MANUAL DE POLITICAS Y PROCEDIMIENTOS PARA EL TRATAMIENTO DE DATOS PERSONALES

canal extensia
américa

CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO 4
3. ALCANCE 4
4. DESTINATARIOS 5
5. MARCO NORMATIVO 5
6. DEFINICIONES 5
7. ROLES Y RESPONSABILIDADES 9
8. PRINCIPIOS RECTORES PARA EL TRATAMIENTO DE DATOS PERSONALES 9
8.1 PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS. 9
8.2 PRINCIPIO DE FINALIDAD 9
8.3 PRINCIPIO DE LIBERTAD 9
8.4 PRINCIPIO DE VERACIDAD O CALIDAD 9
8.5 PRINCIPIO DE TRANSPARENCIA 10
8.6 PRINCIPIO DE ACCESO Y CIRCULACION RESTRINGIDA 10
8.7 PRINCIPIO DE SEGURIDAD 10
8.8 PRINCIPIO DE CONFIDENCIALIDAD 10
8.9 PRINCIPIO DE TEMPORALIDAD 11
8.10 PRINCIPIO DE NECESIDAD O PERTINENCIA 11
8.11 INTERPRETACIÓN INTEGRAL DE LOS DERECHOS CONSTITUCIONALES 11
9. TRATAMIENTO DE DATOS PERSONALES 11
9.1 AUTORIZACION 11
9.2 FORMA Y MECANISMOS PARA OTORGAR LA AUTORIZACION 12
9.3 PRUEBA DE LA AUTORIZACION 12
9.4 RESPONSABLE DEL TRATAMIENTO 13
9.5 AVISO DE PRIVACIDAD 13
9.5.1 Contenido Mínimo Del Aviso De Privacidad 13
9.5.2 Aviso De Privacidad Y Las Políticas De Tratamiento De La Información 13

10. DERECHOS Y DEBERES 13
10.1 DERECHOS DE LOS TITULARES DE LOS DATOS 14
10.1.1. Derecho de acceso o consulta 14
10.1.2. Derechos de quejas y reclamos 15
10.1.3. Derecho a solicitar prueba de la autorización otorgada al Responsable del tratamiento 15
10.1.4. Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones 15
10.2 PERSONAS A QUIENES SE LES PUEDE SUMINISTRAR LA INFORMACIÓN 15
DEBERES DE CEXA CUANDO ACTUE COMO RESPONSABLE DEL 15
10.3 TRATAMIENTO DE DATOS 15
DEBERES DE CEXA CUANDO ACTUE COMO ENCARGADO DEL 17
10.4 TRATAMIENTO 17
11. DATOS PERSONALES SENSIBLES Y DE MENORES 18
11.1 TRATAMIENTO DE DATOS PERSONALES SENSIBLES 18
11.1.1 Autorización Especial De Datos Personales Sensibles 18
11.2 TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES. 18
12. PROCEDIMIENTOS PARA EL EJERCICIO DE DERECHOS 19
PROCEDIMIENTO PARA LA ATENCION DE SOLICITUDES Y CONSULTAS RELACIONADAS CON EL ... 20
12.1 TRATAMIENTO DE DATOS PERSONALES 20
PROCEDIMIENTO PARA LA ATENCION DE RECLAMOS RELACIONADOS CON EL TRATAMIENTO 21
12.2 DE DATOS PERSONALES 21
12.3 LEGITIMIDAD 22
12.4 VERIFICACIÓN DE LA FACULTAD PARA SOLICITAR O RECIBIR INFORMACIÓN 22
12.5 COMPETENCIA 23
13. MEDIDAS DE SEGURIDAD 23
13.1 COOKIES O WEB BUGS 26
13.2 ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS 27
13.3 CONTROL DE ACCESO 28
13.4 VIDEOVIGILANCIA 28

14. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES CON DATOS PERSONALES 28
15. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES 30
16. TRATAMIENTO DE DATOS BIOMÉTRICOS 31
17. PERÍODO DE VIGENCIA DE LAS BASES DE DATOS 31
18. REGISTRO NACIONAL DE BASES DE DATOS 31
19. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES 32
20. GESTIÓN DE DOCUMENTOS 32
21. VIGENCIA, VERSIONES Y ACTUALIZACIÓN DE LA POLÍTICA 33

1. INTRODUCCIÓN

El artículo 15 de la Constitución Política de Colombia define el derecho de protección de datos personales como el derecho de toda persona para conocer, actualizar y rectificar la información y datos personales que de ella se hayan recolectado y/o tratado en bases de datos públicas o privadas. Así mismo, la Ley 1581 de 2012 reglamenta este derecho al establecer las Disposiciones Generales para la Protección de Datos Personales en Colombia.

SOCIEDAD CANAL EXTENSIA AMÉRICA S.A., en adelante CEXA, en cumplimiento de las normas aplicables sobre recolección y tratamiento de datos personales y teniendo en cuenta que la compañía en desarrollo de sus funciones recolecta datos personales de diversos titulares, ha dispuesto el presente manual de políticas y procedimientos para el tratamiento de datos personales el cual incluye mecanismos que garantizan la protección, almacenamiento y buen uso de los datos personales, procurando que el titular de los mismos pueda ejercer su derecho a conocerlos, suprimirlos y/o elevar reclamaciones; así como el cumplimiento de las obligaciones legales en materia de protección de datos personales.

2. OBJETIVO

El presente documento tiene por objeto reglamentar las políticas y procedimientos para el Tratamiento al cual serán sometidos los datos personales que componen las Bases de Datos respecto de las cuales CEXA actúa como Responsable y/o Encargado, así como los derechos de los Titulares de los datos personales, los compromisos adquiridos por CEXA con los Titulares de los datos, en su calidad de Responsable o Encargado del Tratamiento y el procedimiento adoptado para que los Titulares puedan ejercer adecuadamente sus derechos.

3. ALCANCE

Este documento se aplica al Tratamiento de los datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos de CEXA, respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las obligaciones y lineamientos de CEXA para la administración y tratamiento de los datos personales que reposen en sus bases de datos y archivos , ya sea de forma física o digital. Dependiendo de su naturaleza y finalidad, CEXA podrá ostentar la calidad de Responsable del Tratamiento y/o Encargado del Tratamiento de los datos personales que compongan las respectivas Base de Datos. Por tanto, los principios y disposiciones dados en esta política de tratamiento de datos personales son aplicables a los procesos de CEXA que deban realizar el Tratamiento de los datos (datos públicos, datos semiprivados, datos privados, datos sensibles, datos de los niños, niñas y adolescentes), en calidad de Responsable y de Encargado

CEXA se encuentra domiciliada en la ciudad de Barranquilla (Colombia), con asiento principal en la Carrera 54 No. 72-142 Piso 6, teléfono (+57) 6053605739 y correo electrónico info@cexa.com.co

4. DESTINATARIOS

Esta política es de obligatorio conocimiento y cumplimiento para todas las personas naturales o jurídicas responsables de la administración de bases de datos de CEXA, en especial:

a) Representantes legales y/o administradores de CEXA.
b) Administradores de bases de datos personales a cargo o responsabilidad de CEXA.
c) Empleados que custodien y traten las bases de datos personales.
d) Contratistas y personas naturales o jurídicas que presten sus servicios a CEXA y que con base en su relación contractual realice cualquier tratamiento de datos personales.
e) Personas que reciben, atienden y den respuesta directa o indirectamente a las peticiones (consultas o reclamos) de información relacionada con la ley de protección de datos personales.
f) Accionistas
g) Revisores Fiscales
h) Personas Públicas y Privadas que sean usuarios de las bases de datos personales
i) Personas con las que exista una relación legal de orden estatutario
j) Las demás personas que establezca la ley.

5. MARCO NORMATIVO

Para aquellas situaciones no reguladas por el presente Manual, se estará a lo dispuesto por las el siguiente marco normativo y demás normas que les sean complementarias.

- Constitución política de Colombia. Artículos 15 y 20;
- Ley Estatutaria 1266 de 2008
- Ley 1273 de 2009
- Ley Estatutaria 1581 de 2012
- Decreto 1377 de 2013
- Decreto 886 de 2014
- Decreto 1074 de 2015
- Ley 1928 de 2018
- Título V de la Circular Única de la Superintendencia de Industria y Comercio

6. DEFINICIONES

Para efectos interpretativos de las reglas contenidas en el presente documento se adoptan las siguientes definiciones:

Acceso Restringido:	Nivel de acceso a la información limitado a parámetros previamente definidos. La compañía no hará disponibles Datos Personales para su acceso a través de Internet u otros medios de comunicación masiva, a menos que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas autorizadas.
Área Responsable de Protección de Datos:	Es el área dentro de la compañía, que tiene como función la vigilancia y control de la aplicación de la Política de Protección de Datos Personales y la implementación del Programa Integral de Protección de Datos Personales. El área de Cumplimiento de CEXA cumple con esta función.
Área Responsable de la Atención a Peticiones, Quejas, Reclamos y Consultas:	Las peticiones, quejas, reclamos y consultas formuladas por los titulares de datos serán atendidas por el área de Cumplimiento a través de la figura del Oficial de Protección de Datos,
Autorización:	Consentimiento previo, expreso e informado, emitido por el titular, para efectos de someter sus datos a una actividad de tratamiento.
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 sean objeto de tratamiento. Incluye archivos físicos y electrónicos.
Calidad Del Dato:	El dato personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. Cuando se esté en poder de datos personales parciales, incompletos, fraccionados o que induzcan a error, la compañía deberá abstenerse de someterlo a Tratamiento, o solicitar a su Titular la completitud o corrección de la información.
Cliente:	Toda persona natural o jurídica que adquiera bienes y/o servicios comercializados o provistos por CEXA.
Circulación Restringida:	Los datos personales sólo serán tratados por aquel personal de la compañía o quienes dentro de sus funciones tengan a cargo la realización de tales actividades. No podrán entregarse Datos Personales a quienes no cuenten con autorización o no hayan sido habilitados por la compañía para tratarlos.
Confidencialidad:	Elemento de seguridad de la información que permite establecer quienes y bajo qué circunstancias se puede acceder a la misma.
Dato personal:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales, determinadas o determinables. Debe entonces

	entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).
Dato privado:	El dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
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.
Dato semiprivado:	Es aquella información que no es de naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como es el caso de los datos financieros, crediticios o actividades comerciales.
Dato sensible:	Es aquel dato que afecta la intimidad personal 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.
Derecho de los niños, niñas y adolescentes:	En el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Sólo podrán tratarse aquellos datos que sean de naturaleza pública.
Dato biométrico:	Todos aquellos datos relativos a las características físicas, fisiológicas o comportamentales de una persona que faciliten su identificación.
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. CEXA, actúa como encargado del tratamiento de datos personales en aquellos casos, en los que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta de un responsable del tratamiento.
Información Digital:	Toda aquella información que es almacenada o transmitida por medios electrónicos y digitales como el correo electrónico u otros sistemas de información.
Oficial de protección de Datos:	Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales,

	que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012. En el caso de CEXA esta función la cumple el Oficial de Cumplimiento.
Propietario de la base de datos personales:	Dentro de los distintos procesos ejecutados por CEXA, se considera propietario de la base de datos al área que tiene bajo su responsabilidad el tratamiento de los mismos y su gestión.
Proveedor:	Toda persona natural o jurídica que provea bienes y/o servicios a CEXA en virtud de una relación contractual.
Responsable de administrar las bases de datos:	Colaborador encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos específica; así como de poner en práctica las directrices que dicte el Responsable del tratamiento y el Oficial de Protección de datos.
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. Como responsable del tratamiento de datos, CEXA recolecta los datos personales y decide sobre la finalidad, contenido y uso de la base de datos.
Titular del dato:	Persona natural cuyos datos personales son objeto de tratamiento.
Transferencia:	La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.
Transmisión:	Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.
Tratamiento:	Es cualquier operación o conjunto de operaciones sobre datos personales que realice CEXA o los encargados del tratamiento, tales como la recolección, almacenamiento, uso, modificación, conservación, circulación o supresión, entre otras.
Usuario:	Es la persona, natural o jurídica, que tiene interés en el uso de la información personal.
Incidente de Seguridad de los Datos Personales:	Cualquier situación que implique la violación de las medidas de seguridad adoptadas por CEXA para la protección de los datos personales entregados para su custodia, sea como Responsable y/o Encargado, así como cualquier conducta inadecuada que infrinja lo dispuesto en esta política o la ley de protección de datos personales. Los incidentes de seguridad que comprometan los datos personales

en poder de la compañía deberán ser informados a la autoridad de control competente.

7. ROLES Y RESPONSABILIDADES

La responsabilidad del tratamiento adecuado de los datos personales corresponde a todos sus empleados y administradores. En consecuencia, cada área de la compañía que trata los datos personales, dada su condición de Propietario de la base de datos, debe adoptar reglas y procedimientos para la aplicación y el cumplimiento de esta política. En caso de duda sobre el tratamiento de los datos personales, se debe contactar al oficial de Datos Personales, al área responsable de la seguridad de la información y/o a la Dirección Jurídica para establecer las pautas a seguir en función de la protección de los datos personales.

8. PRINCIPIOS RECTORES PARA EL TRATAMIENTO DE DATOS PERSONALES

Para el adecuado tratamiento de datos personales que componen las Bases de Datos al igual que en lo referente a la interpretación y ejecución de las presentes políticas, se acatarán de manera armónica e integral los siguientes principios:

8.1 PRINCIPIO DE LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS.

Durante todas las etapas y actividades de Tratamiento de información por parte de CEXA en calidad de Responsable y/o Encargado o quien esta designe como Encargado de Tratamiento, se dará aplicación además de a lo establecido en la presente política, a lo establecido en la Ley Estatutaria de Protección de Datos Personales o Ley 1581 de 2012, el Decreto 1377 de 2013 Compilado en el Capítulo 25 del Decreto 1074 de 2015 y todas aquellas que las reglamenten, adicionen, modifiquen o supriman.

8.2 PRINCIPIO DE FINALIDAD

El Tratamiento de los Datos Personales recolectados por CEXA tendrá por objeto una finalidad legítima, de acuerdo con la Constitución Politica y la Ley, la cual debe ser informada a su Titular.

8.3 PRINCIPIO DE LIBERTAD

El Tratamiento sólo se ejercerá con el consentimiento, previo, expreso e informado del Titular. CEXA no obtendrá o divulgará datos personales sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

8.4 PRINCIPIO DE VERACIDAD O CALIDAD

CEXA se compromete con los Titulares de la información que compone sus bases de datos, a garantizar que la misma sea veraz, completa, exacta, actualizada, comprobable y comprensible, consecuencialmente. La compañía se abstendrá de tratar datos parciales, incompletos, fraccionados o que induzcan a error.

8.5 PRINCIPIO DE TRANSPARENCIA

CEXA establece que 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. 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.

8.6 PRINCIPIO DE ACCESO Y CIRCULACION RESTRINGIDA

El acceso a la información que compone la Base de Datos está restringido al personal especializado y previamente capacitado para la manipulación de este tipo de información. El tratamiento de los datos personales está sujeto a los límites que se derivan de su naturaleza, de las disposiciones de la ley y la Constitución Política. CEXA no publica la información personal objeto de tratamiento en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la ley.

8.7 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 de todo el 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 DC-084 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, de obligado cumplimiento para todo usuario y personal de la empresa. 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.

8.8 PRINCIPIO DE CONFIDENCIALIDAD

CEXA garantiza la reserva de la información que no tiene la naturaleza de pública, incluso después de finalizada la relación con los terceros que intervengan en el tratamiento de los datos, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

8.9 PRINCIPIO DE TEMPORALIDAD

Los datos personales se conservarán únicamente por el tiempo necesario de acuerdo a las finalidades que justificaron su tratamiento. Así mismo, se tendrán en cuenta para su conservación aquellas disposiciones aplicables, así como aspectos administrativos, contables, fiscales, jurídicos e históricos de la información; o cuando sea necesaria su conservación para el cumplimiento de una obligación legal o contractual. Agotadas todas las condiciones para su conservación, CEXA deberá proceder a la supresión de los datos.

8.10 PRINCIPIO DE NECESIDAD O PERTINENCIA

Los datos personales recolectados deben ser los estrictamente necesarios, adecuados y pertinentes en relación con la finalidad por la cual se obtienen.

8.11 INTERPRETACIÓN INTEGRAL DE LOS DERECHOS CONSTITUCIONALES

La interpretación de los derechos se realizará em completa armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución Política de Colombia y los demás derechos constitucionales aplicables.

9. TRATAMIENTO DE DATOS PERSONALES

CEXA en el desarrollo de su actividad empresarial, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley. El tratamiento al cual serán sometidos los datos personales incluye recolección, almacenamiento, uso, circulación o supresión. El tratamiento de los datos estará sujeto a las finalidades autorizadas por el Titular, a las obligaciones contractuales entre las partes, así como, a los casos en los cuales existan obligaciones legales que deba cumplir.

El documento denominado DC-083 Organización Bases de Datos, contiene la información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

9.1 AUTORIZACION

CEXA solicitará al Titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015. Las actividades de tratamiento de información reglamentadas por la presente política, serán ejecutadas exclusivamente sobre datos personales cuyos titulares hayan emitido su autorización de manera previa expresa e informada.

Sin perjuicio de lo anterior, CEXA se reserva el derecho a ejecutar actividades de tratamiento sobre información cuya autorización no sea requerida en virtud de las disposiciones legales que

reglamentan la materia, caso en el cual continúan vigentes los compromisos de CEXA frente a los titulares establecidos en la presente política.

Para los efectos pertinentes, CEXA puede obtener los datos sometidos a tratamiento recolectándolos directamente, para lo cual deberá contar con la respectiva autorización, o de bases de datos suministradas por terceros, quienes previamente hayan obtenido autorización de los Titulares.
No será necesaria la autorización del Titular cuando se trate de:

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

9.2 FORMA Y MECANISMOS PARA OTORGAR LA AUTORIZACION

La autorización puede constar en un documento físico, electrónico o en cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo mediante el cual se pueda concluir de manera inequívoca, que de no haberse surtido una conducta del Titular, los datos nunca hubieren sido recolectados y almacenados en la base de datos. El formato para la autorización será elaborado por CEXA y será puesto a disposición del Titular previo al tratamiento de sus datos personales, de conformidad con lo que establece la Ley 1581 de 2102 y el Decreto 1377 de 2013 y demás normas complementarias. Con el procedimiento de autorización consentida se garantiza que se ha puesto en conocimiento del Titular de los datos personales, que su información personal será recogida y utilizada para fines determinados y conocidos, y el derecho que le asiste para solicitar el acceso, la actualización, rectificación y eliminación de sus datos personales en cualquier momento, a través de los mecanismos puestos a su disposición por CEXA. Lo anterior con el fin de que el Titular tome decisiones informadas con relación a sus datos personales y controle el uso de su información personal.

Al momento de solicitar la autorización del Titular, CEXA le informará de manera clara y expresa:

a) El Tratamiento de los datos y su finalidad
b) Los datos que serán recolectados
c) Los derechos que le asisten como titular
d) Si se trata de datos sensibles, el derecho a decidir si suministra o no la información solicitada.
e) La identificación, dirección física y/o electrónica y teléfono del responsable del tratamiento.

9.3 PRUEBA DE LA AUTORIZACION

CEXA adoptará las medidas necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo la autorización por parte de los titulares de datos personales para el tratamiento de los mismos.

9.4 RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es CEXA, cuyos datos de contacto son los siguientes:

Dirección: Carrera 54 72-142 Piso 6
Correo electrónico: info@cexa.com.co
Teléfono: 6053605739

9.5 AVISO DE PRIVACIDAD

El Aviso de Privacidad es el documento físico, electrónico o en cualquier otro formato, que es puesto a disposición del Titular para el tratamiento de sus datos personales a más tardar al momento de recolección de los datos personales. A través de este documento se informa al Titular la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

9.5.1 Contenido Mínimo Del Aviso De Privacidad

El Aviso de Privacidad, como mínimo, deberá contener la siguiente información:

a) La identidad, domicilio y datos de contacto del Responsable del Tratamiento;
b) El tipo de tratamiento al cual serán sometidos los datos y la finalidad del mismo;
c) Los derechos que le asisten al Titular;
d) Los mecanismos generales dispuestos por CEXA para que el Titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de tratamiento de información.

No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad señalará expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

9.5.2 Aviso De Privacidad Y Las Políticas De Tratamiento De La Información

CEXA conservará el modelo del aviso de privacidad que se transmitió a los Titulares mientras se lleve a cabo el tratamiento de datos personales y perduren las obligaciones que de este se deriven. Para el almacenamiento del modelo, CEXA podrá emplear medios informáticos, electrónicos o cualquier otra tecnología.

10. DERECHOS Y DEBERES

10.1 DERECHOS DE LOS TITULARES DE LOS DATOS

El Titular de los Datos Personales tiene derecho a:

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 o así lo establezcan las normas aplicables;

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 la Ley de Protección de Datos o aquellas que la modifiquen, adicionen o complementen;

e) Revocar la autorización y/o solicitar la supresión del dato cuando: (i) En el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, siempre que la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias al ordenamiento; y/o (ii) Así lo solicite voluntariamente, salvo que exista obligación legal o contractual que le imponga el deber de permanecer en la base de datos;

Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Estos derechos podrán ejercerse por las siguientes personas.

a. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el Responsable.

b. Por sus causahabientes, quienes deberán acreditar tal calidad.
c. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
d. 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

10.1.1. 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.

10.1.2. Derechos de quejas y reclamos

La Ley distingue cuatro tipos de reclamos:

- Reclamo de corrección: el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Reclamo de supresión: el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- Reclamo de revocación: el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- Reclamo de infracción: el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

10.1.3. 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 1581 de 2012 de Protección de Datos (LEPD).

10.1.4. Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones

El Titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el Responsable del tratamiento o Encargado del tratamiento.

10.2 PERSONAS A QUIENES SE LES PUEDE SUMINISTRAR LA INFORMACIÓN

De acuerdo a lo contemplado en la ley, la información que reúna las condiciones establecidas podrá ser suministrada a las siguientes personas:

a) Titulares, causahabientes o sus representantes legales.
b) Entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
c) Terceros autorizados por el titular o por la ley.

10.3 DEBERES DE CEXA CUANDO ACTUE COMO RESPONSABLE DEL TRATAMIENTO DE DATOS

Cuando actúe como responsable del Tratamiento, CEXA velará por el cumplimiento de:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Solicitar la Autorización al Titular

c) Conservar copia de la Autorización otorgada por el Titular;

d) Entregar copia de la Autorización cuando el Titular o quien esté autorizado, la solicite;

e) Informar al Titular sobre la finalidad de la recolección y los derechos que le asisten con ocasión de su Autorización;

f) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

g) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

h) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, las novedades respecto de los Datos que previamente le haya suministrado y adoptar las medidas para que la información suministrada a éste se mantenga actualizada;

i) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

j) Suministrar al Encargado del Tratamiento, únicamente Datos cuyo Tratamiento esté previamente autorizado;

k) Exigir al Encargado del Tratamiento el respeto a las condiciones de seguridad y privacidad de la información del Titular;

l) Tramitar las consultas y reclamos formulados;

m) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

n) Informar a solicitud del Titular sobre el uso dado a sus datos;

o) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

p) Cumplir las instrucciones y requerimientos de la Superintendencia de Industria y Comercio.

PARÁGRAFO: CEXA se reserva la facultad de delegar ciertas actividades de tratamiento a un tercero, para que las ejecute en su nombre, caso en el cual este último observará los deberes establecidos en la sección 17 de la presente política.

10.4 DEBERES DE CEXA CUANDO ACTUE COMO ENCARGADO DEL TRATAMIENTO

Cuando CEXA actúe como Encargado del Tratamiento, velará por el cumplimiento de:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

c) Realizar oportunamente la actualización, rectificación o supresión de los datos;

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

e) Tramitar las consultas y los reclamos formulados por los Titulares;

f) Contar con un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento la Ley de Protección de Datos y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

g) Registrar en la base de datos la leyenda "reclamo en trámite", cuando ello corresponda;

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez sea notificada por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

11. DATOS PERSONALES SENSIBLES Y DE MENORES

11.1 TRATAMIENTO DE DATOS PERSONALES SENSIBLES

CEXA reconoce que ciertos datos sometidos a tratamiento revisten o pueden revestir la calidad de datos sensibles, por lo cual, la compañía ha adoptado las medidas para que cuando los datos sometidos a tratamiento sean de aquellos definidos legalmente como sensibles:

- Reforzar el cumplimiento de los principios que regulan el tratamiento de información personal, establecidos en el proceso de acceso, consulta y reclamación.
- Ninguna actividad está condicionada al suministro de datos personales sensibles.
- Obtener la autorización expresa, informada y facultativa de los titulares de dichos datos, antes de la ejecución de actividades de tratamiento.

11.1.1 Autorización Especial De Datos Personales Sensibles

CEXA informará a través de los diversos medios de obtención de la autorización a todos sus titulares, que en virtud de la ley 1581 de 2012 y demás normas reglamentarias, estos no están obligados a otorgar autorización para el tratamiento de datos sensibles.

En el caso de tratamiento de datos relacionados con la salud, la compañía implementará las medidas necesarias para proteger la confidencialidad de la información.

11.2 TRATAMIENTO DE DATOS PERSONALES DE 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, de conformidad con lo establecido en el artículo 7 de la Ley 1581 de 2012 y cuando dicho Tratamiento cumpla con los siguientes parámetros y requisitos:

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

b) 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 de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

CEXA, en cuanto Responsable y Encargado involucrado en el Tratamiento de los datos personales de niños, niñas y adolescentes, velará por el uso adecuado de los mismos.
Para este fin aplicará los principios y obligaciones establecidos en la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 1074 de 2015 y demás normas complementarias.

Por regla general, en la ejecución de cualquier actividad de tratamiento de datos personales, CEXA se abstendrá de manipular datos cuyo titular sea un menor, a la luz de lo dispuesto en el artículo 7 de la Ley 1581 de 2012.

Excepcionalmente, CEXA requerirá someter a tratamiento datos personales de menores de edad. Cuando ello ocurra, CEXA someterá el tratamiento de los datos de esta naturaleza a las siguientes reglas:

- Respeto del interés superior del menor titular del dato.
- Respeto de los derechos fundamentales del menor titular del dato.
- Autorización emitida por el representante legal del menor titular del dato.

12. PROCEDIMIENTOS PARA EL EJERCICIO DE DERECHOS

Con el fin de garantizar el desarrollo del derecho constitucional de Habeas Data respecto a los derechos de acceso, actualización, rectificación, supresión, y/o revocamiento de la autorización otorgada por parte del Titular, o interesado habilitado legalmente para ello, entre los que se cuentan sus causahabientes y representantes legales, la compañía ha dispuesto procedimientos que lo faciliten.

Así mismo, para la aplicación de estas medidas, todo titular y/o interesado en ejercer los derechos deberá acreditar esta condición mediante copia del documento pertinente y de su documento de identidad, los cuales podrán acreditarse de forma física o digital. En el caso de tratarse de un apoderado, deberá presentarse poder por escrito y debidamente notariado, y acreditar su identidad.

La solicitud para ejercer cualquiera de los derechos incluidos en esta política y derivados de la ley deberá hacerse en soporte escrito ya sea de manera física en las instalaciones de la compañía. o de manera electrónica o digital a través de los siguientes mecanismos:

a) Requerimiento escrito en: Carrera 54 No. 72-142 Piso 6, Barranquilla, Colombia.
b) Correo electrónico a la dirección: info@cexa.com.co
c) Página Web: www.canalextensiaamerica.com en la sección Contáctenos.

La solicitud deberá contener la siguiente información:

a) Nombre del titular, y de sus representantes, de ser el caso.
b) Petición concreta y precisa de información, acceso, actualización, rectificación, supresión y/o revocar la autorización otorgada. En cada caso la petición debe estar razonablemente fundamentada para que CEXA proceda como Responsable de la Base de Datos a dar la respectiva respuesta.
c) Dirección física y/o electrónica para notificaciones.
d) Documentos que soportan la solicitud.
e) Firma de la solicitud por parte del Titular.

La compañía documentará y almacenará las solicitudes, consultas y reclamos realizados por los Titulares de los datos personales o por los interesados en ejercicio de cualquiera de los derechos, así como las respectivas respuestas. Esta información será tratada de acuerdo con las normas de archivo aplicables a la compañía.

12.1 PROCEDIMIENTO PARA LA ATENCION DE SOLICITUDES Y CONSULTAS RELACIONADAS CON EL TRATAMIENTO DE DATOS PERSONALES

Mediante este procedimiento el Titular o quien esté autorizado podrá formular solicitudes y consultas para:

a) Conocer la información personal del Titular que repose en CEXA;
b) Solicitar copia de la autorización otorgada por el Titular a CEXA para tratar sus Datos Personales.

Estas consultas se podrán realizar de forma gratuita una vez cada mes calendario y cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de Datos Personales que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, CEXA sólo podrá cobrar al Titular los 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.

El procedimiento para la atención de las solicitudes y/o consultas sobre los datos personales del Titular es el siguiente:

a) El Titular o quien esté autorizado para ello, podrá formular consultas a CEXA sobre la información personal del Titular a través de los mecanismos mencionados anteriormente.
b) Si la solicitud o consulta estuviera incompleta, CEXA lo comunicará al interesado dentro de los cinco (5) días siguientes a la recepción de la solicitud para que sean subsanadas las fallas y poder proceder a dar trámite a la solicitud. Transcurridos dos (2) meses sin que se presente la información requerida, se entenderá que se ha desistido de la solicitud.
c) CEXA en los casos en los que ostente la calidad de Encargado del Tratamiento, informará tal situación al Titular o interesado en el dato personal, y comunicará la solicitud al Responsable del Tratamiento, con el fin de que éste de respuesta a la solicitud de reclamo presentada. Copia de tal solicitud será enviada al Titular del dato personal o interesado, con el fin de que este último tenga conocimiento sobre la identidad del Responsable del dato personal y obligado principal de garantizar el ejercicio de su derecho.
d) La solicitud o consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma a satisfacción con todos los requisitos mencionados en el ítem anterior.

e) Cuando no fuere posible atender la solicitud o consulta dentro del término antes indicado, CEXA lo informará al interesado, expresando los motivos y señalando la fecha en que se atenderá su consulta, a más tardar dentro de los cinco (5) días hábiles siguientes al vencimiento del primer término.

Los términos antes mencionados pueden variar en caso de que se emitan leyes o reglamentos que establezcan términos inferiores, de acuerdo con la naturaleza el Dato Personal.

12.2 PROCEDIMIENTO PARA LA ATENCION DE RECLAMOS RELACIONADOS CON EL TRATAMIENTO DE DATOS PERSONALES

Mediante este procedimiento el Titular o quien esté autorizado podrá formular reclamaciones para:

a) Actualizar, modificar, rectificar o suprimir los datos del Titular,

b) Revocar la Autorización del Titular para el Tratamiento de Datos

c) Presentar un reclamo cuando considere que existe un presunto incumplimiento de los deberes de CEXA relacionado con el Tratamiento de Datos Personales, de acuerdo con lo previsto en estas Políticas o en la Ley de Protección de Datos Personales y las normas que la complementen o modifiquen.

El Titular podrá revocar la autorización y solicitar la supresión de sus datos cuando: (i) no se respeten los principios, derechos y garantías constitucionales y legales, siempre y cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias al ordenamiento y (ii) en virtud de la solicitud libre y voluntaria del Titular del dato, cuando no exista una obligación legal o contractual que imponga al Titular el deber de permanecer en la base de datos.

Lo anterior, sin perjuicio de las normas que CEXA debe cumplir en materia de retención documental. En consecuencia, CEXA suprimirá los datos o suspenderá su uso cuando a ello haya lugar, respetando las normas sobre conservación documental que le son aplicables

El procedimiento para la atención de los reclamos sobre los datos personales del Titular es el siguiente:

a) El Titular o quien esté autorizado para ello, podrán formular reclamos a CEXA cuando: (i) Considere que la información del Titular contenida en una base de datos debe ser objeto de corrección, actualización o supresión, (ii) Advierta el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley de Protección de Datos, o (iii) Revoque la autorización para el Tratamiento del Titular.

El interesado (el Titular o quien esté autorizado para ello) podrá formular el reclamo a través de los canales mencionados en el ítem anterior del presente documento.

b) El reclamo del interesado debe contener: la identificación del Titular (nombres y apellidos, tipo y número de documento de identidad, dirección y teléfono de contacto y el e-mail (opcional), la descripción de los hechos que dan lugar al reclamo los documentos que soporten su reclamación. En caso de no contar con la anterior información, se entenderá que el reclamo no se encuentra completo.

c) Si el reclamo está incompleto, CEXA solicitará al interesado subsanar las fallas o remitir la información o documentación que se requiera dentro de los cinco (5) días siguientes a la recepción del reclamo en CEXA. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

d) CEXA en los casos en los que ostente la calidad de Encargado del Tratamiento, informará tal situación al Titular o interesado en el dato personal, y comunicará la solicitud al Responsable del Tratamiento, con el fin de que éste de respuesta a la solicitud de reclamo presentada. Copia de tal solicitud será enviada al Titular del dato personal o interesado, con el fin de que este último tenga conocimiento sobre la identidad del Responsable del dato personal y obligado principal de garantizar el ejercicio de su derecho.

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

f) CEXA atenderá el reclamo en un término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo en CEXA. Cuando no fuere posible atender el reclamo dentro de dicho término, el (las) área(s) responsables de dar respuesta al interior de CEXA, informará(n) al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual no podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

12.3 LEGITIMIDAD

Están legitimados para ejercer los derechos establecidos en esta política y los demás reconocidos por la ley, el titular del dato, sus causahabientes y las personas autorizadas por aquel o estos; en los dos últimos casos, se deberá acreditar la calidad cuyo reconocimiento se solicita, a través de mecanismos idóneos.

12.4 VERIFICACIÓN DE LA FACULTAD PARA SOLICITAR O RECIBIR INFORMACIÓN

Para la gestión de la solicitud de consulta o reclamo, el solicitante deberá aportar los siguientes documentos para acreditar su titularidad o la facultad para recibir la información requerida, de acuerdo con los siguientes casos:

Titular: Copia del documento de identidad.

Causahabiente: Documento de identidad, registro civil de defunción del Titular, documento que acredite la calidad en que actúa y copia del documento de identidad del Titular.

Representante legal y/o apoderado: Documento de identidad válido, documento que acredite la calidad en la que actúa (Poder) y copia del documento de identidad del Titular.

12.5 COMPETENCIA

CEXA velará por la protección de los datos personales que reposen en las bases de datos de la compañía y dará trámite a las solicitudes y reclamos de los Titulares para el ejercicio de los derechos de acceso, consulta, rectificación, actualización, supresión y revocatoria a que se refiere la Ley 1581 de 2012 y sus decretos reglamentarios, a través de los canales establecidos.

13. MEDIDAS DE SEGURIDAD

CEXA, 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, CEXA, 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.

A continuación, se exponen las medidas de seguridad implantadas por CEXA que están recogidas y desarrolladas en el DC-084 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (Tablas I, II, III y IV).

TABLA I: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) y bases de datos (automatizadas, no automatizadas)	
Gestión de documentos y soportes	1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable de Administrar las bases de datos para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.
Control de acceso	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado

Incidencias	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.
Personal	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos. 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.
Manual Interno de Seguridad	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.
Manual Interno de Seguridad	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.

TABLA II: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) según el tipo de bases de datos	
Bases de datos no automatizadas	
Archivo	1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta, que permitan el ejercicio de los derechos de los Titulares.
Almacenamiento de documentos	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.
Custodia de documentos	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.
Bases de datos automatizadas	
Identificación y autenticación	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 y caducidad.
Telecomunicaciones	1. Acceso a datos mediante redes seguras.

TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos
Bases de datos no automatizadas

Auditoría	1. Auditoría ordinaria (interna o externa) cada dos meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
Responsable de seguridad	1. Designación de uno o varios Administradores de las bases de datos. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del Responsable del tratamiento en los Administradores de las bases de datos.
Manual Interno de Seguridad	1. Controles periódicos de cumplimiento.
Bases de datos automatizadas	
Gestión de documentos y soportes	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.
Control de acceso	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.
Identificación y autenticación	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados. 2. Mecanismos de cifrado de datos para la transmisión.
Incidencias	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IV: Medidas de seguridad para datos sensibles según el tipo de bases de datos	
Bases de datos no automatizadas	
Control de acceso	1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados. 4. Destrucción que impida el acceso o recuperación de los datos.
Almacenamiento de documentos	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. 2. Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.
Bases de datos automatizadas	

Control de acceso	1. Sistema de etiquetado confidencial.
Identificación y autenticación	1. Mecanismos de cifrado de datos para la transmisión y almacenamiento.
Almacenamiento de documentos	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede 2. Control del registro de accesos por el responsable de seguridad. Informe mensual.
Telecomunicaciones	1. Acceso y transmisión de datos mediante redes electrónicas seguras. 2. Transmisión de datos mediante redes cifrados (VPN).

13.1 COOKIES O WEB BUGS

CEXA puede recolectar información personal de sus Usuarios mientras utilizan la Página Web, la Aplicación o las Páginas Vinculadas (Landing Page). Los usuarios pueden optar por almacenar esta información personal en la página web, la aplicación o en el portal vinculado (Landing Page), con el fin de facilitar las transacciones y los servicios a prestar por parte de CEXA y/o de sus portales vinculados (Landing Page). Por lo que, CEXA utiliza diferentes tecnologías de seguimiento y recopilación de datos como, Cookies propias y de terceros, esta es la herramienta de análisis que ayuda a los propietarios de sitios web y de aplicaciones a entender cómo interactúan los visitantes con sus propiedades. Esta herramienta puede utilizar un conjunto de cookies para recopilar información y ofrecer estadísticas de uso de los sitios web sin identificar personalmente a los visitantes de Google.

Esta información nos permite conocer sus patrones de navegación y ofrecerle servicios personalizados. CEXA podrá utilizar estas tecnologías para autenticarlo, para recordar sus preferencias para el uso de la página web, la aplicación y las páginas vinculadas (Landing Page), para presentar ofertas que puedan ser de su interés y para facilitar transacciones, para analizar el uso de la página web, la aplicación o de las páginas vinculadas y sus servicios, para usarla en el agregado o combinarla con la información personal que tengamos y compartirla con las entidades autorizadas.

Si un usuario no quiere que su información personal sea recogida a través de Cookies, puede cambiar las preferencias en su propio navegador web. No obstante, es importante señalar que, si un navegador web no acepta Cookies, algunas de las funcionalidades de la página web, la aplicación y/o las páginas vinculadas (Landing Page) podrían no estar disponibles o no funcionar correctamente. Puede permitir, bloquear o eliminar las cookies instaladas en su dispositivo mediante la configuración de las opciones del navegador instalado en su dispositivo, así:

- Chrome: https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es

- Microsoft Edge: https://support.microsoft.com/es-es/microsoft-edge/permitir-temporalmente-las-cookies-y-los-datos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c-7c2b-541086362bd2

- Firefox: https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias

- Safari: https://support.apple.com/es-es/HT201265

13.2 ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

CEXA ha identificado riesgos relacionados con el tratamiento de los datos personales y establecidos controles con el fin de mitigar sus causas, mediante la implementación de la Política de Seguridad de la Información. Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

El sistema de gestión de riesgos determinará las fuentes tales como: tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo. Por lo que, para garantizar la protección de datos personales se tendrá en cuenta el tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), tales como:

- Criminalidad: Entendida como las acciones, causadas por la intervención humana, que violan la ley y que están penalizadas por ésta.

- Sucesos de origen físico: Entendidos como los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.

- Negligencia y decisiones institucionales: Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

- CEXA en el programa de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

13.3 CONTROL DE ACCESO

El acceso a la información de datos personales se encuentra restringido al personal que hace uso exclusivo de ellos para lo cual se han establecido perfiles de creación, modificación, eliminación, consulta y administración de las distintas herramientas desde las que se gestionan las bases de datos.

Los usuarios que deben hacer uso de las mismas cuentan con contratos de confidencialidad como una de las principales medidas para salvaguardar la información respectiva.

Así mismo, 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.

13.4 VIDEOVIGILANCIA

CEXA 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 son conservadas por espacio de treinta (30) días. En caso de que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, serán conservadas hasta el momento en que sea resuelta la situación.

El acceso y divulgación de las imágenes será restringido a personas autorizadas por el Titular y/o por solicitud de una autoridad en ejercicio de sus funciones. En consecuencia, la divulgación de la información que se recolecta será controlada y consistente con la ¬finalidad establecida por el Responsable del Tratamiento.

14. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES CON DATOS PERSONALES

Una incidencia es cualquier anomalía que afecte o pudiera afectar la seguridad de las bases de datos o información contenida en las mismas. En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al Oficial de Protección de Datos que adoptará las medidas oportunas frente al incidente reportado.

El Oficial de Protección de Datos Personales informará de la incidencia al comité de ética dentro de los 15 días a partir del conocimiento de esta.

Las incidencias pueden afectar tanto a bases de datos digitales como físicas y generarán las siguientes actividades:

a) Notificación de Incidentes: Cuando se presuma que un incidente pueda afectar o haber afectado a bases de datos con información personal datos personales se deberá informar al Oficial de Protección de Datos Personales quién gestionará su reporte en el Registro Nacional de Bases de Datos.
b) Gestión de Incidentes: Es responsabilidad de cada funcionario, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas

que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de CEXA.

c) Identificación: Todos los eventos sospechosos o anormales, tales como aquellos en los que se observe el potencial de perdida de reserva o confidencialidad de la información, deben ser evaluados para determinar si son o no, un incidente y deben ser reportados al nivel adecuado en la compañía. Cualquier decisión que involucre a las autoridades de investigación y judiciales debe ser hecha en conjunto entre el Oficial de Protección de Datos Personales, el Comité de Ética y la Dirección Jurídica. La comunicación con dichas autoridades será realizada por ellos mismos.

d) Reporte: Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por la compañía, a saber:
info@cexa.com.co o linea.etica@cexa.com.co
Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el Oficial de Protección de Datos Personales, debe ser notificado de forma inmediata. Los empleados deben reportar a su jefe directo y 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 Compañía.
A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún empleado 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, la Dirección Jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.

e) Contención, Investigación y Diagnóstico: El Oficial de Protección de Datos Personales 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 el encargado de la prestación de servicios informáticos de la compañía.
En caso de que se identifique un delito informático, en los términos establecidos en la Ley 1273 de 2009, el Oficial de Protección de Datos Personales y la Dirección Jurídica, reportara tal información a las autoridades de investigaciones judiciales respectivas. Durante los procesos de investigación se deberá garantizar la "Cadena de Custodia" con el fin de preservarla en caso de requerirse establecer una acción legal.

f) Solución: El encargado de la prestación de los servicios informáticos, así como cualquier área comprometida y los directamente responsables de la gestión de datos personales, deben prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades existentes.

g) Cierre de Incidente y Seguimiento: El encargado de la prestación de servicios informáticos conjuntamente con el Oficial de Protección de Datos Personales y las áreas que usan o requieren la información, iniciarán y documentarán todas las tareas de revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad. El Oficial de Protección de Datos Personales preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

h) Reporte de incidentes ante la SIC como autoridad de control: Se reportarán como novedades los incidentes de seguridad que afecten la base de datos, de acuerdo con las siguientes reglas:

- En la parte inferior del menú de cada base de datos registrada en el sistema, se presentan dos (2) opciones para informar las novedades:
- La violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado, deberán reportarse al Registro Nacional de Bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.
- Los líderes de proceso y/o propietarios de activos de información, reportarán de forma interna los incidentes asociados a datos personales ante el Oficial de Protección de Datos Personales, quién dentro del plazo legal procederá a reportarlos ante el Registro Nacional de Bases de Datos

15. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.

De acuerdo a lo estipulado por la Corte Constitucional en sentencia C-748 de 2011, esta prohibición no regirá cuando se trate de:

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

En los casos en los cuales sea necesaria la transferencia de los datos y el país de destino no se encuentre en el listado de países considerados como puertos seguros señalados por la Superintendencia de Industria y Comercio, se deberá gestionar ante el mismo ente una declaración de conformidad relativa a la aprobación para la transferencia internacional de datos personales.

Las transmisiones internacionales de datos personales que se efectúen entre CEXA y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales. Este contrato de transmisión de datos personales deberá suscribirse entre el Responsable y el Encargado para definir el alcance del tratamiento de datos personales bajo su control y responsabilidad, así como, las actividades que el encargado realizará por cuenta del Responsable y las obligaciones del Encargado para con el titular. Adicionalmente, el Encargado deberá cumplir con las siguientes obligaciones y aplicar las normas vigentes en Colombia en materia de protección de datos.

1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan.
2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
3. Guardar confidencialidad respecto del tratamiento de los datos personales.

Corresponderá a la Dirección Jurídica aprobar los acuerdos o contratos que conlleven una transferencia internacional de Datos Personales, atendiendo como directrices los principios aplicables y recogidos en esta política.

16. TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos almacenados en las bases de datos son recolectados y tratados por motivos estrictamente de seguridad, para verificar la identidad personal y realizar control de acceso a los empleados, clientes y visitantes. Los mecanismos biométricos de identificación capturan, procesan y almacenan información relacionada con, entre otros, los rasgos físicos de las personas (las huellas dactilares, reconocimiento de voz y los aspectos faciales), para poder establecer o "autenticar" la identidad de cada sujeto.

La administración de las bases de datos biométrica se ejecuta con medidas de seguridad técnicas que garantizan el debido cumplimiento de los principios y las obligaciones derivadas de Ley Estatutaria en Protección de Datos asegurando además la confidencialidad y reserva de la información de los titulares.

17. PERÍODO DE VIGENCIA DE LAS BASES DE DATOS

La vigencia de la base de datos será el tiempo razonable y necesario para cumplir las finalidades para la cual fue autorizado su tratamiento y de las normas que regulen la materia.

18. REGISTRO NACIONAL DE BASES DE DATOS

De conformidad con el artículo 25 de la Ley 1581 y sus decretos reglamentarios, CEXA registrará sus bases de datos junto con la presente política de tratamiento de Datos Personales, en el Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio, de conformidad con el procedimiento establecido para el efecto por dicha entidad.

El término para registrar las bases de datos en el RNBD será el establecido legalmente. Asimismo, de acuerdo con el artículo 12 del Decreto 886 de 2014, los Responsables del Tratamiento deberán

inscribir sus bases de datos en el Registro Nacional de Bases de Datos en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

19. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

El cumplimiento del marco normativo en Protección de Datos Personales, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para CEXA. Por ello, hemos establecido políticas, lineamientos y procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades de CEXA cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.
Asimismo, garantizamos que en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

En caso de ser necesario suministrar información a un tercero por la existencia de un vínculo contractual, suscribimos contrato de transmisión para garantizar la reserva y confidencialidad de la información, así como, el cumplimiento de la presente Política del tratamiento de los datos, de las políticas y manuales de seguridad de la información y los protocolos de atención a los titulares establecidos en CEXA. En todo caso, adoptamos compromisos para la protección, cuidado, seguridad y preservación de la confidencialidad, integridad y privacidad de los datos almacenados.

20. GESTIÓN DE DOCUMENTOS

Los documentos que contengan datos personales deben ser fácilmente recuperables, es por ello que se debe dejar documentado el lugar donde reposa cada uno de los documentos tanto físicos como digitales, se deben hacer inspecciones a estas rutas de almacenamiento de forma frecuente, se debe garantizar su conservación dejando definido en que soporte y bajo qué condiciones se llevará a cabo esta conservación, teniendo en cuenta condiciones ambientales, lugares de almacenamiento, riesgos a los cuales están expuestos entre otros, el tiempo de retención de los documentos se determina en función de los requisitos legales si aplica, de lo contrario cada organización lo define de acuerdo a sus necesidades, así mismo debe tener clara la disposición final de los mismos, identificando si se recicla, reutiliza, se conserva, se digitaliza entre otros.

Los documentos que tienen que ver con la protección de datos personales deben ser elaborados por personal o una entidad competente para ello, así mismo la organización debe ser quien revise y apruebe todos los documentos y lo deje registrado en la casilla de aprobación de los documentos.

A finde que sean fácilmente trazables, los documentos deberán estar codificados, serán actualizados y modificados por el personal responsable, esta modificación se efectuara siempre y cuando sea necesario, para la eliminación de un documento se debe tener la justificación para ello descrita en el histórico el cual se encuentra en la parte inferior de todos los documentos.

Los documentos tanto físicos como digitales que contengan datos personales, deben ser protegidos por agentes externos o internos que puedan alterar su contenido, siguiendo los lineamientos descritos en el DC-084 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La distribución de los documentos que contengan datos personales la efectuara el responsable del tratamiento, este dejará documentada la evidencia de dicha distribución, donde entre otros se especifique; el tipo de documento y la identificación de la persona a la cual se le entregó la información.

Se deberá designar un responsable de garantizar la confidencialidad de los datos personales de los titulares, este será quien custodie documentos, garantice su protección tanto física como digital, evite alteraciones de la información, así mismo garantizará que los documentos que salgan de su custodia sean identificados y fácilmente trazables.

21. VIGENCIA, VERSIONES Y ACTUALIZACIÓN DE LA POLÍTICA

La presente política rige a partir de la fecha de su firma, el 02 de enero de 2025 y complementa las políticas asociadas con vigencia indefinida.

Los cambios sustanciales en las políticas de Tratamiento que puedan afectar el contenido de la autorización serán comunicados oportunamente a los Titulares a través de los medios habituales de contacto, la página web www.canalextensiaamerica.com y por cualquier otro mecanismo idóneo y eficaz.

ANEXO 1. FINALIDADES DE LAS BASES DE DATOS

BASE DE DATOS ACCIONISTAS

Finalidades

- Finalidades varias - Gestión de estadísticas internas
- Finalidades varias - Procedimientos administrativos
- Gestión contable, fiscal y administrativa - Gestión administrativa

BASE DE DATOS CLIENTES

Finalidades

- Finalidades varias - Atención al ciudadano/cliente (Gestión PQR)/Recepción y gestión de requerimientos internos o externos sobre productos o servicios
- Gestión Técnica y Administrativa – Envío de comunicaciones
- Gestión contable, fiscal y administrativa - Gestión administrativa
- Gestión contable, fiscal y administrativa - Gestión de clientes
- Gestión contable, fiscal y administrativa - Gestión de cobros y pagos
- Gestión contable, fiscal y administrativa - Gestión de facturación
- Gestión contable, fiscal y administrativa - Gestión económica y contable
- Gestión contable, fiscal y administrativa - Gestión fiscal
- Gestión contable, fiscal y administrativa - Históricos de relaciones comerciales
- Gestión contable, fiscal y administrativa - Verificación de datos y referencias
- Gestión contable, fiscal y administrativa - Verificación de requisitos jurídicos, técnicos y/o financieros

BASE DE DATOS EMPLEADOS ACTIVOS

Finalidades

- Gestión contable, fiscal y administrativa - Gestión administrativa
- Recursos humanos - Control de horario
- Recursos humanos - Formación de personal
- Recursos humanos - Gestión de nómina
- Recursos humanos - Gestión de personal
- Recursos humanos - Prestaciones sociales
- Recursos humanos - Prevención de riesgos laborales

BASE DE DATOS EMPLEADOS HISTORICOS

Finalidades

- Finalidades varias - Atención al ciudadano/cliente (Gestión PQR)/Recepción y gestión de requerimientos internos o externos sobre productos o servicios
- Gestión contable, fiscal y administrativa - Gestión administrativa

BASE DE DATOS COLABORADORES DE CONTRATISTAS

Finalidades

- Recursos humanos - Formación de personal
- Recursos humanos - Gestión de trabajo temporal

BASE DE DATOS COLABORADORES DE CONTRATISTAS HISTÓRICO

Finalidades

- Finalidades varias - Atención al ciudadano/cliente (Gestión PQR)/Recepción y gestión de requerimientos internos o externos sobre productos o servicios

BASE DE DATOS JUNTA DIRECTIVA

Finalidades

- Finalidades varias - Gestión de estadísticas internas
- Finalidades varias - Procedimientos administrativos
- Gestión contable, fiscal y administrativa - Gestión administrativa

BASE DE DATOS PRACTICANTES

Finalidades

- Recursos humanos - Control de horario
- Recursos humanos - Formación de personal
- Recursos humanos - Gestión de nómina
- Recursos humanos - Prevención de riesgos laborales

BASE DE DATOS PROCESOS DE SELECCIÓN

Finalidades

- Recursos humanos - Promoción y gestión de empleo
- Recursos humanos - Promoción y selección de personal

BASE DE DATOS PROVEEDORES

Finalidades

- Finalidades varias - Atención al ciudadano/cliente (Gestión PQR)/Recepción y gestión de requerimientos internos o externos sobre productos o servicios
- Finalidades varias - Gestión de estadísticas internas
- Gestión Técnica y Administrativa – Envío de comunicaciones
- Gestión contable, fiscal y administrativa - Gestión administrativa
- Gestión contable, fiscal y administrativa - Gestión de Bienes y Servicios
- Gestión contable, fiscal y administrativa - Gestión de cobros y pagos
- Gestión contable, fiscal y administrativa - Gestión de facturación
- Gestión contable, fiscal y administrativa - Gestión de proveedores y contratistas
- Gestión contable, fiscal y administrativa - Gestión económica y contable
- Gestión contable, fiscal y administrativa - Gestión fiscal
- Gestión contable, fiscal y administrativa - Históricos de relaciones comerciales
- Gestión contable, fiscal y administrativa - Verificación de datos y referencias
- Gestión contable, fiscal y administrativa - Verificación de requisitos jurídicos, técnicos y/o financieros

BASE DE DATOS VIDEO VIGILANCIA

Finalidades

- Seguridad - Seguridad