

POLÍTICA DE TRATAMIENTO DE INFORMACIÓN PERSONAL

Versión	Fecha	Autor	Descripción
1.0	08/12/2016	Luis RIVEROS	Generación de versión preliminar
1.1	17/03/2017	Luis RIVEROS	Modificación al parágrafo 2, uso de la información.
1.2	22/06/2017	Lilia DORADO	Ajustes de forma
1.3	03/06/2020	Rafael MILLOBA	Cambio de dirección y teléfono
1.4	05/08/2021	Rafael MILLOBA	Cambio de logo y correo electrónico de contacto

Esta política aplica para todos los titulares de información personal que sea utilizada y/o se encuentre en las bases de datos de **CRITICAL SECURITY**, quien actúa en calidad de responsable del tratamiento de los datos personales.

Marco Legal

El artículo 15 de la Constitución de la República de Colombia establece que cualquier persona tiene derecho a conocer, actualizar y rectificar los datos personales que existan sobre ella en banco de datos o archivos de entidades públicas o privadas. Igualmente, ordena a quienes tienen datos personales de terceros respetar los derechos y garantía previstos en la Constitución cuando se recolecta, trata y circula esa clase de información.

La Ley Estatutaria 1581 del 17 de octubre de 2012 establece las condiciones mínimas para realizar el tratamiento legítimo de los datos personales de los clientes, empleados y cualquier otra persona natural. El literal k) del artículo 18 de dicha ley obliga a los responsables del tratamiento de datos personales a "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".

El artículo 25 de la misma ley establece que las políticas de tratamiento de datos son de obligatorio cumplimiento y que su desconocimiento acarreará sanciones. Dichas políticas no pueden garantizar un nivel de tratamiento inferior al establecido en la ley 1581 de 2012.

Que el Decreto 1377 de 2013, define la información que debe contener como mínimo las políticas de tratamiento de información.

CRITICAL SECURITY está comprometida con el respeto y garantía de los derechos de sus clientes, empleados y terceros en general. Por eso adopta la siguiente política y procedimientos de tratamiento de Información, de obligatoria aplicación en todas las actividades que involucre, total o parcialmente, la recolección, el almacenamiento, el uso, la circulación y transferencia de esa información.

Estas políticas son de obligatorio y estricto cumplimiento para **CRITICAL SECURITY**, en calidad de responsable, así como todos los terceros que obran en nombre de la Compañía, o que sin actuar en nombre de **CRITICAL SECURITY** tratan datos personales por disposición de ésta como encargados.

Tanto el responsable como encargados, entiéndase, empleados, contratistas y terceros deben observar y respetar estas políticas en el cumplimiento de sus funciones y/o actividades aún después de terminados los vínculos legales, comerciales, laborales o de cualquier índole. De igual manera, se comprometen a guardar estricta confidencialidad en relación con los datos tratados.

Cualquier incumplimiento de las obligaciones y, en general, de las políticas contenidas en este documento debe ser reportado a: info@criticalsecurity.com.co

1. Información de la empresa Responsable del Tratamiento de información personal.

La empresa responsable del tratamiento del dato personal:

- Razón social: **CRITICAL SECURITY S.A.S.**
- Domicilio: **Bogotá - Colombia**
- Nit: **900.572.968-2**
- Dirección de correspondencia: **Cra 60 No. 4D-74 piso 2**
- Email: **info@criticalsecurity.com.co**
- Teléfono: (1) 9 27 86 93

2. Tratamiento al cual serán sometidos los datos personales y su finalidad.

- a) Desarrollar actividades de mercadeo y promocionales.
- b) Evaluar la calidad del servicio.
- c) Controlar el acceso a las oficinas de CRITICAL SECURITY, incluyendo el establecimiento de zonas video-vigiladas;
- d) Dar respuesta a peticiones, quejas y reclamos que sean realizadas por los Titulares de la información.
- e) Recaudo de cartera y cobros administrativo, tesorería, contabilidad, entre otros.
- f) Atención de requerimientos judiciales o administrativos y el cumplimiento de mandatos judiciales o legales;
- g) Cualquier otra actividad de naturaleza similar a las anteriormente descritas que sean necesarias para desarrollar el objeto social de CRITICAL SECURITY.
- h) Enviar información sobre condiciones de los productos y servicios ofrecidos por CRITICAL SECURITY.
- i) Acceder a los distintos servicios a través de los sitios web de CRITICAL SECURITY.
- j) Gestión de 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;
- k) Gestión de Recursos Humanos, 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;
- l) 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;
- m) Notificar a contactos autorizados en caso de emergencias durante el horario de trabajo o con ocasión del desarrollo del mismo;
- n) Coordinar el desarrollo profesional de los empleados, el acceso de los empleados a los recursos informáticos del empleador y dar soporte para su utilización;
- o) Para la evaluación del cumplimiento de sus obligaciones.

3. Derechos de los titulares.

De conformidad con lo establecido en el artículo 8 de la Ley 1581 de 2012 y el decreto 1377 de 2013, el titular de los datos personales tiene los siguientes derechos frente a **CRITICAL SECURITY**

- a) Conocer, actualizar y rectificar sus datos personales.
- b) Solicitar prueba de la autorización otorgada a **CRITICAL SECURITY**, en su condición de responsable del Tratamiento;
- c) Ser informado por **CRITICAL SECURITY** previa solicitud, respecto del uso que le ha dado a sus datos personales;
- d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012, una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento;
- e) 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;
- f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

4. Ejercicio y Procedimiento para ejercer los derechos al Habeas Data.

La Ley 1581 de 2012 proporciona a toda persona titular de datos personales una serie de garantías, de verdaderos poderes jurídicos frente al responsable de los datos personales, los cuales, tanto le garantizan el poder de decisión y control que tiene sobre la información que le concierne, como su derecho a la protección de la misma.

En adición, actúan como complemento del deber del responsable de cumplir con las obligaciones que le son impuestas en la Ley, permitiéndole identificar aquellos casos en los que el tratamiento pudiera no resultar ajustado a los mismos.

Para el ejercicio de los derechos, quienes podrán actuar de conformidad con lo establecido en el artículo 14 de la Ley 1581 de 2012 y el decreto 1377 de 2013 son las siguientes personas: los titulares, los causahabientes, su representante o apoderado o las personas que actúen a favor de otro o para otro.

Cuando la solicitud sea formulada por persona distinta del titular y no se acredite que la misma actúa en representación de aquél, se tendrá por no presentada.

CRITICAL SECURITY cuenta con una infraestructura administrativa destinada, entre otras funciones, a asegurar la debida atención de requerimientos, peticiones, consultas, quejas y reclamos relativos a protección de datos, a fin de garantizar el ejercicio de los derechos contenidos en la Constitución y la ley, especialmente el derecho a conocer, actualizar, rectificar y suprimir información personal; así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales.

Para consultas, reclamos, quejas o para el ejercicio de los derechos que le asisten como titular de información (Datos personales), podrá comunicarse con **CRITICAL SECURITY** así:

En caso de que sea cliente o proveedor: info@criticalsecurity.com.co;

Así mismo, usted podrá llamar a la línea de atención al cliente (571) 9 27 86 93 opción 3 en el horario de lunes a viernes de 8:00 a.m. a 5:00 p.m.

5. Ejercicio de los derechos.

5.1 Derecho de acceso.

El poder de disposición o decisión que tiene el titular sobre la información que le concierne, conlleva necesariamente el derecho de acceder y conocer si su información personal está siendo objeto de tratamiento, así como el alcance, condiciones y generalidades de dicho tratamiento. De esta manera, **CRITICAL SECURITY** garantiza al titular su derecho de acceso en tres vías:

- a) La primera implica que el titular pueda conocer la efectiva existencia del tratamiento a que son sometidos sus datos personales.
- b) La segunda, que el titular pueda tener acceso a sus datos personales que están en posesión del responsable.
- c) La tercera, supone el derecho a conocer las circunstancias esenciales del tratamiento, lo cual se traduce en el deber de **CRITICAL SECURITY** de informar al titular sobre el tipo de datos

personales tratados y todas y cada una de las finalidades que justifican el tratamiento.

CRITICAL SECURITY garantiza el derecho de acceso cuando, previa acreditación de la identidad del titular o personalidad de su representante se ponga a disposición de éste, de manera gratuita, el detalle de los datos personales a través de medios electrónicos que permitan el acceso directo del Titular a ellos.

5.2 Consultas.

CRITICAL SECURITY garantiza el derecho de consulta, suministrando a las personas que actúen en ejercicio de este derecho, toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

Para la atención de solicitudes de consulta de datos personales **CRITICAL SECURITY** garantiza, que existen medios de comunicación electrónica y telefónica.

En cualquier caso, independientemente del mecanismo implementado para la atención de solicitudes de consulta, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

5.3 Reclamos.

CRITICAL SECURITY garantiza el derecho de reclamo, a las bases de datos para la corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012 y demás normas aplicable. El reclamo será tramitado bajo las siguientes reglas:

Si el reclamo recibido no cuenta con información completa que permita darle trámite, esto es, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer, se requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Si por alguna circunstancia **CRITICAL SECURITY** recibe un reclamo que en realidad no debería ir dirigido contra él, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

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

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.

Cuando no fuere posible atenderlo dentro de dicho término se informará al interesado antes del vencimiento del referido plazo los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer

término.

5.4 Implementación de procedimientos para garantizar el derecho a presentar reclamos.

La solicitud de rectificación, actualización o supresión debe ser presentada a través de los medios habilitados por **CRITICAL SECURITY**. Señalados en el aviso de privacidad y en este documento, y contener, como mínimo, la siguiente información:

- 1) El nombre, domicilio del titular y medio de contacto para recibir la respuesta como teléfono, correo electrónico, dirección de residencia.
- 2) Los documentos que acrediten la identidad o la representación de su representante.
- 3) La descripción clara y precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos.
- 4) En caso dado otros elementos o documentos que faciliten la localización de los datos personales.

Parágrafo 1. Rectificación y actualización de datos.

CRITICAL SECURITY tiene la obligación de rectificar y actualizar a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, de conformidad con el procedimiento y los términos arriba señalados. Al respecto se tendrá en cuenta lo siguiente:

CRITICAL SECURITY tiene plena libertad de habilitar mecanismos que le faciliten el ejercicio de este derecho.

Parágrafo 2. Supresión De Datos. El titular tiene el derecho, en todo momento, a solicitar a **CRITICAL SECURITY** la supresión (eliminación) de sus datos personales cuando:

- Considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la Ley 1581 de 2012.
- Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recolectados.
- Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recolectados.

Esta supresión implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por **CRITICAL SECURITY**.

Es importante tener en cuenta que el derecho de cancelación no es absoluto y el responsable puede negar el ejercicio del mismo cuando:

- La solicitud de supresión de la información no procederán cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.
 - La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
 - Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.
-

En caso de resultar procedente la cancelación de los datos personales, **CRITICAL SECURITY** debe realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información.

5.5 Revocatoria De La Autorización.

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal.

Se tendrán dos modalidades en las que la revocación del consentimiento puede darse.

La primera, sobre la totalidad de las finalidades consentidas, esto es, que **CRITICAL SECURITY** deba dejar de tratar por completo los datos del titular; la segunda, puede sobre algunos tipos de tratamiento determinados, como por ejemplo para estudios de mercado.

Por lo anterior, será necesario que el titular al momento elevar la solicitud de revocatoria del consentimiento a **CRITICAL SECURITY**, indique en ésta si la revocación que pretende realizar es total o parcial.

En la revocatoria parcial deberá indicar con cuál tratamiento el titular no está conforme.

Habrán casos en que el consentimiento, por su carácter necesario en la relación entre titular y responsable por el cumplimiento de un contrato, por disposición legal no podrá ser revocado.

6. Procedimiento de quejas ante la Superintendencia de Industria y Comercio:

El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante **CRITICAL SECURITY**, de acuerdo al procedimiento anteriormente mencionado.

7. Deberes de CRITICAL SECURITY.

Cuando obra como responsable del tratamiento de datos personales.

Todos los obligados a cumplir esta política deben tener presente que es responsabilidad de **CRITICAL SECURITY** cumplir los deberes que al respecto imponga la ley.

Por ende, deben obrar de tal forma que cumplan las siguientes obligaciones:

7.1. Deberes de CRITICAL SECURITY respecto del titular del dato.

- a) Solicitar y conservar, en las condiciones previstas en esta política, copia de la respectiva autorización otorgada por el titular.
- b) Informar de manera clara y suficiente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- c) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data, es decir, conocer, actualizar o rectificar sus datos personales.
- d) Informar a solicitud del titular sobre el uso dado a sus datos personales.
- e) Tramitar las consultas y reclamos formulados en los términos señalados en la

presente política.

7.2. Deberes de CRITICAL SECURITY respecto de la calidad, seguridad y confidencialidad de los datos personales

- a) Observar los principios de veracidad, calidad, seguridad y confidencialidad en los términos establecidos en la legislación Colombiana.
- b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- c) Actualizar la información cuando sea necesario.
- d) Rectificar los datos personales cuando ello sea procedente.

7.3. Deberes de CRITICAL SECURITY cuando realiza el tratamiento a través de un Encargado

- a) Suministrar al Encargado del tratamiento únicamente los datos personales que está autorizado a suministrar a terceros.
- b) Garantizar que la información que se suministre al Encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- c) Comunicar de forma oportuna al Encargado del tratamiento todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- d) Informar de manera oportuna al Encargado del tratamiento las rectificaciones realizadas sobre los datos personales para que éste proceda a realizar los ajustes pertinentes.
- e) Exigir al Encargado del tratamiento, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
- f) Informar al Encargado del tratamiento cuando determinada información se encuentre en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

7.4. Deberes de CRITICAL SECURITY respecto de la Superintendencia de Industria y Comercio

- a) Informarle las eventuales violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los titulares.
- b) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

8. Transferencia internacional de datos personales.

Cuando se envíen o transfieran datos a otro país será necesario contar con la autorización del titular de la información que es objeto de transferencia. Salvo que la ley diga lo contrario, es presupuesto necesario la existencia de dicha autorización para efectuar la circulación internacional de datos.

En este sentido, antes de enviar datos personales a otro país, los obligados de cumplir esta política deberán verificar que se cuenta con la autorización previa, expresa e inequívoca del titular que permita transmitir sus datos personales.

Carrera 60 No. 4D-74 piso 2
Calle 118 No. 19-52
Bogotá, Colombia
Teléfono: +571 9 27 86 93



Dicha transferencia de los datos personales se realiza únicamente a terceros con quien **CRITICAL SECURITY** tenga vínculo contractual, comercial y/o jurídico.

9. Aviso de Privacidad

CRITICAL SECURITY, en lo sucesivo y a quien le sean cedidos los derechos, le informa que el aviso de privacidad de tratamiento de sus datos personales puede consultarlo en <http://www.criticalsecurity.com.co>

10. Modificación y/o actualización de la política de protección de datos y manejo de información

Cualquier cambio sustancial en las políticas de Tratamiento, se comunicará de forma oportuna a los titulares de los datos a través de los medios habituales de contacto y/o a través de:

Página pública de CRITICAL SECURITY <http://www.criticalsecurity.com.co>, correo electrónico enviado a los titulares, para los titulares que no tengan acceso a medios electrónicos o aquellos a los que no sea posible contactar, se comunicará a través de correo certificado.

Las comunicaciones se enviarán como mínimo, diez (10) antes de implementar las nuevas políticas y/o actualización sustancial de la misma.

11. Vigencia de las políticas de tratamiento de información personal. Las presentes políticas rigen a partir de Enero 1 de 2017.

Por regla general, el término de las autorizaciones sobre el uso de los datos personales por los clientes y/o usuarios se entiende por el término de la relación comercial o de la vinculación al servicio y durante el ejercicio del objeto social de la compañía.

Las autorizaciones sobre los datos de los clientes y/o usuarios podrán terminar por voluntad de los mismos en cualquier momento.

PUBLIQUESE y CUMPLASE

Dado en Bogotá, D.C. 05 días del mes de agosto de 2021