Política De Protección De Datos Personales Y La Privacidad De La Información Personal de COMPAÑÍA DE RECAUDO E INFORMACION COMERCIAL SAS CORI SAS

1. Objetivo

CORI S.A.S (en adelante CORI), tiene por objeto social complementar al sector financiero y al sector real añadiendo valor a través de servicios que propician crecimiento y estabilidad a las empresas. En tal sentido, CORI comprometida con el respeto y la garantía de los derechos de sus clientes, afiliados, proveedores, colaboradores, subordinados, externos, contratistas, asesores, aliados, entre otros (en adelante "titular o titulares"), adopta la siguiente Política de Protección de Datos Personales y la Privacidad de la Información Personal la cual es de obligatorio cumplimiento, en cada una de las actividades en las que se involucre total o parcialmente, la recolección, el almacenamiento, el uso, la circulación y transmisión de datos personales.

2. Alcance

Cuando el Titular de los datos presta su consentimiento para que estos formen y sean tratados a partir de una base de datos de una organización u empresa, pública o privada, ésta adquiere la obligación de seguir los lineamientos descritos en la normatividad vigente o que la sustituya. La entidad adquiere obligaciones frente al uso, manejo y divulgación de la información, aplicado desde los principios rectores de acceso y circulación restringida y transparencia de la información. El titular ostenta el derecho de conocer, actualizar o suprimir la información objeto de tratamiento de datos. La entidad, como fuente de la información, es el órgano al que se dirige el titular de la información para estos efectos.

En el cumplimiento de la Ley. 1266 de 2008 y Ley 1581 de 2012, el titular puede ejercer en cualquier momento su derecho de conocer, actualizar o eliminar la información suministrada. De conformidad con el artículo 9 del Decreto reglamentario 1377 de 2013 "La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos".

La presente política, será aplicable para cada una de las relaciones contractuales o comerciales que lleguen a ocurrir entre CORI, sus entidades vinculadas y los titulares de la información.

2.1. Base Legal

La presente Política, se desarrolla con el objetivo de dar cumplimiento a los artículos 15 y 20 de la Constitución Política; de los artículos 17, literal k), y 18, literal f), a la Ley Estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la Protección de Datos Personales" ; y el artículo 13 del Decreto 1377 de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012", el Decreto 1074 de 2015 y el Decreto 886 de 2014 que reglamenta parcialmente la ley 1581 de 2012, en lo relativo al Registro Nacional de Bases de Datos. La referida normatividad ha establecido las condiciones mínimas para realizar el tratamiento de los datos personales, y ha consagrado la obligación, en cabeza de los responsables del tratamiento de datos, de desarrollar políticas para el tratamiento de estos, velando por que se dé cabal cumplimiento a las mismas.

Así mismo, se tiene la ley 527 de 1999, que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establece las entidades de certificación, introduciendo así mismo, el concepto de firma electrónica como mecanismo de autenticidad, disponibilidad y confidencialidad de la información.

Finalmente, las disposiciones contempladas dentro de la ley 2300 de 2023 en el marco de ampliar las garantías contempladas en la ley 1581 de 2012 y la efectividad de protección del derecho a la intimidad de los consumidores en lo relativo a la reglamentación de canales autorizados, horarios, periodicidad y condiciones de contacto directo para las gestiones de cobranza, comerciales y publicitaria, de acuerdo con las autorizaciones otorgadas para tales efectos por los titulares.

3. Definiciones

Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de sus datos personales.

Aviso De Privacidad

Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos.

Base De Datos

Conjunto organizado de datos personales que sea objeto de Tratamiento.

Ciberseguridad

Conjunto de protocolos, reglas, métodos, herramientas y leyes que permiten minimizar el impacto de posibles ataques que puede sufrir un sistema informático.

Dato Personal

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato Público

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de Servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado Del Tratamiento

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales, de conformidad con las políticas para el Tratamiento de Datos personales por cuenta del Responsable del Tratamiento.

Entidades Vinculadas

Son sociedades comerciales, empresas y/o patrimonios autónomos, que, a través de un convenio, contrato, mandato y/o cualquier otro vinculo comercial, delegan y/o contratan en CORI la prestación de servicios para el desarrollo de funciones logísticas, administrativas, jurídicas y operacionales. Tales como Reintegra SAS, Negociación de Títulos Net SAS, PRA Group Colombia Holding SAS, Patrimonio Autónomo Reintegra Cartera, los Afiliados del servicio de SEP y ACTIVITY, quienes informaran a los Titulares el vínculo con CORI entre otros.

Registro Nacional De Bases De Datos (Rnbd):

Es el directorio público de las bases de datos sujetas a tratamiento que operan en el país. El registro es administrado por la Superintendencia de Industria y Comercio y es de libre consulta para los ciudadanos.

Responsable Del Tratamiento

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Titular

Persona natural cuyos datos personales sean objeto de Tratamiento.

Tratamiento

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 del Encargado por cuenta del responsable.

4. Responsables

4.1 Responsabilidades

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

Dirección: La Matuna Calle 32 #8-21 Edificio Banco Popular Oficina 1302 en Cartagena, Colombia, email: ernesto@velezbenedetti.com.

Si bien la responsabilidad del tratamiento de los datos recae en CORI en su calidad de responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a sus entidades vinculadas, sus colaboradores, subordinados, aliados, proveedores, contratistas, entre otros.

Cada una de las partes relacionadas a CORI con acceso, directo o indirecto a bases de datos que contienen datos personales deben conocer la Política de Protección de Datos Personales y la Privacidad de la Información Personal, así como las demás políticas de seguridad de la información y ciberseguridad de la organización; y cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Por consiguiente, los trabajadores, colaboradores, subordinados, aliados, proveedores y contratistas de CORI son responsables y/o encargados de la aplicación de esta Política de Protección de Datos Personales y la Privacidad de la Información Personal, en cualquier lugar o entorno en donde se desarrolle la operación determinada. La seguridad de la información corresponde a una función transversal a todos los relacionados a la organización e implica que todos velen por la confidencialidad de los datos a los cuales hayan tenido acceso en razón del vínculo contractual o comercial.

Conforme a lo anterior todos los procesos de CORI en los cuales se reciba, procese y se acceda a la información de titulares tienen un grado de responsabilidad alto respecto de proteger dicha información, contra el mal uso que se dé a la misma y/o divulgación no autorizada por el dueño y/o titular de la información.

El área legal con el apoyo del área de Seguridad de la Información son los responsables de la actualización y divulgación del presente documento a todo el personal.

5. Principios Que Se Tendrán En Cuenta Para El Tratamiento De Datos Personales En CORI

El artículo 4 de la Ley Estatutaria 1581 de 2012 establece los principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley.

En el desarrollo y ejercicio de la presente Política, CORI aplicará, de manera armónica e integral, los siguientes principios:

A). Principio De Legalidad En Materia De Tratamiento De Datos:

El tratamiento a que se refiere la presente política es una actividad regulada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

B). Principio De Finalidad:

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

C). Principio De Libertad:

Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley Estatutaria 1581 de 2012:

• 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.

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 (CORI) o del Encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernen.

F). Principio De Acceso Y Circulación Restringida:

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales. El tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas para la ejecución de los procesos internos dentro de CORI.

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 sólo a los Titulares o terceros autorizados.

G). Principio De Seguridad:

La información sujeta a tratamiento por CORI, 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 a todo personal que tenga acceso, directo o indirecto, a los datos; tanto en los usuarios, como la infraestructura tecnológica y evitar que las personas eventualmente se puedan ver afectadas por lo que sucede en el ciberespacio. 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 Manual 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.

H). Principio De Confidencialidad:

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

5.1 Tratamiento De Datos Personales En CORI

CORI ha obtenido previa y expresamente la autorización de los Titulares para realizar el tratamiento de sus datos personales y de esta forma, recopilar, almacenar, compilar, procesar, distribuir, usar, actualizar, circular, transmitir y/o transferir y dar tratamiento a los mismos directamente, a través de terceros o sus entidades vinculadas (en adelante “empresas autorizadas”).

Estos datos pueden ser recolectados por CORI directamente del Titular por medio de los siguientes mecanismos:

1. Registro de información, para efectos de la prestación del servicio de firma electrónica con validez jurídica.

2. Medios telefónicos, electrónicos (SMS, chat, correo electrónico y demás medios así considerados) físicos y/o personales.

3. Formatos de vinculación.

4. Formatos de registro de asistencia a eventos.

5. Recolección a través de campañas de marketing digital adelantadas por las empresas autorizadas.

6. Registro de información para quejas, reclamos, sugerencias, solicitudes, peticiones, etc.

La información personal no será utilizada o tratada con propósitos diferentes a los aquí manifestados. CORI podrá llevar a cabo el tratamiento de los datos en sus propios servidores o en aquellos provistos por un tercero especializado en la materia y estos podrán estar ubicados en Colombia o en otros países con las respectivas medidas ante incidentes de ciberseguridad. De igual forma, CORI se encuentra comprometida con la confidencialidad y el manejo apropiado de las bases de datos atendiendo a las políticas sobre el tratamiento de la información establecida en nuestra legislación vigente.

5.1.1 Finalidades Del Tratamiento De La Información

La información del Titular se requiere para ser recolectada, consultada, recopilada, evaluada, catalogada, clasificada, ordenada, grabada, almacenada, actualizada, modificada, aclarada, reportada, informada, analizada, utilizada, compartida, circulada, suministrada, suprimida, procesada, solicitada, verificada, intercambiada, retirada, transferida, transmitida divulgada y en general, para efectuar cualquier operación o conjunto de operaciones realizadas por las empresas autorizadas.

Además de las finalidades antes previstas, el tratamiento de la información de los Titulares se diferencia en cuanto a la relación que tenga la persona natural con las empresas autorizadas, de acuerdo con:

5.1.2 Clientes Y Usuarios

1. Prestar de manera adecuada los servicios contratados con CORI.

2. Ser contactado para renovaciones, negociaciones, ofrecimiento de servicios, ser informado e invitado a participar en eventos, capacitaciones, obtención de beneficios.

3. Promocionar, comercializar u ofrecer, de manera individual o conjunta productos y/o servicios propios u ofrecidos en alianza comercial, a través de cualquier medio o canal, o para complementar, optimizar o profundizar el portafolio de productos y/o servicios actualmente ofrecidos, a través del envío de e-mail, mensajes de texto, o a través de cualquier medio análogo y/o digital de comunicación vigente o que se desarrolle posteriormente.

4. Desarrollar actividades comerciales y de mercadeo, tales como análisis de consumo, trazabilidad de marca, envío de beneficios, publicidad, promociones, ofertas, novedades, descuentos, programas de fidelización, investigación de mercado, generación de campañas y eventos de marcas propias o de entidades vinculadas a CORI.

5. Como elemento de análisis en etapas pre-contractuales, contractuales y post-contractuales para establecer y/o mantener cualquier relación contractual, incluyendo como parte de ello, los siguientes propósitos: I. Actualizar bases de datos y tramitar la apertura y/o vinculación de productos y/o servicios con las empresas autorizadas. II. Evaluar riesgos derivados de la relación contractual potencial, vigente o concluida. III. Realizar, validar, autorizar o verificar transacciones incluyendo, cuando sea requerido, la consulta y reproducción de datos sensibles tales como huellas, imagen o voz. IV. Obtener conocimiento del perfil comercial o transaccional del Titular, el nacimiento, modificación, celebración y/o extinción de obligaciones, el incumplimiento de las obligaciones que adquiera con las empresas autorizadas. V. Conocer el estado de las operaciones vigentes activas o pasivas o de cualquier naturaleza o las que en el futuro llegue a celebrar con CORI, con otras entidades financieras o comerciales, con cualquier operador de información o administrador de bases de datos. VI. Prevenir los delitos de lavado de activos, financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva.

6. Validar información con las diferentes bases de datos de CORI, sus entidades autorizadas, bases de autoridades y/o entidades estatales y de terceros tales como operadores de información, empresas prestadoras de servicios públicos y de telefonía móvil, entre otras, para desarrollar las actividades propias de su objeto social principal y conexo y/o cumplir obligaciones legales.

7. Realizar encuestas y/o sondeos de opinión sobre los servicios de CORI.

8. Evaluar la calidad de los servicios.

9. Recopilar información del Usuario respecto de carteras propias o administradas.

10. Actualizar los datos personales de los Titulares de información periódicamente, bien sea directamente o mediante la contratación de terceros que provean este servicio. También, haciendo uso de bases de datos legítimas de terceros, que incluye la base administrada por el Ministerio de Salud y Protección Social, y los datos personales contenidos en bases de datos de Operadores de información financiera, comercial o crediticia y a través de referenciación de terceras personas.

11. Adelantar todas las gestiones requeridas para realizar la cobranza de obligaciones y la recuperación de cartera tanto judicial como extrajudicialmente.

12. Para que los datos personales, comerciales, privados, semiprivados o sensibles recolectados o suministrados por el Titular o terceros puedan ser utilizados como medio de prueba.

13. Realizar consulta y reporte de las obligaciones vigentes o en mora a las centrales de riesgo crediticio legalmente establecidas.

14. Realizar actividades de cobranza, recuperación de cartera, geo-referenciación, estudios estadísticos de comportamiento crediticio, ubicación de deudores a través de interpretación e

interacción de datos de diversas fuentes.

15. Enviar información sobre actividades desarrolladas por las empresas autorizadas, o envío de información que se considere de interés.

16. Hacer estudios de cupo de fianza para los servicios que presta CORI sobre el Titular.

17. Contactar a los Titulares para informar sobre el proceso de cobranza de las obligaciones propias o administradas, informando el estado de las obligaciones e invitando al mismo a la normalización de su obligación.

18. Actualizar las bases de datos de CORI para el logro de un proceso de cobranza efectivo de la cartera propia o administrada.

19. Dar cumplimiento a las obligaciones legales de información a los entes administrativos, así como autoridades judiciales competentes que así lo requieran.

20. Compartir la información con terceros que colaboran con las empresas autorizadas que en el cumplimiento de sus funciones deben acceder en alguna medida a la información, tales como, proveedores del servicio de call y contac center, proveedores del servicio de mensajería, proveedores del servicio de facturación, entidades a nombre de las cuales se realiza la administración integral del Portafolio de Cartera, y se realizan gestiones de cobranza y recuperación de cartera, profesionales del derecho que colaboran con CORI en el desarrollo de su objeto social. En todo caso, esas entidades y personas estarán igualmente sujetas a las mismas obligaciones de confidencialidad en el manejo de la información a que está sujeta CORI con las limitaciones legales impuestas por las leyes aplicables sobre la materia en Colombia.

21. Realizar la consulta y reporte de las obligaciones a los Operadores de Información.

22. Atender y responder las solicitudes, quejas y reclamos que se presenten en el desarrollo de la operación de las empresas autorizadas.

23. Validar su identidad e información en cumplimiento de las políticas internas de las empresas autorizadas.

24. Garantizar el cumplimiento de los protocolos de seguridad de la información.

25. Realizar y cumplir los protocolos de seguridad establecidos por CORI.

26. Adelantar el control y prevención de fraudes, lavado de activos, financiación del terrorismo y/o financiamiento de la proliferación de armas de destrucción masiva.

27. Transmitir y/o Transferir Datos Personales o cualquier dato que haya sido suministrado como consecuencia de la relación contractual con CORI o sus entidades vinculadas, en Colombia o en

el Exterior a un tercero, según lo defina CORI.

28. Validar la identidad personal del Titular, Ofrecer y/o reconocer beneficios, hacer tele mercadeo y/o cobranzas relacionadas con CORI o con sus entidades vinculadas.

5.1.3 Proveedores, Aliados, Contratistas, Terceros

1. Creación y/o actualización de aliados, terceros y/o proveedores, etc., según corresponda.

2. Gestionar toda la Información necesaria para el cumplimiento de las obligaciones contractuales y legales de la ENTIDAD.

3. Como elemento de análisis en etapas pre-contractuales, contractuales y post-contractuales para establecer y/o mantener cualquier relación contractual, incluyendo como parte de ello, los siguientes propósitos: I. Establecer, mantener y profundizar la relación contractual. II. Validar la identificación personal. III) Actualizar la información IV. Evaluar el riesgo. V. Verificar la información brindada, el análisis de referencias comerciales y en general el análisis de toda la información manifestada. VI. Efectuar labores de mercadeo, investigaciones comerciales o estadísticas. VII. Por razones de seguridad.

4. Realizar la Gestión administrativa, de facturación y contable.

5. Realizar el tratamiento de datos sensibles como: ubicación espacial, datos de ordenadores, teléfonos y números celulares, VPN, correo electrónico y otros que se estimen necesarios; que serán utilizados con fines de autenticación e identificación.

6. Suministrar, transmitir, transferir información personal, comercial y financiera para que sea conocida y tratada por las personas naturales o jurídicas que presten sus servicios a las empresas autorizadas en Colombia y/o en el extranjero, cuando esta se justifique dentro del desarrollo normal de la relación comercial.

7. Llevar a cabo las actividades correspondientes en el ámbito del desarrollo normal y ordinario de la relación acordada.

8. Realizar mi georreferenciación de tal manera que garantice que puedo ser contactado efectiva y oportunamente por parte de las empresas autorizadas, para los fines propios de la relación contractual y/o comercial que he establecido.

9. Evaluar la calidad de los bienes o servicios prestados por la parte como Titular de la Información.

5.1.4 Candidatos Y Colaboradores

1. La información de los candidatos, incluida la información contenida en su hoja de vida, se utiliza con el fin de evaluarlos y decidir su ingreso a las empresas autorizadas. Las bases de datos de colaboradores tienen como finalidad, desarrollar las relaciones laborales que existan con estos y hacerlos participes de las actividades previstas por las empresas autorizadas.

2. Realizar el tratamiento de datos sensibles como: historiales clínicos, huellas dactilares o un cálculo sobre ellas, fotografías, imágenes de video, ubicación espacial, datos de ordenadores, teléfonos y números celulares, VPN, correo electrónico, que serán utilizados con fines de autenticación e identificación.

3. Verificar y confirmar la identidad del candidato o colaborador y contactarlo.

4. Adelantar con base en esa información el proceso de selección, conforme a las políticas de las empresas autorizadas.

5. Establecer una relación laboral en el evento de ser el candidato seleccionado.

6. Contactar al mismo para futuros procesos de selección de las empresas autorizadas.

7. Recibir información comercial sobre los productos y/o servicios de las empresas autorizadas.

8. Adoptar medidas tendientes a la prevención de actividades ilícitas.

9. Transferir los datos personales recolectados a otros países, cuando se requiera por la relación laboral.

10. Llevar controles de asistencia a las instalaciones de CORI.

Para el desarrollo de las finalidades previstas en el presente documento CORI podrá contactar al Titular por medio de diferentes mecanismos y/o canales que este autorice, tales como: envío de mensajes de texto, correo físico y/o electrónico, mensajes a través de WhatsApp u otras redes sociales, llamadas telefónicas o cualquier otro medio que la tecnología y la norma permitan y que sea autorizado por el titular.

5.2 Tratamiento De Datos Sensibles

Esta información personal se incluye en una categoría especial por estar relacionada con datos médicos de carácter confidencial, información sobre raza u origen étnico, creencias religiosas, ideología política, sexualidad, condiciones de desplazamiento o calamidad y datos biométricos. Las empresas autorizadas para la prestación de sus servicios requieren la recolección de datos

biométricos como la imagen, la huella y el registro de voz, con la finalidad de realizar el proceso de autenticación de la parte para la posterior emisión de documentos digitales y para ejecutar el correspondiente proceso de firma electrónica. En caso de requerirse este tipo de información para el adecuado desarrollo de las actividades adelantadas por las empresas autorizadas, los Titulares deberán otorgar su autorización expresa, la cual deberá hacerse siempre de manera libre y voluntaria. CORI acepta el carácter facultativo de la respuesta a las preguntas que sean efectuadas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; sin embargo, tales respuestas no podrán ser omitidas cuando los datos que se están requiriendo vayan a ser utilizados en la labor de cobranza dentro del marco legalmente permitido. En ningún momento los datos sensibles se relacionarán en gestiones de cobranza.

5.2.1 Excepciones a la prohibición de datos personales

La información del Titular se requiere para ser recolectada, consultada, recopilada, evaluada, catalogada, clasificada, ordenada, grabada, almacenada, actualizada, modificada, aclarada, reportada, informada, analizada, utilizada, compartida, circulada, suministrada, suprimida, procesada, solicitada, verificada, intercambiada, retirada, transferida, transmitida divulgada y en general, para efectuar cualquier operación o conjunto de operaciones realizadas por las empresas autorizadas.

Además de las finalidades antes previstas, el tratamiento de la información de los Titulares se diferencia en cuanto a la relación que tenga la persona natural con las empresas autorizadas, de acuerdo a:

1. El Titular haya dado a las empresas autorizadas, su consentimiento explícito a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

2. El tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

3. 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;

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

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

5.3 Derechos De Los Titulares

De acuerdo con la legislación colombiana vigente, en particular la Constitución Política y la Ley 1581 de 2012, los Titulares, sus representantes legales o sus causahabientes tienen derecho a:

1. 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;

2. Solicitar prueba de la autorización otorgada a CORI salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la ley Estatutaria 1581 de 2012;

3. Ser informados por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que se le ha dado a sus datos personales;

4. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la normatividad relativa vigente o en la presente Política.

5. 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 CORI ha incurrido en conductas contrarias a la presente Política y en consecuencia con la ley Estatutaria 1581 de 2012, su Decreto Reglamentario 1377 de 2013 y a la Constitución;

6. Acceder en forma gratuita a los datos personales que hayan sido objeto de Tratamiento cada vez que existan modificaciones sustanciales a estas políticas de tratamiento de la información que motiven nuevas consultas.

Para que el Titular ejerza sus derechos podrá contactarse con CORI a través de comunicación escrita dirigida a nuestra área de atención al cliente a la siguiente dirección; Calle 19 No. 7-48 Piso 2° de la ciudad de Bogotá, o al correo electrónico atencion.cliente@CORI.com. La comunicación referida deberá contener todos los datos necesarios y aplicables al derecho de petición para efectos de garantizar la oportuna y efectiva respuesta, acompañada de una descripción clara y precisa de los datos personales respecto de los cuales el Titular busca ejercer sus derechos; así mismo, en el evento de no actuar directamente, el interesado deberá acreditar formalmente la calidad en que actúa.

CORI dará respuesta al peticionario dentro de los términos establecidos por la Ley 1581 de 2012. Es de anotar que mientras el Titular de la información aparezca como deudor de obligaciones de las empresas autorizadas, la información será mantenida y el Titular carecerá de facultades para solicitar la supresión de la información de las bases de datos. Si la solicitud de retiro se hace con

posterioridad a la cancelación total y efectiva de la obligación y/o a finalizada la relación legal o contractual, la eliminación de los datos significará que los mismos no podrán ser accesibles para el desarrollo de las operaciones normales de CORI, sin embargo, podrán mantenerse en sus archivos con fines estadísticos, históricos, conocimiento de sus clientes o atención de requerimiento de autoridades administrativas o judiciales.

5.4 Autorización Del Usuario

Sin perjuicio de las excepciones previstas en la presente política, y conforme a la ley Estatutaria 1581 de 2012 y el Decreto Reglamentario 1377 de 2013, en el Tratamiento se requiere la autorización previa e informada del Titular, así como la ley 2300 de 2023 frente a la protección de la intimidad del Titular, las autorizaciones podrán ser obtenida por cualquier medio físico o electrónico que pueda ser objeto de consulta posterior. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de las empresas autorizadas, en los términos y condiciones recogidos en la misma.

5.5 Casos En Que No Es Necesaria La Autorización

La autorización del Titular no será necesaria cuando se trate de:

1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones administrativas o judiciales.

2. Datos de naturaleza pública;

3. Casos de urgencia médica o sanitaria;

4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

5. Datos relacionados con el Registro Civil de las Personas.

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente Política.

5.6 Suministro De La Información Al Titular Por Parte De CORI

La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

5.7 Deber De Informar Al Usuario

Las empresas autorizadas, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

1. El Tratamiento al cual serán sometidos sus datos personales y la finalidad de este.

2. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

3. Los derechos que le asisten como Titular.

4. La identificación, dirección física o electrónica y teléfono de CORI.

5.8 Deberes De Los Responsables Del Tratamiento

Los responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

2. Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

3. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

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

5. Garantizar que la información que es suministrada sea veraz, completa, exacta, actualizada, comprobable y comprensible.

6. Adoptar las medidas necesarias para que la información suministrada se mantenga actualizada.

7. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado.

8. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

9. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.

10. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

11. Tramitar las consultas y reclamos formulados en los términos señalados en la ley.

12. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.

13. 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.

14. Informar a solicitud del Titular sobre el uso dado a sus datos.

15. 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.

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

5.9 Deberes De Los Encargados Del Tratamiento

Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan la actividad:

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

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

3. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la ley.

4. Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.

5. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados por la ley 1581 de 2012.

6. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley 1581 de 2012, y en especial, para la atención de consultas y reclamos por parte de los Titulares.

7. Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que lo regula la ley 1581 de 2012.

8. Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.

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

10. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

11. 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.

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

5.10 Funciones Y Obligaciones Del Responsable Del Tratamiento

Las obligaciones en materia de seguridad de los datos de CORI son las siguientes:

1. Coordinar e implantar las medidas de seguridad recogidas en las Políticas de Seguridad de la información de la organización.

2. Difundir los documentos referidos entre el personal afectado.

3. Mantener las Políticas de Seguridad de la Información actualizadas y revisadas siempre que se produzcan cambios relevantes en el sistema de gestión de seguridad de la información, el sistema de tratamiento, la organización de la empresa, 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.

4. Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos en el Manual de Seguridad de la Información.

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

6. Autorizar, salvo delegación expresa a usuarios autorizados e identificados, 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.

7. Verificar la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.

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

9. Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctivas oportunamente.

10. Realizar auditorías, internas o externas, para verificar el cumplimiento de las medidas de seguridad de la información y en materia de protección de datos.

5.11 Terceros Y La Información Personal

Las obligaciones en materia de seguridad de los datos de CORI son las siguientes:

1. Coordinar e implantar las medidas de seguridad recogidas en las Políticas de Seguridad de la información de la organización.

2. Difundir los referidos documentos entre el personal afectado.

3. Mantener las Políticas de Seguridad de la Información actualizadas y revisadas siempre que se produzcan cambios relevantes en el sistema de gestión de seguridad de la información, el sistema de tratamiento, la organización de la empresa, 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.

4. Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos en el Manual de Seguridad de la Información.

5. Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante

acceso identificado y contraseña.

6. Autorizar, salvo delegación expresa a usuarios autorizados e identificados, 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.

7. Verificar la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.

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

9. Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctivas oportunamente.

10. Realizar auditorías, internas o externas, para verificar el cumplimiento de las medidas de seguridad de la información y en materia de protección de datos.

5.11.1 Información Proveniente De Terceros

CORI en desarrollo de su objeto social realiza la administración o actúa como proveedor de servicios de terceros, personas naturales y jurídicas pertenecientes al sector financiero, real, industrial, solidario y público, entre otros sectores.

En estos casos CORI desarrolla el papel de encargado de la información, de tal manera que su actuación siempre estará basada en la certeza de que esos terceros cuentan con las autorizaciones necesarias para las finalidades para la cual es entregada la información a CORI. En caso de que la solicitud que se realice por el Titular de los datos o sus causahabientes, recaiga sobre las autorizaciones existentes para el tratamiento de los datos que son recopilados por esos terceros, CORI realizará el traslado de la solicitud a los responsables correspondientes, procurando en toda medida brindar una respuesta adecuada a las necesidades del peticionario, sin embargo, en tales casos CORI, no se hará responsable por el alcance de las autorizaciones otorgadas ni por el contenido de las respuestas que se otorguen a las solicitudes.

5.11.2 Información De Terceros

CORI reitera que la recepción de la información entregada por sus clientes, contratantes y/o terceras personas que contratan a CORI para la prestación de servicios, y teniendo en consideración la ley 1581 de 2012, debe estar precedida por la debida autorización previa y expresa de los Titulares de la información. De esta manera, CORI entiende que quien realiza entrega de información para la realización de sus actividades empresariales como administrador

de obligaciones de cartera y cobranza cuenta con todas las autorizaciones pertinentes de acuerdo con la ley 1581 de 2012 y que las finalidades para las que la entrega han sido plenamente conocidas y aceptadas por el Titular y en ese sentido libera a CORI de cualquier responsabilidad por el uso que le dé a los datos de acuerdo con las finalidades para las cuales se le hace entrega de la información. En todo caso, CORI en desarrollo de sus políticas internas o por orden de autoridad competente podrá requerir las pruebas de tales autorizaciones.

5.12 Funciones Y Obligaciones De Los Terceros Vinculados Con CORI

Todas las personas que sean vinculadas como empleados, proveedores, aliados contratistas y/o cualquier tercero que reciba información de las empresas autorizadas, en delante denominado "Tercero Vinculado", así como aquellos que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de CORI deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

CORI cumple con el deber de mantener la información acerca de la inclusión en los acuerdos de confidencialidad y del secreto empresarial que suscriben, en su caso, los usuarios de sistemas de información y bases de datos de la organización.

Las funciones y obligaciones de los terceros se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la entidad o para la entidad y, específicamente, por el contenido de esta política. Con carácter general, cuando un Tercero Vinculado trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar el acceso a ellos por personas no autorizadas.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en esta política por parte del Tercero Vinculado al servicio de CORI, es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre las partes.

Ahora bien, las obligaciones en materia de seguridad y privacidad de la información por parte de los terceros vinculados a CORI son las siguientes:

1. No comunicar a terceros, salvo expresa autorización, la información que sea de naturaleza reservada o confidencial y cuya divulgación pueda ocasionar perjuicios a la empresa.

2. Cada persona tendrá un usuario y clave de acceso de carácter personal e intransferible para acceder a los sistemas de cómputo, computadores de la empresa o sistemas de información incluyendo el correo corporativo cuando corresponda; dichas claves no podrán darse a conocer a nadie, ni se deberán digitar ante otros trabajadores.

Adicionalmente, todos los Terceros Vinculados deberán atender los siguientes lineamientos:

• Deber de secreto: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula todos los Terceros Vinculados con CORI; en cumplimiento de este deber, los terceros vinculados no pueden comunicar o revelar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de estos.

• Funciones de control y autorizaciones delegadas: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.

• Obligaciones relacionadas con las medidas de seguridad implantadas:

- Acceder a las bases de datos únicamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.

- No revelar información a terceras personas ni a usuarios no autorizados.

- Observar las normas de seguridad y trabajar para mejorarlas.

- No realizar acciones que supongan un peligro para la seguridad de la información.

- No 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 funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse 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 estos.

• 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.

• Deber de custodia de los soportes utilizados: Obliga al usuario autorizado a vigilar y controlar

que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.

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

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

• Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

• Copias de respaldo y recuperación de datos: Debe realizarse copia de seguridad de toda la información de bases de datos personales de la empresa.

• Deber de archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en las Políticas de Seguridad de la Información y en el Manual de Seguridad de la Información.

• Confidencialidad: CORI, vela por que la información que sea considere de carácter confidencial, no sea revelada, divulgada y/ o entregada a terceros bajo ningún medio o modalidad por quienes la conocen, en virtud de un contrato o acuerdo comercial. Para tal efecto se han implementado, medidas de seguridad, tales como la firma de acuerdos de confidencialidad para los empleados, y terceros vinculados con los cuales se comparta información de carácter confidencial.

5.13 Medidas De Seguridad Aplicables Al Trabajo En Casa

Cuando CORI acuerde con sus empleados la prestación de sus servicios de manera no presencial, el empleado dará cabal cumplimiento a las políticas y medidas contenidas en la presente política y tendrá en cuenta las siguientes medidas propias de la labor en la modalidad de trabajo en casa:

• Solo se autoriza el trabajo en casa desde equipos de cómputo asignados por CORI o aquellos que cumplan con requisitos para establecer una comunicación segura a través de VPN a los sistemas de cómputo, computadores de la empresa o sistemas de información de CORI.

• La conexión a los sistemas de cómputo, computadores de la empresa o sistemas de información de CORI únicamente se debe realizar desde la VPN que asigne CORI y/o a través del acceso habilitado por medio de usuario y contraseña (en el caso de aplicativos o portales web) establecidos en la organización.

• Únicamente se autorizará el uso de sistemas de almacenamiento en la nube previamente validados por el área de seguridad de la información.

• Las licencias instaladas en los equipos de cómputo asignados para el trabajo en casa son propiedad de CORI, por tanto, no se autoriza la instalación de otras licencias.

• No se autoriza salida o intercambio de información en medio físico para efectos de trabajo en casa.

• La conexión a los sistemas de cómputo, computadores de la empresa o sistemas de información de CORI, debe realizarse desde sitios seguros, preferiblemente a través de redes domésticas.

• Al retirar un equipo de cómputo propiedad de CORI se debe velar por su cuidado no exponiéndolo, ni abandonándolo en lugares públicos o privados, y en viajes debe siempre tenerlo consigo llevándolo como equipaje de mano y nunca almacenándolo en la bodega de carga.

• CORI realizará monitoreo permanente a los tiempos de navegación y páginas de internet visitadas por los empleados a través del canal de salida a internet establecido en la organización. Así mismo, se podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación en el internet proporcionado por medio de la red de CORI, de acuerdo con la normatividad aplicable.

• Todo uso indebido de la información y del entorno físico es responsabilidad del empleado.

5.14 Medidas Para El Uso De Firma Electrónica

La firma electrónica es una alternativa de identificación en el contexto digital. La firma electrónica es definida como “métodos que permiten identificar a una persona”, tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Así bien, para la solicitud y uso de la firma electrónica por parte de las empresas autorizadas, se

deberá tener en cuenta lo siguiente:

• El Tratamiento sólo podrá ejercerse con el consentimiento, previo, expreso e informado del firmante.

• Los procesos, datos o cualquier tipo de información ligada a la firma electrónica, como dato personal no podrá ser obtenido o divulgado sin previa autorización, o en ausencia de un mandato legal o judicial que releve el consentimiento.

• Los procedimientos para solicitar la autorización se realizarán a más tardar al momento de la recolección de los datos del firmante y se conservará dicha prueba para aportarla cuando éste o un organismo de control la requiera.

Así bien, las empresas autorizadas conforme a lo dispuesto en el Artículo 7 del Decreto 2364 de 2012, deberán requerir la autorización y aceptación para que los códigos, contraseñas (OTP, u otros), datos biométricos o cualquier otro mecanismo dispuesto, constituyan técnicas de identificación personal o autenticación electrónica, apropiadas y confiables, en cumplimiento de los requisitos de firma electrónica para el reconocimiento de autorías y el contenido de los actos o negocios jurídicos que nazcan del vínculo contractual o comercial. Con el objetivo de que la misma sea vinculante y sustituya o reemplace a cabalidad la firma física del Titular, de conformidad con lo previsto en la ley 527 de 1999.

En consecuencia, el firmante deberá autorizar que la firma electrónica o digital según sea el caso, sea almacenada, conservada y consultada en los aplicativos de gestión de las empresas autorizadas con la finalidad de verificar su autenticidad, como también recuperada cada vez que el mismo realice o autorice una transacción o genere cualquier tipo de documentación requerida.

El firmante deberá obligarse a mantener en control y custodia los datos de creación de la firma, actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma y dar aviso oportuno a CORI S.A. o sus entidades autorizadas, sobre cualquier situación que ponga en duda la seguridad de la firma recolectada o que genere reparos sobre la calidad de esta.

5.15 Medidas Aplicables en Relación con la Ley 2300 de 2023 - Protección a la Intimidad

Para efectos de lo aquí dispuesto, se entenderá que hay contacto directo con el titular cuando a través de un canal bidireccional, se tiene comunicación con el titular estableciendo una interacción con este.

COVINCOC informa y socializa que ha establecido los siguientes canales de contacto:

• Teléfono fijo

• Teléfono Celular (SMS - WhatsApp - llamada)

• Correo electrónico

• Correspondencia física

Las gestiones de cobro, comerciales y/o publicitarias que efectúen las empresas autorizadas se llevarán a cabo dando aplicación a los siguientes lineamientos:

1. El titular únicamente será contactado por los canales autorizados por este.

2. Las gestiones de cobranza, comerciales y/o publicitarias se efectuarán de lunes a viernes de 7: 00 a.m. a 7:00 p.m. y los sábados de 8:00 a.m. a 3:00 p.m. Se excluyen de cualquier tipo de contacto domingos y festivos.

3. Una vez establecido un contacto directo con el titular, este no podrá ser contactado mediante varios canales dentro de una misma semana, ni en más de una ocasión durante el mismo día.

4. Únicamente se efectuarán contactos fuera del horario establecido, en más de una ocasión durante el día y/o mediante varios canales en una misma semana, cuando el titular así lo requiera expresamente.

5. Al avalista, codeudor o deudor solidario se le contactará en la misma condición que establece la Ley para el titular.

6. No se realizarán gestiones de contacto respecto de las referencias personales, laborales y/o de cualquier otra índole del titular.

7. Las visitas al domicilio y/o lugar de trabajo del titular únicamente se efectuarán de acuerdo con lo dispuesto en el artículo 6 de la Ley 2300 de 2023.

8. Se ofrecerán al titular alternativas para normalizar sus obligaciones de acuerdo con su situación financiera sin indagar respecto de los motivos del incumplimiento.

• CORI habilitará y dispondrá del siguiente mecanismo para modificar en cualquier momento los canales autorizados: Ingresando a www.corisasabogados.com.

• La actualización de canales autorizados se hará efectiva a partir del lunes de la semana siguiente a aquella en la que se haya efectuado el registro exitoso de la actualización. En caso de no hacer elección, el titular está de acuerdo con que CORI utilice los canales autorizados habituales y existentes.

5.16 Medidas De Seguridad Aplicables A Terceros Vinculados (Proveedores, Contratistas O Aliados) De CORI

• CORI identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

• Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

• Los terceros vinculados podrán acceder en forma remota a los activos tecnológicos de CORI a través de herramientas tales como VPN, cuando ello fuere necesario para el cumplimiento de las obligaciones que emanan del contrato respectivo. Dicho acceso será autorizado por el área de Seguridad de la Información previa verificación de los requisitos tecnológicos de seguridad que salvaguarden la integridad y confidencialidad de CORI.

• Se tendrá un registro de los accesos que se han realizado a través de las herramientas establecidas por CORI para efectos de trazabilidad y posterior revisión en caso de ser requerido.

• Para asegurar que los terceros vinculados que prestan servicios en el tratamiento de información de propiedad de CORI cuenten con estándares y niveles adecuados en materia de seguridad, CORI se reserva el derecho de solicitar evidencia de la ejecución de auditorías independientes relacionadas a riesgo tecnológico, control interno, o auditorías de certificación relacionados con dicha materia, los que para cualquier efecto serán facilitados de manera temporal y con el objeto de revisar el alcance del trabajo realizado y el detalle de los resultados obtenidos.

5.17 Veracidad Y Cambios En La Información Suministrada

La información compartida con CORI debe ser completa, actual y veraz, resultando de entera responsabilidad de quien la otorga. Toda modificación en la Información suministrada a la entidad deberá ser notificada a CORI dentro de los cinco (5) días hábiles siguientes al acontecimiento de los hechos que condujeren a la modificación de los datos, a través del canal dispuesto para el efecto.

5.18 Medidas Que Adoptará CORI

CORI, adoptara las medidas técnica humanas y administrativas que sean necesarias para proteger y otorgar la seguridad a la información, evitando su adulteración, perdida, consulta u acceso no autorizado tanto internamente como desde el ciberespacio.

5.18.1 Seguridad, Filmaciones Y Comunicaciones

CORI dentro de sus políticas de calidad, seguridad, monitoreo de sus actividades, controles de entrada y salida de sus oficinas y actualización o complemento de la información mantenida en sus bases de datos, realizará grabaciones de audio y video en sus oficinas y sitios comunes de CORI. Tales grabaciones tendrán una duración en los archivos de CORI de un máximo de 5 años para posteriormente ser objeto de borrado o destrucción, salvo que deba conservarlos para efecto de dar cumplimiento a normas vigentes o deberes contractuales. Igualmente, CORI hará uso de las tecnologías de la información para la remisión de diversas comunicaciones tales como el envío de extractos de cuenta, certificaciones, comunicaciones de interés y avisos de reporte a los Operadores de Información.

CORI como parte de su estrategia de comunicación tienen a disposición de sus clientes, proveedores, aliados, colaboradores, contratistas y otros, la página web www.corisasabogados.com, en la cual podrán ser publicadas imágenes, referencias, artículos o comunicaciones de los empleados de CORI, sus clientes o sus familias. En esa medida CORI se compromete a revisar cuidadosamente la información de tal forma que de ninguna manera se atente contra la dignidad, intimidad o buen nombre de ninguna de las personas que podrán aparecer en las publicaciones. La entrega de información por parte de los Titulares en cualquier forma no trasmite a CORI la propiedad intelectual o los derechos morales sobre la misma. Los derechos de propiedad intelectual seguirán siendo de los Titulares y si incluye cualquier tipo de información personal correspondiente a terceros, como es el caso de la entrega de referencias, éste tendrá que asegurarse de contar con todas las autorizaciones por parte de su Titular, de tal manera que CORI no se hará responsable por ninguno de los contenidos que le sean entregados, aunque si se reserva los derechos para utilizarlos o eliminarlos de acuerdo con sus políticas de privacidad. De otra parte, CORI está comprometida para efectuar un adecuado uso y tratamiento de los datos personales de los Titulares, con el fin de evitar al máximo el acceso no autorizado a terceros que permita conocer o vulnerar, modificar, divulgar y/o destruir la información que reposa en las bases de datos de CORI.

CORI cuenta con protocolos de seguridad y acceso a nuestros sistemas de información, almacenamiento y procesamiento, incluidas medidas físicas y lógicas de control de riesgos de seguridad que provienen de la acción humana o de ambientes en el ciberespacio. En el caso que el Titular suministre algún tipo de información a través del portal web o internet, el mismo es consciente que conoce y acepta que ninguna transmisión por internet es absolutamente segura, ni puede garantizarse dicho extremo, por lo tanto, asume y conoce que eventualmente podrá generarse un riesgo de vulnerabilidad. Así mismo, CORI cuenta con mecanismos de seguridad acordes con los servicios que ofrece; no obstante, lo anterior, CORI no se responsabiliza por cualquier consecuencia derivada del ingreso fraudulento por parte de terceros a la base de datos

y por alguna falla técnica en el funcionamiento que sobrepasen las actividades desarrolladas con la debida diligencia.

5.19 Revelación De La Información

El USUARIO, con la aceptación de la presente política de privacidad, declara conocer que CORI, puede suministrar esta información a sus filiales y a las entidades judiciales o administrativas y demás entidades del Estado que, en ejercicio de sus funciones, soliciten esta información.

5.20 Modificaciones A Las Políticas

CORI se reserva el derecho de modificar la Política de Protección de Datos Personales y la Privacidad de la Información Personal, en cualquier momento y de manera unilateral. Para el efecto informará cualquier cambio sustancial por medio de un aviso en su página web o en cualquier otro medio que considere pertinente. En caso de no estar de acuerdo por razones válidas y que se constituyan en una justa causa con las nuevas políticas de manejo de la información personal, los Titulares de la información o sus representantes podrán solicitar a CORI el retiro de su información a través del medio indicado anteriormente, sin embargo, no se podrá solicitar el retiro de los datos mientras se mantenga un vínculo de cualquier orden con CORI. El uso permanente de los servicios con CORI o no desvinculación de estos por el Titular después de la notificación de la nueva política de privacidad constituye la aceptación de la misma por parte del mismo.

5.21 Ámbito De Aplicación

La presente política se publicó y entró en vigencia a partir del 4 de diciembre del 2013 para todos los colaboradores, proveedores, contratistas y terceras partes, que tengan acceso a la información, a los sistemas, procesos y equipos utilizados dentro del desarrollo del trabajo perteneciente a CORI a partir de esta misma fecha.

Toda interpretación, actuación judicial o administrativa derivada del tratamiento de los datos personales que conforman las bases de datos de CORI y la presente declaración de privacidad estará sujeta a las normas de protección personal establecidas en la República de Colombia y las autoridades administrativas o jurisdiccionales competentes para la resolución de cualquier inquietud, queja o demanda sobre las mismas serán las de la República de Colombia.