÓDIGO BPIN 2017000100053, del Valle del Cauca.

A). Principio de legalidad en materia de tratamiento de datos: el tratamiento de las bases de datos es una actividad reglada que debe sujetarse a lo establecido en la Ley y en las demás disposiciones que la desarrollen y complementen.
B) Principio de finalidad: el tratamiento obedece a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual será informada al titular en todos los casos.
C) Principio de libertad: el tratamiento solo será ejercido cuando se cuente con el consentimiento, previo expreso e informado. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
D) 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**.**
E). Principio de transparencia: en el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
F). 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 previstas en la Ley y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular o por las personas que la Ley prevea expresamente, cuando haya lugar a ello. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u 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.

G). Principio de seguridad: la información sujeta a tratamiento por el responsable o encargado del tratamiento, debe manejarse 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.

H). Principio de confidencialidad: todas las personas que intervengan en el tratamiento de datos personales, salvo aquellos que 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.

CL 36 # 128-321 Business Center
Oficinas: A-101 a la A-104
Edificio A
Zona Franca - Zonamerica

2. Restricción de uso de Categorías Especiales de Datos

En el desarrollo de sus actividades el CDT 4.0**,** restringirá al máximo el uso de categorías especiales de datos personales, pero en el evento de requerirse el uso de datos de carácter sensible para efectos estadísticos y de atención a poblaciones especiales, se verificara de manera previa que dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, para lo cual se cumplirá las siguientes obligaciones:

1. Informar al Titular que por tratarse de datos sensibles no está obligado a autorizar su

Tratamiento.

2. Informar al Titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

2.1. Obligaciones Para El Tratamiento De Datos Sensibles.

CDT 4.0 generará salvaguardas sobre los datos sensibles, entendiendo estos, como son aquellos que podrían afectar la intimidad del Titular o cuyo uso indebido pudiera generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la pertenencia a organizaciones sociales, de derechos humanos o que promueva intereses de una comunidad en particular, así como los datos biométricos.

CDT 4.0 se acoge a las excepciones del artículo 6 de la Ley Estatutaria de Protección de Datos, y que indica que los datos sensibles se podrán tratar cuando.

“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” y “El tratamiento tenga una finalidad histórica, estadística o científica”

En todo caso CDT 4.0 adoptará las medidas conducentes a objetivos estadísticos y de cumplimiento adoptando cuando lo amerite, la supresión de identidad de los Titulares.

2.2. Derechos de los titulares de datos personales:

De conformidad con lo previsto en el artículo 8 de la Ley 1581 de 2012, el titular de los datos personales tiene los siguientes derechos: *"a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado; b) 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 presente ley; c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales; d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen; e) <Literal CONDICIONALMENTE exequible> Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución; f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.*

2.3. Derechos de los niños, niñas y adolescentes titulares de datos personales:

El CDT 4.0 podrá hacer tratamiento de datos personales de niños, niñas y adolescentes, restringiendo el tratamiento a datos de naturaleza pública, y cumpliendo con los siguientes requisitos:

- Respondiendo y respetando el interés superior de los niños, niñas y adolescentes.

- Asegurando 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.

Consideramos parte de nuestra obligación y como ente que ejerce el rol de capacitación, aportar a la 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 a la privacidad y protección de su información personal y la de los demás.

2.4 **Deberes del CDT 4.0 en relación con el tratamiento de datos personales:**

- Garantizar al titular el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar constancia de la autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Cuando sea del caso, garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información y adoptar las demás medidas necesarias para que la información suministrada se mantenga actualizada, en el evento de ser necesario.
- Rectificar la información cuando sea incorrecta, y comunicar lo pertinente al encargado del tratamiento.
- Tramitar las consultas y reclamos formulados por los titulares.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

2.5. Autorización para el Tratamiento de Datos Personales:

Conforme al ARTÍCULO 9o. Ley 1581 de 2012, AUTORIZACIÓN DEL TITULAR, el tratamiento de datos personales realizados por el CDT 4.0**,** requiere del consentimiento libre, previo e informado del titular de dichos datos, bien de manera expresa o bien mediante una conducta inequívoca, salvo que los datos sean públicos. Por lo anterior, el CDT 4.0**,** en su condición de responsable del tratamiento de datos personales, dispondrá de los mecanismos necesarios para obtener la autorización de los titulares, garantizándoles, en todo caso, que sea posible verificar el otorgamiento de dicha autorización. La autorización deberá conservarse por medio que permita garantizar su posterior consulta. En cualquier caso, la autorización debe ser dada por el Titular y en esta se debe poder verificar que este conoce y acepta que el CDT 4.0 recoja y utilice la información para los fines que se le indicarán de manera previa al otorgamiento de la autorización. En caso de que los datos solicitados sean sensibles, el CDT 4.0 deberá advertir que el titular no está obligado a la autorización del tratamiento. No será necesaria la autorización del titular cuando se trate de los siguientes datos personales: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública; c) Casos de

urgencia médica o sanitaria; d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) Datos relacionados con el Registro Civil de las Personas.

3. Políticas y procedimientos para consultas y reclamaciones:

El CDT 4.0, con fundamento en los parámetros legalmente establecidos en la Ley 1581 de 2012, TÍTULO V, PROCEDIMIENTOS, fija los procedimientos para consultas y reclamaciones que eventualmente serán presentados por los Titulares de datos personales, de la siguiente manera:

a) el Área encargada para la presentación de cualquier consulta o reclamo por parte de un titular (o persona legalmente legitimada) de datos personales, será la dependencia de servicio al cliente del CDT 4.0, la cual es la encargada de la atención de peticiones, consultas y reclamos del público en general y coordinará el trámite de cada requerimiento presentado con las respectivas áreas responsables de las bases de datos.

b) Procedimiento para que los titulares de la información puedan ejercer sus derechos. En todo momento, el titular de los datos podrá realizar consultas y solicitar el retiro, actualización, corrección y/o supresión de sus datos, de conformidad con lo previsto en la Ley 1581 de 2012 a través del correo electrónico: servicioalcliente@cidti4.0.com.

Los derechos de los titulares podrán ejercerse por las siguientes personas legitimadas, de conformidad con el artículo 20 del Decreto 1377 de 2013: Por el titular, quien deberá acreditar su identidad en forma suficiente. Por sus causahabientes, quienes deberán acreditar tal calidad. Por el representante o apoderado del titular, previa acreditación de la representación o apoderamiento. Por estipulación a favor de otro o para otro.

La solicitud de consulta o reclamo presentada por el titular de datos personales o un tercero legalmente legitimado deberá incluir los siguientes datos: -Nombres y apellidos. -Tipo de documento. -Número de documento. -Teléfono. -Correo electrónico. -País. -Asunto. Para la atención de las solicitudes presentadas por los titulares o personas legitimadas, el término será de máximo diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender el requerimiento dentro de dicho término, se informará al interesado expresando los motivos de la demora y con indicación de la fecha en que se atenderá su consulta, la cual, en ningún caso, podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo. Para la atención de reclamos el término máximo para atenderlos será de quince (15) días hábiles contados a partir del día siguiente de la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término se informará al interesado los motivos de la demora y la fecha en la que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer plazo.

4. Tratamiento, finalidad y vigencia de las bases de datos:

Las bases de datos sujetas al tratamiento de datos personales por parte de el CDT 4.0**,** serán de: Empresas del valle del Cauca, estudiantes, proveedores, empleados, contratistas, sociedad civil como resultado de eventos y vinculaciones comerciales. Los datos de los titulares que reposan en las bases de datos serán utilizados para los siguientes fines: Desarrollo de las actividades: envío de información, invitación a eventos de capacitación, elaboración de estadísticas y realización de estudios en áreas de tecnología e investigación entre otras. Vinculación comercial o publicitaria para eventos de difusión, promoción y sensibilización en materia de Investigación, tecnología e innovación en la era Digital, adquisición de bienes o servicios, con el fin de garantizar el Cumplimiento de las obligaciones legales y contractuales derivadas de la ejecución del proyecto: ***PROYECTO "FORTALECIMIENTO DEL CENTRO DE DESARROLLO TECNOLÓGICO PARA LA TRANSFORMACIÓN DIGITAL Y LA INDUSTRIA 4.0, EN EL MARCO DEL ECOSISTEMA DE INNOVACIÓN DIGITAL DEL VALLE DEL CAUCA" - CÓDIGO BPIN 2017000100053.***

Adicional a ello el uso de las bases de datos del CDT 4.0 estará destinado a:

a) Generar comunicaciones al interior y por fuera de CDT 4.0, que tengan por objeto dar a conocer la actividad de difusión y promoción del Centro que se han adelantado en cumplimiento del proyecto ***"FORTALECIMIENTO DEL CENTRO DE DESARROLLO TECNOLÓGICO PARA LA TRANSFORMACIÓN DIGITAL Y LA INDUSTRIA 4.0, EN EL MARCO DEL ECOSISTEMA DE INNOVACIÓN DIGITAL DEL VALLE DEL CAUCA" - CÓDIGO BPIN 2017000100053.***

b) Usar la foto y/o videograbación para ser publicada en repositorios como redes sociales tales como Twitter, Instagram, Youtube, Facebook u otras conocidas o por conocer, la página web institucional e inclusive para la publicación en medios impresos y/o publicitarios, a fin de fomentar el interés de la comunidad en el campo investigativo, de innovación y tecnología;

c) Estas fotos y/o videograbaciones podrán tratarse en formato o soporte material, en ediciones impresas o en medio electrónico, óptico, magnético, en redes, (Intranet e Internet), mensajes de datos o similares y en general para cualquier medio o soporte conocido o por conocer en el futuro.

Los datos serán conservados por un período acorde con la finalidad y necesidad de CDT 4.0.

5. Funciones y Obligaciones del CDT 4.0 para el tratamiento de datos personales.

5.1. Las obligaciones específicas en materia de seguridad de protección de los datos personales que recogerá el CDT 4.0, son las siguientes:

- Coordinar e implementar de manera eficaz y efectiva las medidas de seguridad, para la protección de los datos personales.

- Difundir el referido documento entre el personal responsable, involucrado en el manejo y protección de los datos personales en el CDT 4.0, para que sean garantes de la protección de los mismos.

- Mantener el Manual Interno de Seguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la entidad, 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 en el Manual Interno de Seguridad.

- 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 el Manual Interno de Seguridad, 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 módems y las descargas de datos.

- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de 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 tres meses (Anexo II).

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

5.2. 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 Interno de Seguridad.

- 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 el Manual Interno de Seguridad.

- 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. (Anexo II)

- 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 del Manual Interno de Seguridad y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

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

5.3. Usuarios y Colaboradores

Todas las personas, usuarios o colaboradores, que en el desarrollo de su relación con CDT 4.0, intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de CDT 4.0, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

CDT 4.0, cumple con el deber de comunicar esta política, con su inclusión en los acuerdos de confidencialidad y deber de secreto que suscriben con terceros, especialmente con los usuarios con acceso a sistemas de identificación sobre bases de datos y sistemas de información. Esta comunicación se refuerza mediante una circular informativa dirigida a los usuarios.

Las funciones y obligaciones del personal y usuarios del CDT 4.0, se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la entidad y, específicamente, por el contenido de este Manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el Manual Interno de Seguridad.

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 por parte del personal al servicio del CDT 4.0, es sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el usuario y CDT 4.0.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de CDT 4.0**,** son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su relación 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 CDT 4.0**,** no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus actividades, 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, siempre y cuando exista y sea aprobado 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 actividades.

  - 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 retirar 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 actividades 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 las actividades desarrolladas, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá 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 entrada.

- **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc. (Anexo II)

- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.

- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción

- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la entidad.

- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por

primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la entidad.

- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en el Manual de Políticas y Procedimiento y en el Manual Interno de Seguridad.

6. Modificaciones O Actualizaciones:

De implementarse cualquier cambio sustancial en las políticas de tratamiento de Datos Personales del CDT 4.0, dicho cambio será comunicado oportunamente a los titulares de los datos personales. Cuando el cambio se refiera a la finalidad del tratamiento, se obtendrá una nueva autorización por parte del titular.

7. Responsable de atender consultas y reclamaciones en materia de tratamiento de datos personales:

El área de servicio al cliente del CDT 4.0, será la encargada de adelantar el tramite pertinente, frente a las consultas o reclamaciones elevadas por el titular de datos personales, por medio del correo electrónico: servicioalcliente@cidti4.0.com teléfono: 3023849324 o mediante correo ordinario remitido a la dirección: Calle 36#128-321 Privado Locales Nos. A-101, A-102, A-103 y A-104, Zonamerica – zona franca Cali - Valle del Cauca, Colombia.

Anexo I - Solicitudes de Acceso y Reclamos por los Titulares de derechos personales.

Identificación del usuario	
Nombre y apellidos del usuario	
Departamento	
Identificación del solicitante	
Tipo de procedimiento	
Fecha	
Tipo de solicitud	
Nombre y apellidos del solicitante	
C.C./NIT	
Observaciones	

Tabla I. Registro de solicitudes de acceso y de reclamos por parte de los Titulares

Anexo II - Registro de Incidencias internas en el CDT, para el tratamiento de los datos personales.

Fecha y hora	
Tipo de incidencia	
Descripción	
Efectos	
Medidas correctivas	
Emisor de la notificación	
Receptor de la notificación	
Persona que ejecuta el proceso de recuperación	
Datos restaurados	
Datos grabados manualmente	

Tabla II. Modelo de registro de incidencias