

POLÍTICA DE TRATAMIENTO DE DATOS

RAZÓN SOCIAL E IDENTIFICACIÓN DE RESPONSABLE TRATAMIENTO DE DATOS

VC@SOFT S.A.S, que en adelante se denominará LA EMPRESA, sociedad comercial identificada con NIT. 830.086.348-8 y creada por escritura pública No. 0000761 de Notaría 39 de Bogotá D.C. el 10 de Mayo de 2001 y registrada en Cámara de Comercio, fecha de matrícula: 15 de Mayo de 2001.

En consideración a lo anterior, VC@SOFT realiza la protección de datos personales de sus clientes, trabajadores y ex trabajadores, proveedores o contratistas en el marco de las relaciones pre-contractuales, contractuales y pos-contractuales con VC@SOFT, por lo cual se ha desarrollado y adoptado esta Política de Tratamiento de datos personales con la finalidad de proteger, respetar e informar los derechos de los Titulares de los datos que encuentran en su posesión y control.

DOMICILIO Y DIRECCIÓN:

LA EMPRESA tiene su domicilio en:

Dirección del domicilio principal	Calle 100 No. 17A 36 Of. 301
Municipio	Bogotá D.C.
Teléfono comercial	(601) 6219348
Correo electrónico	habeasdata@vc-soft.com

DEFINICIONES

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus Datos Personales, mediante la cual se le informa acerca de la existencia de las Políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.
- **Base de Datos:** Conjunto organizado de Datos Personales que sea objeto de Tratamiento.
- **Clientes:** Persona natural o jurídica, pública o privada con los cuales LA EMPRESA tiene una relación comercial.
- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables..
- **Datos personales sensibles:** son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **Datos personales privados:** son datos que por su naturaleza íntima o reservada sólo interesan a su Titular y para su tratamiento requiere de su autorización expresa. Por ejemplo: Nivel de escolaridad, libros de los comerciantes, entre otros.
- **Datos semiprivados:** Aquellos que no poseen una naturaleza íntima, reservada ni pública, y cuyo conocimiento o divulgación puede interesar tanto a su titular como a cierto sector, grupo de personas o a la sociedad en general. Entre los ejemplos se encuentran los datos financieros, crediticios, de ubicación, números de teléfono y direcciones de correo electrónico.
- **Datos personales públicos:** son aquellos tipos de datos personales que las normas y la Constitución han determinado expresamente como públicos y, para cuya recolección y tratamiento, no es necesaria la autorización del Titular de la información. Por ejemplo: estado civil de las personas, datos contenidos del RUNT, datos contenidos en sentencias judiciales ejecutoriadas, entre otros.
- **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. En los eventos en que el Responsable no ejerza como Encargado de la Base de Datos, se identificará expresamente quién será el Encargado.
- **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.

- **Reclamo:** Solicitud del titular del dato o de las personas autorizadas por éste o por la Ley para corregir, actualizar o suprimir sus datos personales o para revocar la autorización en los casos establecidos en la Ley.
- **Titular:** Persona natural cuyos Datos Personales sean 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:** Cualquier operación o conjunto de operaciones sobre Datos Personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

OBJETIVOS DE LA POLÍTICA

La presente Política de Tratamiento de Datos Personales tiene como propósito definir los criterios y lineamientos corporativos bajo los cuales LA EMPRESA realiza la recolección, almacenamiento, uso, circulación, supresión y protección de la información personal alojada en sus bases de datos y archivos físicos o digitales. Su implementación garantiza el ejercicio del derecho constitucional al Habeas Data de los titulares, en estricto cumplimiento de los artículos 15 y 20 de la Constitución Política de Colombia, la Ley Estatutaria 1581 de 2012, la Ley 1266 de 2008 (modificada por la Ley 2157 de 2021 - Borrón y Cuenta Nueva), el Capítulo 25 del Decreto Único Reglamentario 1074 de 2015 (que integra los Decretos 1377 de 2013 y 886 de 2014), el Decreto 620 de 2020, la Circular Externa 005 de 2017 y la Sentencia C-748 de 2011 de la Corte Constitucional.

ALCANCE DE LA POLÍTICA

Esta política aplica para toda la información personal registrada en las bases de datos de La EMPRESA, quien actúa en calidad de responsable del tratamiento de datos personales. Así mismo establece los criterios que la EMPRESA ha incorporado para el tratamiento de los datos personales, los mecanismos para que los titulares puedan ejercer sus derechos, las finalidades, las medidas de seguridad, y otros aspectos relacionados con la protección de la información personal.

La presente Política de tratamiento de datos personales está dirigida a cualquier titular de la información o aquel que actúe como su representante legal y del cual la EMPRESA haya requerido información personal para el desarrollo de alguna actividad.

PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS PERSONALES

En todo tratamiento de datos personales que realice LA EMPRESA se aplicarán, los principios consagrados en el Régimen General de Protección de Datos Personales Colombiano, en especial los siguientes:

- **Principio de Legalidad:** Para el Tratamiento de datos personales se aplican las normas del ordenamiento jurídico colombiano relativas al Régimen General de Tratamiento de Datos Personales y las contenidas en la presente política.
- **Principio de Finalidad:** El tratamiento dado por LA EMPRESA a los datos personales que trata, obedecen a las finalidades establecidas en la presente política, las cuales están en armonía con el ordenamiento jurídico colombiano. En lo no regulado en la presente política se aplicarán las normas de carácter superior que la reglamenten, adicionen, modifiquen o deroguen.
- **Principio de Libertad:** La recolección de los Datos Personales sólo podrá ejercerse con la autorización, previa, expresa e informada del Titular de los datos personales.
- **Principio de Veracidad o Calidad:** La información sujeta al Tratamiento de Datos Personales debe ser veraz, completa, actualizada, comprobable y comprensible.
- **Principio de Transparencia:** LA EMPRESA garantiza que el titular de los datos personales puede obtener información sobre sus datos en cualquier momento y sin restricciones de acuerdo a los procedimientos descritos en la presente política.
- **Principio de Acceso y circulación restringida:** El Tratamiento de datos personales únicamente podrá realizarse por las personas autorizadas por el Titular y/o por las personas previstas en la Ley.
- **Principio de Seguridad:** Los Datos Personales sujetos a Tratamiento se manejarán adoptando todas las medidas de seguridad que sean necesarias para evitar su pérdida, adulteración, consulta, uso o acceso no autorizado o fraudulento.
- **Principio de Confidencialidad:** Todos los funcionarios que trabajen en LA EMPRESA están obligados a guardar reserva sobre la información personal a la que tengan acceso con ocasión de su trabajo en LA EMPRESA.

Para ampliación de estos principios, puede consultarse la Ley 1581 de 2012 y el Decreto 1377 de 2013, así como las demás disposiciones normativas que los modifiquen, aclaren, complementen o deroguen.

TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS Y SU FINALIDAD

LA EMPRESA, actuando en calidad de Responsable del Tratamiento de Datos Personales, para el adecuado desarrollo de sus actividades comerciales, así como para el fortalecimiento de sus relaciones con terceros, recolecta, almacena, usa, circula y suprime Datos Personales correspondientes a personas naturales con quienes tiene o ha tenido relación, tales como, sin que la enumeración signifique limitación, trabajadores y familiares de éstos, accionistas, consumidores, clientes, distribuidores, proveedores, acreedores y deudores, para los siguientes propósitos o finalidades.

El tratamiento de los datos personales de la persona con la cual LA EMPRESA tuviere establecida o estableciera una relación, permanente u ocasional, se realizará en el marco legal que regula la materia. En todo caso, los datos personales podrán ser recolectados y tratados en los siguientes casos:

- Desarrollar el objeto social de LA EMPRESA conforme a sus estatutos legales.
- Cumplir las normas aplicables, tributarias y comerciales.
- Uso de información, medios audiovisuales informáticos y técnicos para la realización de actividades de publicidad o marketing de la EMPRESA.
- Actividades de vigilancia y seguridad de la empresa y de las personas que accedan a sus instalaciones o sus sistemas de información.
- Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia laboral y de seguridad social, entre otras, aplicables a ex-empleados, empleados actuales y candidatos a futuro empleo.
- Realizar encuestas relacionadas con los servicios o bienes de LA EMPRESA.
- Remitir información comercial de LA EMPRESA.
- Desarrollar programas conformes con sus estatutos.
- Cumplir todos sus compromisos contractuales, legales y reglamentarios de la empresa.
- Administrar y operar, directamente o por conducto de terceros, los procesos de selección y vinculación de personal, incluyendo la evaluación y calificación de los participantes y la verificación de referencias laborales y personales, y la realización de estudios de seguridad.
- Desarrollar las actividades propias de la gestión de Recursos Humanos dentro de LA EMPRESA, tales como nómina, afiliaciones a entidades del sistema general de seguridad social, actividades de bienestar y salud ocupacional, ejercicio de la potestad sancionatoria del empleador, entre otras;
- Realizar los pagos necesarios derivados de la ejecución del contrato de trabajo y/o su terminación, y las demás prestaciones sociales a que haya lugar de conformidad con la ley aplicable;
- Contratar beneficios laborales con terceros, tales como seguros de vida, gastos médicos, entre otros.
- Notificar a contactos autorizados en caso de emergencias durante el horario de trabajo o con ocasión del desarrollo del mismo.

- Coordinar el desarrollo profesional de los empleados, el acceso de los empleados a los recursos informáticos del empleador y dar soporte para su utilización;
- Planificar actividades empresariales.
- Realizar el proceso de vinculación formal, verificación de idoneidad, estudios de cumplimiento normativo y gestión de la relación contractual.
- Consultar, verificar y monitorear a titulares (empleados, clientes, proveedores y aliados) en listas restrictivas, vinculantes e informativas, nacionales e internacionales.
- Prevenir, detectar y gestionar riesgos asociados al Lavado de Activos, Financiación del Terrorismo, Proliferación de Armas de Destrucción Masiva (LA/FT/PADM) y actos de corrupción o transnacionales, en cumplimiento de los alineamientos del sistema SAGRILAF de la compañía.

CONSERVACIÓN, RETENCIÓN Y SUPRESIÓN DE DATOS PERSONALES

LA EMPRESA conservará la información personal de los titulares registrada en sus archivos físicos y digitales de acuerdo con los principios de temporalidad, necesidad, razonabilidad y caducidad.

Algunos criterios para la conservación incluyen:

- **Sustento Operativo y Contractual:** Los datos serán conservados mientras permanezca vigente la relación legal, comercial, laboral o de prestación de servicios entre el Titular y LA EMPRESA, o mientras subsista la finalidad para la cual fueron recolectados.
- **Cumplimiento Legales y Contables:** Una vez finalizada la relación contractual, ciertos datos serán conservados durante los términos exigidos por la legislación colombiana (comercial, tributaria, contable, laboral y de seguridad social).
- **Defensa Legal:** Se mantendrá la información necesaria durante los plazos de prescripción de acciones legales para la atención de posibles reclamos, litigios o requerimientos de autoridades.

Finalizado el término de conservación o cuando se cumpla la finalidad del tratamiento y siempre que no exista un deber legal o contractual de permanecer en la base de datos, LA EMPRESA procederá a la supresión, destrucción o anonimización irreversible de la información tanto en soporte físico como en sus servidores locales y repositorios en la nube.

TRATAMIENTO DE DATOS SENSIBLES

Los datos sensibles recolectados serán tratados con las siguientes finalidades:

Datos de Salud:

- Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia de seguridad y salud en el trabajo.
- Trámite de requerimientos por parte de entidades como IPS, EPS, ARL.
- Cumplir con los requisitos de pago de prestaciones sociales.
- Cumplir con los protocolos de bioseguridad exigidos por el ministerio de salud en concordancia con la prevención del COVID-19.
- Cumplir con los requisitos de gestión de riesgos laborales.
- Cumplir con la declaración y pago de aportes de seguridad social.
- Adelantar la gestión de riesgos laborales y la prevención y protección del recurso humano ante enfermedades y accidentes del ámbito laboral.
- Realizar la verificación de riesgo de salud.

Como regla general, LA EMPRESA no realizará el tratamiento de datos sensibles, salvo en las situaciones expresamente exceptuadas por la ley y cuando concurran las siguientes condiciones:

1. **Autorización Explícita:** Se informará de manera previa y expresa al titular que la entrega de información sensible es de carácter totalmente facultativo y opcional.
2. **Información de la Finalidad:** Se informará al titular de forma transparente la finalidad específica y el uso exclusivo que se le dará a sus datos sensibles, por ejemplo, gestión de la salud ocupacional en el marco del SG-SST.
3. **Excepciones Ley 1581 de 2012:** El tratamiento se realizará cuando sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado, o cuando sea ejecutado en el curso de actividades legítimas con las debidas garantías por parte de la organización.

TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES

En LA EMPRESA el tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública y su tratamiento cumpla con los siguientes parámetros y requisitos exigidos por la ley:

- **Interés superior:** Que las actividades de tratamiento respondan y respeten de manera prioritaria el interés superior de los niños, niñas y adolescentes.
- **Derechos fundamentales:** Que se asegure y garantice el respeto absoluto de sus derechos fundamentales.

Parágrafo: Una vez verificados y cumplidos los requisitos anteriores, el representante legal del menor de edad otorgará la respectiva autorización. Este consentimiento se dará previo ejercicio

del derecho del menor a ser escuchado, opinión que será debidamente valorada por la compañía teniendo en cuenta la madurez, autonomía y capacidad del niño, niña o adolescente para comprender el asunto.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS

LA EMPRESA solicitará de manera libre, previa, expresa y debidamente informada, la autorización por parte de los titulares de los datos personales y para ello generará mecanismos idóneos garantizando para cada caso que sea posible verificar el otorgamiento de dicha autorización. La misma, podrá constar en cualquier medio, bien sea un documento físico, digital, electrónico o en cualquier formato que garantice su posterior consulta a través de herramientas técnicas, cumpliendo con los requisitos establecidos en la Ley.

Autorización especial para el tratamiento de datos sensibles

LA EMPRESA únicamente realizará operaciones o tratamiento de datos sensibles cuando cuente con la autorización previa, explícita e informada del titular. Para la recolección de este tipo de datos se cumplirán rigurosamente los siguientes requisitos:

- La autorización debe ser explícita y verificable.
- Se debe informar de manera clara al Titular que no está obligado a autorizar el tratamiento de dicha información, dado su carácter estrictamente facultativo.
- Se debe informar de forma explícita y previa al Titular cuáles de los datos que se recolectarán tienen el carácter de sensibles y la finalidad específica de su uso (por ejemplo, registros biométricos de acceso o gestión de la salud ocupacional).

Autorización tratamiento de datos niños, niñas y adolescentes

En el Tratamiento de datos personales de niños, niñas y adolescentes se asegurará el respeto a los derechos de los menores de edad. LA EMPRESA podrá requerir el tratamiento de datos personales de menores de edad para dar cumplimiento a aspectos legales como: I) El artículo 32 de la Ley 789 de 2002 relacionado con la obligación de adelantar la vinculación de aprendices y II) El derecho de los afiliados al Sistema de Seguridad Social de afiliarse a cualquier pariente dentro del tercer grado de consanguinidad o a cualquier menor de 12 años (sea o no pariente) siempre y cuando dependa económicamente.

En caso de requerir la recolección directa de datos personales de niños, niñas y adolescentes, LA EMPRESA solicitará la autorización de tratamiento con el consentimiento informado de los padres o adultos responsables de los menores de edad.

LA EMPRESA velará por el uso adecuado y la protección prevalente de los derechos fundamentales de los niños, niñas y adolescentes, asegurando el respeto estricto a su interés superior. Por regla general, el suministro de datos de NNA tiene un carácter estrictamente

facultativo y opcional. No obstante, LA EMPRESA podrá requerir el tratamiento de datos de menores de edad únicamente en los siguientes casos de excepción legal y corporativa:

- **Cumplimiento de Obligaciones Laborales y Seguridad Social:** Para la inscripción de dependientes al Sistema de Seguridad Social Integral y Cajas de Compensación Familiar (de acuerdo con el derecho de los afiliados de vincular a sus familiares o menores a cargo), así como para la gestión de programas de bienestar corporativo.
- **Vinculación de Aprendices:** En desarrollo de la Ley 789 de 2002 (artículo 32) para el cumplimiento de la cuota de aprendizaje de menores aptos según la legislación laboral.

DERECHOS DEL TITULAR DE LA INFORMACIÓN

De acuerdo con lo prescrito por la normatividad vigente aplicable en materia de protección de datos, los titulares de los datos personales tienen derecho a:

- Acceder, conocer, actualizar y rectificar sus datos personales frente a la EMPRESA en su condición de responsable 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.
- Solicitar prueba de la autorización otorgada a la EMPRESA para el tratamiento de datos, mediante cualquier medio válido, salvo en los casos en que no sea necesaria la autorización.
- Ser informado por LA EMPRESA, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y en las demás normas que la modifiquen, adicionen o complementen, previo trámite de consulta o requerimiento ante LA EMPRESA.
- Revocar la autorización o solicitar la supresión del dato.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, al menos una vez cada mes calendario, y cada vez que existan modificaciones sustanciales de la presente política que motiven nuevas consultas.
- Abstenerse de responder las preguntas sobre datos sensibles. Tendrán carácter facultativo las respuestas que versen sobre datos sensibles o sobre datos de las niñas y niños y adolescentes.

Estos derechos podrán ser ejercidos por:

- El titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición LA EMPRESA.
- Los causahabientes del titular, quienes deberán acreditar tal calidad.
- El representante o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Otro a favor o para el cual el titular hubiere estipulado.

RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

VCSOFT designará una persona para desempeñar el rol de Oficial de Tratamiento de Datos Personales, con el propósito de velar y garantizar el uso adecuado de la información suministrada en las bases de datos. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al Responsable del Tratamiento sobre una determinada base de datos. Adicionalmente, cada una de las áreas de VCSOFT apoyará la gestión del Oficial de Protección de Datos.

Las responsabilidades asignadas al Oficial de Protección de Datos Personales, además de todas aquellas que generalmente establecen las leyes de protección de datos personales vigentes, son las siguientes:

- Supervisar y auditar continuamente el tratamiento, flujo y almacenamiento de los datos personales y sensibles en todas las áreas y plataformas de la empresa.
- Asesorar y capacitar a los empleados, equipos de desarrollo y directivos sobre sus obligaciones legales y las mejores prácticas en el manejo y protección de la información privada.
- Atender y gestionar de manera oportuna los requerimientos, quejas y solicitudes de los titulares de los datos frente al ejercicio de sus derechos.
- Informar y orientar a la alta dirección y a los líderes de proyectos sobre el impacto y los riesgos en la privacidad de los datos ante la implementación de nuevas iniciativas de negocio o soluciones tecnológicas.
- Evaluar el nivel de riesgo sobre la privacidad de la información frente a nuevas vulnerabilidades o amenazas tecnológicas.
- Participar activamente en los protocolos de respuesta a incidentes de seguridad, liderando la clasificación, el análisis de impacto y la notificación legal obligatoria en caso de presentarse una fuga, alteración, pérdida o acceso no autorizado a datos personales.
- Garantizar que las políticas del SGSI referidas al ciclo de vida del dato, se ejecuten en estricto cumplimiento con las regulaciones aplicables.
- Colaborar estrechamente con el CISO y el Líder de Seguridad en la realización de Evaluaciones de Impacto relativos a la Protección de Datos (**EIPD**).
- Monitorear los acuerdos de nivel de servicio (SLA) y las auditorías de seguridad a terceros y proveedores, asegurando que los contratistas mantengan los mismos estándares de protección y confidencialidad exigidos por VCSOFT para el tratamiento de datos.

El oficial de protección de datos entregará a la Gerencia General, de manera semestral, un informe detallado sobre el estado y avance del programa de protección de datos personales.

Transferencias y transmisiones para tratamiento por terceros de datos personales suministrados a LA EMPRESA

La aceptación de la presente política implica para el titular de los datos personales la aceptación de la posibilidad que tiene LA EMPRESA, respetando en todo momento las disposiciones legales que regulan la materia, para transmitir o transferir la totalidad de los datos del titular a terceros en el país o en el exterior.

A su vez, LA EMPRESA se compromete a informar a los terceros, los parámetros bajo los cuales se ha concedido la autorización y el debido respeto que debe hacerse de la presente política, informando a los terceros que sólo podrán hacer uso de dichos datos y/o información mientras subsista el vínculo legal o contractual con LA EMPRESA, única y exclusivamente, para los usos expresamente definidos por ésta.

GESTIÓN DE INCIDENTES DE SEGURIDAD Y BRECHAS DE INFORMACIÓN

Se considera incidencia cualquier anomalía que afecte o pueda afectar la seguridad de las bases de datos de VCSOFT que contienen datos personales sensibles. Ante una eventualidad, todo usuario debe notificar al Oficial de Protección de Datos Personales, quien registrará el evento detallando:

- Tipo y fecha del incidente.
- Fecha de conocimiento y causal.
- Información comprometida, tipo de datos y cantidad de titulares afectados.

a. Notificación y reporte

Todo colaborador, contratista o tercero debe reportar oportunamente cualquier evento sospechoso o vulnerabilidad. En caso de pérdida o divulgación no autorizada de datos sensibles o confidenciales, se debe notificar inmediatamente al correo dispuesto por la empresa para este fin.

b. Identificación y evaluación

Los eventos reportados se evaluarán para confirmar el incidente. Si se determina la existencia de un delito informático, la Gerencia y El área de Seguridad de la Información de VCSOFT definirán las acciones legales o reportes ante las autoridades competentes.

c. Contención e investigación

Se documentará el proceso de gestión para determinar la causa raíz y contener la falla. Adicionalmente, se realizará la debida investigación y se garantizará la cadena de custodia de las pruebas.

d. Solución y seguimiento

El área de Seguridad de la Información de VCSOFT corregirá las vulnerabilidades para evitar su recurrencia. El Oficial de Protección de Datos documentará la remediación y generará un reporte de lecciones aprendidas para actualizar las medidas de seguridad.

e. Reporte ante la SIC

Se reportarán las novedades o incidentes de seguridad que afecten las bases de datos ante la Superintendencia de Industria y Comercio mediante la plataforma del Registro Nacional de Bases de Datos (RNBD).

PROCEDIMIENTO PARA LA ATENCIÓN DE CONSULTAS, RECLAMOS, PETICIONES DE RECTIFICACIÓN, ACTUALIZACIÓN Y SUPRESIÓN DE DATOS

VCSOFT ha definido canales y un procedimiento ágil para que los titulares de la información puedan ejercer de forma efectiva sus derechos de acceso, consulta, actualización, corrección, supresión y revocatoria de la autorización.

Presentación de la solicitud

El titular o su representante autorizado puede radicar su solicitud mediante comunicación escrita enviada a través de los siguientes canales:

- **Correo físico:** Dirigido a la sede principal de VCSOFT en la ciudad de Bogotá D.C.
- **Correo electrónico:** Enviar la solicitud a la cuenta habilitada para la protección de datos personales: **habeasdata@vc-soft.com**

La solicitud debe contener la siguiente información básica:

1. Nombres y apellidos completos del titular.
2. Copia del documento de identidad del titular (y del representante, cuando aplique).
3. Descripción clara y precisa del derecho que desea ejercer (consulta, corrección, supresión, etc.).
4. Dirección física o electrónica para recibir notificaciones, fecha y firma del solicitante.
5. Documentos soporte que fundamenten la petición (cuando corresponda).

Recepción y trámite de la solicitud

El Oficial de Protección de Datos Personales de VCSOFT recibe la solicitud, valida la identidad del titular y gestiona el requerimiento de acuerdo con su naturaleza:

a. Acceso o consulta

- El responsable de la base de datos recopila la información asociada al titular y genera un reporte en un formato seguro (como PDF).
- Se remite la respuesta directamente al titular con copia al Oficial de Protección de Datos Personales para su archivo.

b. Actualización o corrección

- El responsable del sistema de información efectúa las modificaciones solicitadas y genera la constancia del cambio en la base de datos.
- Se envía al titular una comunicación formal confirmando la actualización de sus datos.

c. Eliminación o supresión

El titular tiene derecho a solicitar la eliminación de sus datos personales cuando considere que no están siendo tratados bajo los principios de ley, cuando dejen de ser necesarios para la finalidad autorizada o cuando haya expirado el término de su conservación.

Excepciones al derecho de supresión: La supresión no procederá cuando el titular tenga el deber legal o contractual de permanecer en la base de datos, cuando la eliminación obstaculice procesos judiciales o administrativos, o cuando los datos sean indispensables para salvaguardar el interés público o cumplir obligaciones de ley.

d. Revocatoria de la autorización

- El Oficial de Protección de Datos realiza el seguimiento a las revocaciones de autorización para asegurar su cumplimiento en las plataformas y herramientas de la compañía.
- En el caso de grabaciones u otros registros en sistemas de comunicación internos, estos se eliminarán según los plazos establecidos por las políticas de retención y copia de seguridad de VCSOFT.

e. Gestión de Reclamos

- **Reclamo incompleto:** Si la solicitud carece de información necesaria, el Oficial de Protección de Datos requerirá al titular dentro de los cinco (5) días hábiles siguientes a la recepción para que subsane las fallas. Transcurridos dos (2) meses sin que el interesado presente la información, se entenderá que ha desistido del reclamo.
- **Traslado por incompetencia:** Si el área que recibe la petición no es la competente para resolverla, la trasladará al Oficial de Datos Personales en un plazo máximo de dos (2) días hábiles, informando de esto al titular.
- **Inscripción en la base de datos:** Una vez recibido el reclamo completo, se incorporará en la base de datos correspondiente la leyenda "*reclamo en trámite*" junto con el motivo de este, en un término no mayor a dos (2) días hábiles. Esta anotación se mantendrá hasta que el caso sea resuelto.
- **Plazos de respuesta:** El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Si no es posible dar respuesta dentro de este término, se informará al titular los motivos de la demora y la fecha en que se resolverá, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer plazo.

Registro y control de solicitudes

Para garantizar la trazabilidad de cada caso, el Oficial de Protección de Datos Personales mantendrá actualizado un registro interno denominado "**Control de Solicitudes de Habeas Data**", en el cual se consignarán las fechas de radicación, el estado del trámite, las acciones ejecutadas y las respuestas definitivas entregadas a los titulares.

MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

Dando cumplimiento al principio de seguridad establecido en la normatividad vigente, LA EMPRESA adoptará 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.

La sociedad está comprometida a dar un correcto uso y tratamiento de los datos personales de sus clientes y usuarios, evitando 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 la compañía. Por tal motivo, la sociedad cuenta con protocolos de seguridad y acceso a sus sistemas de información, almacenamiento y procesamiento incluidas medidas físicas de control de riesgos de seguridad.

Por tanto, deberá adoptar las medidas que le permitan dar cumplimiento a lo dispuesto por las Leyes 1581 de 2012, y cualquier otra ley o norma que las modifique o sustituya. Consecuencia de esta obligación legal, entre otras, deberá adoptar las medidas de seguridad de tipo lógico, administrativo y físico, acorde a la criticidad de la información personal a la que accede, para garantizar que este tipo de información no será usada, comercializada, cedida, transferida y/o no será sometida a cualquier otro tratamiento contrario a la finalidad comprendida en lo dispuesto en el objeto del presente contrato. Se informará cualquier sospecha de pérdida, fuga o ataque contra la información personal que repose en las bases de datos de LA EMPRESA, aviso que deberá dar una vez tenga conocimiento de tales eventualidades a través de los mecanismos más pertinentes o eficaces, tales como, publicación en la página web o redes de la empresa, comunicación directa al correo electrónico reportado del afectado o al medio establecido por éste para tales efectos o de cualquier manera que garantice el derecho a la información del titular. La pérdida, fuga o ataque contra la información personal implica así mismo la obligación de gestionar el incidente de seguridad conforme los lineamientos legales en la materia.

COMPROMISO CON LA MEJORA CONTINUA

LA EMPRESA reafirma su compromiso corporativo con la protección de datos e integridad de sus procesos mediante la ejecución de las siguientes acciones obligatorias:

- **Capacitación Continua:** Ejecutar programas anuales de formación obligatoria en materia de tratamiento y protección de datos personales para todos los funcionarios.
- **Auditorías de Cumplimiento:** Realizar auditorías internas y/o externas periódicas (mínimo una vez al año) para evaluar la eficacia y el nivel de cumplimiento de la presente política.
- **Continuidad del Negocio:** Alinear los protocolos de gestión de datos personales con el Plan de Continuidad del Negocio (BCP) de la organización, garantizando la

disponibilidad, confidencialidad y resiliencia de la información ante posibles contingencias.

VIGENCIA

La presente política rige a partir del 1 de Agosto del año 2016.

CONTROL DE VERSIONES

VERSIÓN	FECHA	RESUMEN DE CAMBIO
1.0	01/08/2016	Documento inicial: Creación y publicación original de la Política de Tratamiento de Datos Personales conforme a la Ley 1581 de 2012 y Decreto 1377 de 2013.
1.1	15/03/2018	Actualizaciones intermedias: Ajuste de finalidades operativas, inclusión de nuevos canales de atención y actualización normativa de soporte (Decreto 1074 de 2015).
1.2	10/11/2021	Alineación Ley Habeas Data Financiero: Incorporación de disposiciones y ajustes de retención en el marco de la Ley 2157 de 2021 (<i>Borrón y Cuenta Nueva</i>).
1.3	05/06/2023	Ajustes de Infraestructura: Definición de criterios sobre conservación, supresión y anonimización de datos en repositorios locales y de la nube.
1.4	12/09/2024	Protocolo de Incidentes y RNBD: Actualización de los procedimientos de respuesta ante brechas de seguridad y reporte ante la SIC.
1.5	02/02/2026	Alineación Integral (SAGRILAF, IA y Gobierno): Vinculación con listas restrictivas/SAGRILAF y designación del Área de Seguridad de la Información como responsable.