



BRINKS DE COLOMBIA S.A. NIT. 860.350.234-8
POLÍTICAS DE PRIVACIDAD Y TRATAMIENTO
DE DATOS PERSONALES

TABLA DE CONTENIDO

Introducción	3
1. Objetivo	4
2. Ámbito de aplicación	4
2.1. Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales	4
3. Marco normativo	5
4. Glosario.....	5
5. Principios del tratamiento de datos	7
6. Principio de acceso y circulación restringida	8
7. Principio de seguridad	8
8. Autorización para el tratamiento de datos personales	9
8.1. Casos en que no es necesaria la autorización	10
8.2. Cómo obtener la autorización	10
9. Aviso de privacidad	10
10. Datos del responsable del tratamiento	11
11. Tratamiento y finalidades de las bases de datos	11
12.1. Vigencia de las bases de datos	11
12.2. Derechos de los titulares de los datos	12
12.3. Los derechos los podrán ejercer	12
12.4. Relación de derechos de los titulares.....	12
13. Tratamiento de datos de menores	13
14. Tratamiento de datos sensibles	13
15. Datos biométricos	14
17. Deberes como responsable y encargado del tratamiento	14
17.1. Deberes de Brinks de Colombia S.A. Cuando actúe como responsable del tratamiento	14
17.2. Deberes de encargado del tratamiento	15
18. Procedimientos para ejercer los derechos del titular	16
18.1. Derecho de acceso o consulta	16

18.2. Peticiones quejas y reclamos	17
18.3. Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda	17
18.4. Facultados para recibir información	18
18.5. Verificación de la facultad para solicitar o recibir información	18
19. Canales habilitados	18
20. Entrega de datos personales a las autoridades	19
21. Medidas de seguridad	19
22. Cookies o web bugs	21
23. Gestión de incidentes habeas data	22
24. Reporte de problemas técnicos	23
25. Administración de riesgos asociados al tratamiento de los datos	24
26. Seguridad de la información y datos personales	24
27. Transferencia y transmisión internacional de datos personales	25
29. Vigencia de la política de tratamiento de datos	27

INTRODUCCIÓN

El avance de las tecnologías de la información y su inusitado progreso se ha implicado de manera directa en las actividades cotidianas de los seres humanos, a tal punto de que el acceso a ese mundo informáticamente globalizado; a pesar de la brecha digital, ya es el menor de los problemas pues el punto álgido de atención debe centrarse en función de los datos y su tratamiento.

En este preciso instante, en cualquier lugar del mundo, hay un tráfico de información digital en el cual nuestros datos están siendo utilizados con fines diversos y sin contar con nuestro propio consentimiento; lo que a simple vista se evidencia como una amenaza oculta tras el progreso globalizado. Allí es donde radica el desafío del derecho en la informática, en ese concepto de la privacidad, en el cual el constante y rápido intercambio de datos en los diferentes sectores de la actividad económica y social se ve amenazado, generando riesgos para la intimidad de las personas de cualquier edad y condición social.

El derecho de habeas data, está consagrado en la constitución política de Colombia, y desarrollado a través de la Ley de Protección de Datos Personales como el derecho que tiene toda persona para conocer, actualizar y rectificar toda aquella información que se relacione con ella y que se recopile o almacene en centrales de información. De allí se genera la importancia de difundir el conocimiento y procedimientos aplicables a la materia, de manera que las personas tengan los argumentos necesarios para defender sus derechos y salvaguardar el tratamiento de sus datos personales.

El presente documento contiene las políticas de tratamiento de datos personales que deben ser aplicadas por la empresa Brinks de Colombia S.A. de acuerdo al marco legal establecido en la ley estatutaria 1581 de 2012 y reglamentado por los Decretos 1377 de 2013 y 886 de 2014, normas compiladas en el Decreto Único Nacional del Sector Comercio, Industria y Turismo 1074 de 2015 (Artículos 2.2.2.25.1.1. al 2.2.2.26.3.4), y demás normas que la modifiquen, adicionen, complementen, desarrollen o sustituyan.

En virtud del objeto social de Brinks de Colombia S.A. se hace necesario que en el desarrollo de la actividad económica, se realice tratamiento de datos personales con el fin de gestionar dichas relaciones contractuales o de servicios, entre otros fines descritos en el Anexo 1 PL-01 denominado Organización Bases de Datos, contiene la información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

Todo empleado de Brinks de Colombia S.A. al ingresar con la empresa, recibe la capacitación sobre el correcto tratamiento y protección de datos personales para poder conocer y aplicar la normativa vigente.

La primera línea de reporte a Presidencia para Brinks de Colombia S.A., será el oficial de protección de datos personales principal y el oficial de protección de datos nombrados por el Gerente Corporativo de Riesgo, quien debe establecer las directrices para el manejo apropiado de los datos personales, la alta dirección es la encargada de velar por el adecuado seguimiento y control de la normativa en términos de tratamiento y protección de bases de datos personales que tenga a su cargo.

1. OBJETIVO

Con la implementación de ésta política, se pretende garantizar la reserva de la información y la seguridad y será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento de quienes Brinks de Colombia S.A., ha obtenido legalmente información de datos personales conforme a los lineamientos establecidos por la ley del derecho al Habeas Data (Ley 1581 de 2012). Asimismo, a través de la expedición de la presente política se da cumplimiento a lo previsto los artículos 15 y 20 de la Constitución Política, así como, con fundamento en los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD). Adicionalmente, en cumplimiento del artículo 2.2.2.25.1.1 sección 1 capítulo 25 del Decreto 1074 de 2015, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por Brinks de Colombia S.A.

El presente documento aplicará para todos aquellos datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos de Brinks de Colombia S.A., respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las obligaciones y lineamientos de Brinks de Colombia S.A. para la administración y tratamiento de los datos personales que reposen en sus bases de datos y archivos. La presente política es aplicable a los procesos de Brinks de Colombia S.A. que deban realizar el Tratamiento de los datos (datos públicos, datos semiprivados, datos privados, datos sensibles, datos de los niños, niñas y adolescentes), en calidad de Responsable y de Encargado.

Brinks de Colombia S.A. entiende por protección de datos, todas aquellas medidas necesarias que deben tomarse, tanto a nivel físico, técnico, como jurídico para garantizar que la información de nuestros clientes, proveedores, empleados y terceros, almacenada en las distintas bases de datos, estén totalmente seguras de cualquier intento de manipulación por parte de personas no autorizadas.

2. ÁMBITO DE APLICACIÓN

La política de tratamiento establecida en la presente política, cobijará a los datos personales, información y archivos registrados en las Bases de Datos de Brinks de Colombia S.A. con el fin de dar cumplimiento a los fines descritos en esta política de tratamiento.

2.1. EXCEPCIÓN AL ÁMBITO DE APLICACIÓN DE LAS POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

Se exceptúan del régimen de protección de Datos Personales establecido en la Ley 1581 de 2012 artículo 2 y sus Decretos Reglamentarios, los cuales comprenden:

- Bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- Bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo
- Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
- Bases de datos y archivos de información periodística y otros contenidos editoriales;

3. MARCO NORMATIVO

- Constitución Política de Colombia
- Ley 1581 de 2012
- Decreto 1074 de 2015 Capítulo 25 y Capítulo 26 compilatorios de los decretos:
 - Decreto 1377 de 2013
 - Decreto 886 de 2014
- Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data”.
- Actos administrativos expedidos por la Superintendencia de Industria y Comercio.

4. GLOSARIO

El objetivo de este glosario es contar con una definición de los principales términos presentes en la Ley 1581 de 2012, su Decreto Reglamentario 1377 del año 2013, y/o en las presentes políticas, puntualizando de forma muy clara el significado de ellos:

a) Autorización: Es el consentimiento previo, expreso e informado que da cualquier persona para que Brinks de Colombia S.A., pueda llevar a cabo el Tratamiento de datos personales.

b) Aviso de Privacidad: Es la comunicación verbal o escrita realizada 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.

c) Base de Datos: Es el conjunto o colección de información organizada que contenga datos personales que sea objeto de Tratamiento.

d) Canales de Atención: Son los medios que tiene habilitado Brinks de Colombia S.A. para el ejercicio de Consultas y/o Reclamos por parte de los Titulares Los Titulares de los datos podrán remitir sus peticiones o consultas a través de los siguientes canales:

e) Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales

- Correo electrónico: proteccion.datosb@brinks.com.co
- Dirección: Cl 21 68 d 8, Bogotá D.C - Bogotá D.C. Teléfonos: 7428421 – 0.

determinadas o determinables. . Estos datos se clasifican en públicos, semiprivados, privados y sensibles:

f) 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 del servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

g) Dato Semiprivado: Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

h) Dato Privado: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

i) Dato Sensible: 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.

j) 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.

k) Proveedor: Es la persona natural o jurídica con la cual Brinks de Colombia S.A. establece y mantiene una relación contractual o legal que suministra a la Compañía cualquier producto y/o servicio.

l) Responsable del Tratamiento: Es la Persona natural o jurídica de naturaleza pública o privada, que actuando por ella misma o conjuntamente con otros, decida sobre la base de datos y/o el Tratamiento de los datos. Para efectos del presente documento, el Responsable del Tratamiento es Brinks de Colombia S.A., con domicilio en la ciudad de Bogotá.

m) Responsable de Administrar las Bases de Datos: Colaborador encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base datos específica; así como de poner en práctica las directrices que dicte el Responsable del tratamiento y el Oficial de Protección de datos.

n) Oficial de Protección de Datos: Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.

o) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

p) 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.

q) 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.

r) Tratamiento: Es cualquier actividad, operación o conjunto de trabajos realizados sobre datos personales tales como la recolección, almacenamiento, uso, circulación o supresión.

s) Requisito de Procedibilidad: Paso previo que debe surtir el Titular antes de interponer una queja ante la Superintendencia de Industria y Comercio. Este consiste en una reclamación directa al Encargado o Responsable de sus Datos Personales.

5. PRINCIPIOS DEL TRATAMIENTO DE DATOS

El artículo 4 de la lepd establece unos 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, son el fin de establecer los cimientos y las bases de las presentes políticas, se consagran los siguientes principios rectores del tratamiento de los datos personales.

A) Principio de Legalidad en Materia de Tratamiento de Datos: el tratamiento de la información contenida en las bases de datos custodiadas por brinks de colombia s.a., en virtud de la relación contractual o de servicio sostenida o que se haya sostenido, es una actividad reglada que debe sujetarse a lo establecido en la ley 1581 de 2012 y en las demás disposiciones que la desarrollen.

B) Principio de Finalidad: el tratamiento que le damos a los datos personales obedece a una finalidad, la cual será previamente informada al titular. La aplicación de este principio implica: (i) un ámbito temporal: que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y (ii) un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.

C) Principio de Libertad: el tratamiento de nuestras bases de datos sólo podrá ejercerse con el consentimiento libre, previo, expreso e informado del titular. 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 de los datos requiere la autorización previa e informada del titular por cualquier medio que permita ser consultado con posterioridad.

D) Principio de Veracidad o Calidad: la información sujeta al tratamiento por parte de brinks de colombia s.a., será 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 de brinks de colombia s.a., en cualquier momento y sin restricciones, información acerca de la existencia de sus datos, se debe informar que datos tengo del él. En virtud de este principio, brinks de colombia s.a. Suministrará, la siguiente información a los titulares:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

6. PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA

El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la LEPD y la Constitución. El Tratamiento de los datos autorizados por el titular, sólo podrá hacerse por personas autorizadas dentro de la organización y/o por las personas previstas en la Ley., con niveles específicos de seguridad, para el cumplimiento de las finalidades autorizadas Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

7. PRINCIPIO DE SEGURIDAD

La información sujeta a Tratamiento por Brinks de Colombia S.A. a que se refiere la Ley 1581 de 2012, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El Responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento de todo el personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del Responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el PL-02 Políticas Internas de Seguridad, 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.

a) 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 solo realizar suministro o

comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la lepd y en los términos de esta.

b) Principio de Interpretación Integral de los Derechos Constitucionales: los derechos de los titulares de los datos personales se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la constitución y con los derechos constitucionales aplicables, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad, entre otros.

8. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Tal como se define en el glosario de este documento, la autorización será solicitada por Brinks de Colombia S.A. cuando actúe como Responsable del Tratamiento, debiendo implementar los procedimientos adecuados, *con el fin de informar sobre los datos personales que serán recolectados y las finalidades específicas del tratamiento para las cuales se solicita dicha autorización.*

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización del Titular, salvo en los casos expresamente señalados en las normas que reglamentan la protección de los datos personales. Con antelación y/o al momento de efectuar la recolección del dato personal, Brinks de Colombia S.A. solicitará al Titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015.

No será necesaria la autorización del Titular cuando se trate de:

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

En aquellos casos en que se produzcan cambios sustanciales en el contenido de las políticas de tratamiento, Brinks de Colombia S.A. deberá comunicar al Titular de dichas modificaciones con anterioridad o a más tardar al momento de implementar las nuevas políticas. Se comunicarán los cambios sustanciales en el contenido de las políticas de tratamiento.

Se deberá solicitar una nueva autorización al titular de los datos personales, cuando se realicen cambios con respecto a la finalidad del tratamiento.

Todos los formatos físicos, formularios digitales que se encuentren en intranet o páginas web de Brinks de Colombia S.A., aplicaciones móviles, chat y video chat, así como en la recepción de llamadas telefónicas donde se capturen datos

personales, deberá contener la autorización para el tratamiento de datos personales.

Todos los funcionarios dueños o encargados de bases de datos deberán conservar dichas autorizaciones conforme lo indicado en la presente política para posterior consulta.

El responsable de administrar las bases de datos deberá coordinar la aplicación de este procedimiento y gestionará las autorizaciones generadas en formularios físicos, digitales y audios para que se encuentren bajo custodia, la conservación y realizar la disposición final de acuerdo con los lineamientos de su proceso operativo o lo regulado en la presente política.

8.1. CASOS EN QUE NO ES NECESARIA LA AUTORIZACIÓN

La autorización del cliente, proveedor, colaborador o tercero, no será necesaria cuando se trate de:

- Entrega de información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Tratamiento de Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Para el tratamiento de información autorizado por la ley para fines históricos, Estadísticos o científicos.
- Cuando se trata de datos relacionados con el Registro Civil.

8.2. COMO OBTENER LA AUTORIZACIÓN

La autorización para el uso y/o tratamiento de los datos será gestionada por Brinks de Colombia S.A., a través de mecanismos que garanticen su consulta posterior y la manifestación de la voluntad del Titular a través de los siguientes medios:

- Por Escrito,
- De forma Oral:
 - Mediante canales automatizados
 - Mediante Conductas Inequívocas

En todos los casos las áreas encargadas establecerán cuales actividades en las que se soliciten datos se consideran conductas inequívocas, y deberá informar al correo proteccion.datosb@brinks.com.co, o en auditoria periódica con el fin de incorporar dicha novedad, por otra parte se conservará prueba de la autorización, sea cualquiera de las 4 formas ya mencionadas, pues la Ley 1581 de 2012 es clara en afirmar que se debe “solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular”.

Brinks de Colombia S.A., con antelación y/o al momento de efectuar la recolección del dato personal, informará de manera clara y expresa al Titular, lo siguiente:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
- 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;
- Los derechos que le asisten como Titular;
- La identificación, dirección física o electrónica y teléfono Brinks de Colombia S.A.T

9. AVISO DE PRIVACIDAD

El aviso de privacidad a través del cual Brinks de Colombia S.A. informará la existencia de las políticas de tratamiento de información que les serán aplicables, la forma de acceder a las mismas y la finalidad del tratamiento que pretenda dar a sus datos personales, en aquellos casos en los que no sea posible poner a disposición de estos las políticas de tratamiento de la información, estará puesto a disposición en la página web de Brinks de Colombia S.A.

10. DATOS DEL RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de las bases de datos objeto de esta política es Brinks de Colombia S.A., cuyos datos de contacto son los siguientes:

- Razón social: Brinks de Colombia S.A.
- NIT. 860.350.234 - 8
- Dirección: Calle 21 # 68D - 08, Bogotá D.C., Colombia.
- Correo electrónico: proteccion.datosb@brinks.com.co
- Teléfono: (+57 1) 7428421.

11. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

Brinks de Colombia S.A., informa a los titulares que los datos recolectados podrán ser utilizados para las finalidades indicadas en el Anexo 1 PL-01 denominado Organización Bases de Datos, el cual contiene la información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

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

El tratamiento podrá realizarlo Brinks de Colombia S.A. directamente o por intermedio de sus Encargados Del Tratamiento de datos personales, para que lleven a cabo cualquier operación o conjunto de operaciones tales como la recolección, almacenamiento, uso, circulación, supresión, clasificación, transferencia y transmisión sea nacional o internacional (el "Tratamiento") sobre la totalidad o parte de sus datos personales.

12. REGISTRO NACIONAL DE BASES DE DATOS – RNBD

El término para registrar las bases de datos en el RNBD será el establecido legalmente. Asimismo, de acuerdo con el artículo 12 del Decreto 886 de 2014, los Responsables del Tratamiento deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

12.1. Vigencia de las Bases De Datos

Los datos personales incorporados en las bases de datos estarán vigentes durante el plazo necesario para cumplir las finalidades para el cual se autorizó su tratamiento y de las normas especiales que regulen la materia, también se tendrán en cuenta las normas vigentes relacionadas con el periodo de conservación

12.2. Derechos de los Titulares de los Datos

De acuerdo con el artículo 8 de la LEPD, artículo 2.2.2.25.4.1 sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículos 21 y 22 del Decreto 1377 de 2013), los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. El Titular de los datos personales tendrá los siguientes derechos:

- 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;
- Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;
- Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución;
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento

12.3. Los Derechos los Podrán Ejercer

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

Por sus causahabientes, quienes deberán acreditar tal calidad.

Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

En el caso de ser menores de edad, los padres o representantes legales

12.4. Relación de Derechos de los Titulares

Derecho de Acceso o Consulta:

Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

Derechos de Quejas y Reclamos:

La Ley distingue cuatro tipos de reclamos:

Reclamo de Corrección: el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

Reclamo de Supresión: el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.

Reclamo de revocación: el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

Reclamo de Infracción: el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

Derecho a Solicitar Prueba de la Autorización Otorgada al Responsable del Tratamiento:

Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

Derecho a Presentar Ante la Superintendencia de Industria y Comercio Quejas por Infracciones:

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

13. TRATAMIENTO DE DATOS DE MENORES

Brinks de Colombia S.A. de acuerdo con el artículo 7° de la Ley 1581 de 2012, realiza Tratamiento de datos personales de niños, niñas y adolescentes en el marco de los criterios señalados en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013), con observancia de los siguientes parámetros y requisitos:

- Que el uso del dato responda y respete el interés superior de los niños, niñas y adolescentes.
- Que en el uso del dato se asegure el respeto de sus derechos fundamentales del menor.

Cumplidos los anteriores requisitos, Brinks de Colombia S.A. solicitará al representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. En calidad de Responsable y/o Encargado velará por el uso adecuado de los datos de niños, niñas y adolescentes aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias. Asimismo, identificará los datos sensibles recolectados o almacenados con el fin de incrementar la seguridad y tratamiento de la información

14. TRATAMIENTO DE DATOS SENSIBLES

Cuando se vaya a realizar cualquier tipo de tratamiento sobre datos sensibles (Ver Glosario), se debe cumplir con dos obligaciones:

- Informar al titular que no está obligado a suministrar la información, dado que hace parte de la clasificación de datos sensibles;
- Informar al titular, cuales datos son objeto de Tratamiento son sensibles.

15. DATOS BIOMÉTRICOS

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

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

16. TRATAMIENTO DE DATOS EN LOS SISTEMAS DE VIDEOVIGILANCIA

Brinks de Colombia S.A. informará a las personas sobre la existencia de mecanismos de videovigilancia, mediante la fijación de anuncios visibles al alcance de todos los titulares e instalados en las zonas de videovigilancia, principalmente en las zonas de ingreso a los lugares que están siendo vigilados y monitoreados y al interior de estos. En estos avisos informará quién es el Responsable del Tratamiento, las finalidades del tratamiento, los derechos del Titular, los canales habilitados para ejercer los derechos del Titular, así como, dónde se encuentra publicada la Política de Tratamiento de la Información. De otra parte, conservará las imágenes solo por el tiempo estrictamente necesario para cumplir con la finalidad del e inscribirá la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos, salvo que el Tratamiento consista solo en la reproducción o emisión de imágenes en tiempo real.

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

17. DEBERES COMO RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

17.1. Deberes de Brinks de Colombia S.A. Cuando Actúe Como Responsable del Tratamiento

Cuando Brinks de Colombia S.A. actúe como Responsable del Tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la Ley 1581 de 2012 y en otras que rijan su actividad:

Frente al Titular

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.

- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
- e) Informar a solicitud del Titular sobre el uso dado a sus datos.

Frente al Encargado:

- a) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- b) Actualizar la información, comunicando 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.
- c) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- d) 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.
- e) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- f) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

Frente a los Principios y Otras Obligaciones:

- a) Observar los principios Legalidad, finalidad, libertad, calidad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
- b) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
- c) 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.
- d) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- e) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

17.2. Deberes de Encargado del Tratamiento

Conforme a lo establecido por la ley 1581 de 2012, la persona natural o jurídica escogida por Brinks de Colombia S.A., debe sujetarse a lo expuesto en dicha norma lo cual obedece a:

- a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
- d) Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- e) Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la presente ley.
- f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
- g) Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la superintendencia de industria y comercio.

- h) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- i) 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.
- j) Cumplir las instrucciones y requerimientos que imparta la superintendencia de industria y comercio.
- k) Registrar en la base de datos la leyenda “reclamo en trámite” cuando el titular, su representante o causahabiente haya realizado reclamación.
- l) 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.

18. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

18.1. Derecho de Acceso o Consulta

Brinks de Colombia S.A. garantizará al Titular la consulta de forma gratuita de sus datos personales en los siguientes casos (Artículo 2.2.2.25.4.2. sección 4 capítulo 25 del Decreto 1074 de 2015):

- Al menos una vez cada mes calendario.
- Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, Brinks de Colombia S.A. podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, Brinks de Colombia S.A. demostrará a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a Brinks de Colombia S.A. enviado, mediante correo electrónico a: proteccion.datosb@brinks.com.co, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a CL 21 68 D 8, Bogotá D.C - Bogotá D.C. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por Brinks de Colombia S.A.

Una vez recibida la solicitud, Brinks de Colombia S.A. resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, 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 término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

18.2. Peticiones Quejas y Reclamos

Para efectos de recibir las peticiones, quejas y reclamaciones, relacionadas con el manejo y tratamiento de datos personales, Brinks de Colombia S.A. ha destinado los siguientes canales: Correo electrónico: proteccion.datosb@brinks.com.co, Dirección: CL 21 68 D 8, BOGOTÁ D.C – BOGOTÁ D.C. y Teléfonos: 7428421 - 0 para canalizarlas, estudiarlas y contestarlas. Por lo tanto, a dicha dirección podrán enviar sus solicitudes, las cuales se tratarán conforme lo dispone la Ley 1581 de 2012 y sus demás normas concordantes:

Los titulares podrán presentar una petición o reclamo ante Brinks de Colombia S.A. quien actúa como Responsable del Tratamiento, el cual será tramitado bajo las siguientes reglas:

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a Brinks de Colombia S.A. enviado, mediante correo electrónico a proteccion.datosb@brinks.com.co, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a CL 21 68 D 8, Bogotá D.C - Bogotá D.C. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.

18.3. Documentos Acreditativos de la Petición Formulada que se Quieran Hacer Valer, Cuando Corresponda

A. El reclamo se formulará mediante solicitud dirigida a Brinks de Colombia S.A., con la identificación del titular la descripción de los hechos que dan lugar al reclamo, la dirección, y se acompañará de los documentos que se quieran hacer valer. Si el reclamo resulta incompleto, se requerirá al peticionario 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 de la petición o reclamo.

B. Brinks de Colombia S.A. dará respuesta oportuna al CLIENTE, PROVEEDOR, COLABORADOR o TERCERO, atendiendo su petición dentro de un término de 15 días hábiles, contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, y se señalará la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

C. El área responsable para efectuar la recepción y trámite de las reclamaciones es la Gerencia de Corporativa de Riesgo.

D. La solicitud de supresión de la información y la revocatoria de la autorización no procederá cuando el titular tenga un deber legal o contractual de permanecer en la base de datos.

E. En caso que Brinks de Colombia S.A. no sea competente para resolver el reclamo, dará traslado a quien corresponda e informará de la situación al peticionario.

18.4. Facultados para Recibir Información

Brinks de Colombia S.A. suministrará la información de los Titulares de sus bases de datos a las siguientes personas habilitadas o facultadas para recibirla, de acuerdo con el artículo 13 de la Ley 1581 de 2012:

- A los Titulares, sus causahabientes o sus representantes legales;
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;
- A los terceros autorizados por el Titular o por la ley.

18.5. Verificación de la Facultad para Solicitar o Recibir Información

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

Titular: Copia del documento de identidad.

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

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

19. CANALES HABILITADOS:

El titular de los datos personales o sus causahabientes cuando consideren que la información contenida en la base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán ejercer sus derechos y presentar un reclamo ante Brinks de Colombia S.A. ubicada en la Calle 21 # 68D - 08 Bogotá D.C., contactándose a la Gerencia Corporativa de Riesgos en el correo proteccion.datosb@brinks.com.co o al teléfono 7428421 - 0

20. ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES

Cuando por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial se soliciten a Brinks de Colombia S.A. acceso y/o entrega de datos de carácter personal contenidos en cualquiera de sus bases de datos, se verificará la legalidad de la petición, la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad. Para la entrega se suscribirá un acta indicando los datos de la entidad solicitante y las características de la información personal solicitada, precisando la obligación de garantizar los derechos del Titular, tanto al funcionario que hace la solicitud, a quien la recibe, así como a la entidad requirente.

21. MEDIDAS DE SEGURIDAD

Brinks de Colombia S.A., con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, Brinks de Colombia S.A., mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por Brinks de Colombia S.A. que están recogidas y desarrolladas en su PL-02 Políticas Internas de Seguridad (Tablas I, II, III y IV).

TABLA I: MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICA, PRIVADA, CONFIDENCIAL, RESERVADA) Y BASES DE DATOS (AUTOMATIZADAS, NO AUTOMATIZADAS)

<p>Gestión de Documentos y Soportes</p>	<ul style="list-style-type: none"> • Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. • Acceso restringido al lugar donde se almacenan los datos. • Autorización del responsable de Administrar las bases de datos para la salida de documentos o soportes por medio físico o electrónico. • Sistema de etiquetado o identificación del tipo de información. • Inventario de soportes.
<p>Control de Acceso</p>	<ul style="list-style-type: none"> • Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. • Lista actualizada de usuarios y accesos autorizados. • Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. • Concesión, alteración o anulación de permisos por el personal autorizado.
<p>Incidencias</p>	<ul style="list-style-type: none"> • Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. • Procedimiento de notificación y gestión de incidencias.
<p>Personal</p>	<ul style="list-style-type: none"> • Definición de las funciones y obligaciones de los usuarios con acceso a los datos. • Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. • Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.
<p>Manual Interno de Seguridad</p>	<ul style="list-style-type: none"> • Elaboración e implementación del Manual de obligado cumplimiento para el personal. • Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.

TABLA II: MEDIDAS DE SEGURIDAD COMUNES PARA TODO TIPO DE DATOS (PÚBLICA, PRIVADA, CONFIDENCIAL, RESERVADA) SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS	
Archivo	<ul style="list-style-type: none"> • Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta, que permitan el ejercicio de los derechos de los Titulares.
Almacenamiento de Documentos	<ul style="list-style-type: none"> • Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.
Custodia de Documentos	<ul style="list-style-type: none"> • Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos.
BASES DE DATOS AUTOMATIZADAS	
Identificación y Autenticación	<ul style="list-style-type: none"> • Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. • Mecanismos de identificación y autenticación; Contraseñas: asignación y caducidad.
Telecomunicaciones	<ul style="list-style-type: none"> • Acceso a datos mediante redes seguras.

TABLA III: MEDIDAS DE SEGURIDAD PARA DATOS PRIVADOS SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS	
Auditoría	<ul style="list-style-type: none"> • Auditoría ordinaria (interna o externa) cada dos meses. • Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. • Informe de detección de deficiencias y propuesta de correcciones. • Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
Almacenamiento de Documentos	<ul style="list-style-type: none"> • Designación de uno o varios Administradores de las bases de datos. • Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. • Prohibición de delegación de la responsabilidad del Responsable del tratamiento en los Administradores de las bases de datos.
Manual Interno de Seguridad	<ul style="list-style-type: none"> • Controles periódicos de cumplimiento.

BASES DE DATOS AUTOMATIZADAS

Gestión de Documentos y Soportes	<ul style="list-style-type: none"> ● Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.
Control de acceso	<ul style="list-style-type: none"> ● Control de acceso al lugar o lugares donde se ubican los sistemas de información.
Identificación y Autenticación	<ul style="list-style-type: none"> ● Mecanismo que limite el número de intentos reiterados de acceso no autorizados. ● Mecanismos de cifrado de datos para la transmisión.
Incidencias	<ul style="list-style-type: none"> ● Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. ● Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IV: MEDIDAS DE SEGURIDAD PARA DATOS SENSIBLES SEGÚN EL TIPO DE BASES DE DATOS

BASES DE DATOS NO AUTOMATIZADAS

Control de Acceso	<ul style="list-style-type: none"> ● Acceso solo para personal autorizado. ● Mecanismo de identificación de acceso. ● Registro de accesos de usuarios no autorizados. ● Destrucción que impida el acceso o recuperación de los datos.
Almacenamiento de Documentos	<ul style="list-style-type: none"> ● Archiveros, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. ● Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.

BASES DE DATOS AUTOMATIZADAS

Control de acceso	<ul style="list-style-type: none"> ● Sistema de etiquetado confidencial.
Identificación y Autenticación	<ul style="list-style-type: none"> ● Mecanismos de cifrado de datos para la transmisión y almacenamiento.
Almacenamiento de documentos	<ul style="list-style-type: none"> ● Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede ● Control del registro de accesos por el responsable de seguridad. Informe mensual.
Control de acceso	<ul style="list-style-type: none"> ● Sistema de etiquetado confidencial.

22. COOKIES O WEB BUGS

Brinks de Colombia S.A. puede recolectar información personal de sus Usuarios mientras utilizan la Página Web, la Aplicación o las Páginas Vinculadas (Landing Page). Los usuarios pueden optar por almacenar esta información personal en la página web, la aplicación o en el portal vinculado (Landing Page), con el fin de facilitar las transacciones y los servicios a prestar por parte de la empresa Brinks de Colombia S.A. y/o de sus portales vinculados (Landing Page). Por lo que, Brinks de Colombia S.A. utiliza diferentes tecnologías de seguimiento y recopilación de datos como, Cookies propias y de terceros, esta es la herramienta de análisis que ayuda a los propietarios de sitios web y de aplicaciones a entender

cómo interactúan los visitantes con sus propiedades. Esta herramienta puede utilizar un conjunto de cookies para recopilar información y ofrecer estadísticas de uso de los sitios web sin identificar personalmente a los visitantes de Google.

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

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

- Chrome:
<https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es>
- Microsoft Edge:
<https://support.microsoft.com/es-es/microsoft-edge/permitir-temporalmente-las-cookies-y-los-datos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c-7c2b-541086362bd2>
- Firefox:
<https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias>
- Safari: <https://support.apple.com/es-es/HT201265>

23. GESTIÓN DE INCIDENTES HABEAS DATA

Brinks de Colombia S.A. cuenta con un procedimiento de reporte de incidentes para la comunicación y notificación, entre los colaboradores, oficial de protección de datos personales, encargados de tratamiento, Titulares de los datos, ente de vigilancia y control, así como, los entes judiciales: para la gestión y respuesta ante incidentes de seguridad desde el momento en que son detectados con el fin de ser evaluados y gestionar las vulnerabilidades identificadas, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros.

Todos los usuarios y responsables de administrar bases de datos, así como, cualquier persona que tenga relación con la recolección, el almacenamiento, uso, circulación o cualquier tratamiento o consulta de las bases de datos, deberá conocer el procedimiento para actuar en caso de incidentes de seguridad para garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que se encuentran bajo su responsabilidad.

Algunos ejemplos de incidencias de seguridad son: caída de sistemas de seguridad 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, entre otros.

En caso de presentarse un incidente de seguridad, el equipo o Comité de respuesta tendrá en cuenta los siguientes criterios:

Estrategia para Identificar, Contener y Mitigar los Incidentes de Seguridad

Aplicar las medidas para contener y revertir el impacto que puede tener el incidente de seguridad.

Evaluar adecuadamente el incidente de seguridad y su impacto en los Titulares de la información.

Verificar los requisitos legales o contractuales con proveedores de servicios asociados al incidente de seguridad.

Determinar el nivel de riesgo para los Titulares de la Información y notificar la ocurrencia.

Verificar los roles y responsabilidades del personal responsable de la operación de la información o datos afectados.

Línea de Tiempo para la Gestión del Incidente de Seguridad

Aplicar el procedimiento para atender los incidentes de seguridad, de acuerdo con parámetros que permitan una adecuada gestión y mitigación de impacto. Verificar de acuerdo con la evaluación del incidente de seguridad, la necesidad de notificar a entidades, tales como: la Fiscalía General de la Nación, la Procuraduría General de la Nación, Gula, Policía Nacional, Superintendencia Financiera de Colombia, Centro Cibernético Policial, colCERT; CSIRT Policial, CSIRT Asobancaria, CSIRT Sectorial, entre otras.

Progreso del Reporte del Incidente de Seguridad

Realizar monitoreo en la gestión estableciendo plazos, evaluar su progreso e identificar los posibles puntos conflictivos que se puedan generar en el manejo del incidente de seguridad.

Evaluación de Respuesta Ante el Incidente de Seguridad

Una vez se haya gestionado y controlado el incidente de seguridad, el equipo de respuesta deberá revisar las acciones ejecutadas para contenerlo y realizar los ajustes pertinentes para implementar plan de mejora.

Acciones Implementadas y Planes de Mejora

Establecer las acciones necesarias para mitigar el impacto del incidente de seguridad y evitar que vuelva a ocurrir, mediante acciones correctivas y preventivas, así como, planes de mejora que debe adoptar el equipo de respuesta.

Documentación y Reporte Ante el Ente de Vigilancia y Control

Documentar en un registro interno la información relacionada con el incidente de seguridad, así como, elaborar informe con soportes de las acciones adelantadas que deberá ser radicado ante Superintendencia de Industria y Comercio, a través del RNBD dentro de los 15 días hábiles siguientes de haber sido detectado del incidente.

Revisión

Evaluación de las causas que ocasionaron el incidente de seguridad y el éxito de su gestión para valorar la efectividad de los controles y acciones implementadas. Documentar las lecciones aprendidas para tenerlas presentes en futuras ocasiones.

24. REPORTE DE PROBLEMAS TÉCNICOS

Nombres, apellidos, dirección, teléfonos, ciudad, email y comentarios. Estos datos pueden ser almacenados y/o procesados en servidores ubicados en centro de procesamiento de datos ya sean propios o contratados con proveedores, localizados en distintos países, lo cual es autorizado por nuestros clientes/usuarios, Para mayor información, sobre las empresas que hacen parte de Brinks de Colombia S.A., la identidad, domicilios y formas de contacto puede consultarlo en la siguiente dirección electrónica proteccion.datosb@brinks.com.co Brinks de Colombia S.A., se reserva el derecho a mejorar, actualizar, modificar, suprimir cualquier tipo de

información, contenido, dominio o subdominio, que pudiera aparecer en el sitio web, sin que exista obligación de preaviso, entendiéndose como suficiente con la publicación en los sitios web de Brinks de Colombia S.A. Para la solución de peticiones legales o internas y para la prestación u ofrecimiento de nuevos servicios o productos.

25. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

Brinks de Colombia S.A. ha identificado riesgos relacionados con el tratamiento de los datos personales y establecidos controles con el fin de mitigar sus causas, mediante la implementación de la PL-02 Políticas Internas de Seguridad. Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

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

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

- Sucesos de origen físico: Entendidos como los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.
- Negligencia y decisiones institucionales: Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Brinks de Colombia S.A. en el programa de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

26. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

El cumplimiento del marco normativo en Protección de Datos Personales, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para Brinks de Colombia S.A. Por ello, hemos establecido políticas, lineamientos y procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades de Brinks de Colombia S.A. cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.

Asimismo, garantizamos que en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

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

27. TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS PERSONALES

Brinks de Colombia S.A. realizará transferencia de datos personales a países que proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la Ley 1581 de 2012 exige a sus destinatarios. Esta prohibición no registrá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.

- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

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

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

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

Las anteriores condiciones fijadas para las transmisiones de datos internacionales, también le serán aplicables a las transmisiones de datos nacionales.

28. GESTIÓN DE DOCUMENTOS

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

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

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

Los documentos tanto físicos como digitales que contengan datos personales, deben ser protegidos por agentes externos o internos que puedan alterar su contenido, siguiendo los lineamientos descritos en el PL-02 Manual Interno de Políticas de Seguridad.

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

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

29. VIGENCIA DE LA POLÍTICA DE TRATAMIENTO DE DATOS

La presente política de Tratamiento de la Información entrará en vigencia desde el 15 de Agosto de 2018 y los datos suministrados serán conservados hasta por el tiempo de la vigencia de la sociedad o la que la sustituya a cualquier título, el de su liquidación y los que la ley establezca.

El área responsable de la Política de Tratamiento de datos es la Gerencia Corporativa de Riesgo quien podrá ser contactada a través del correo electrónico proteccion.datos@brinks.com.co , teléfono: (1) 7428421 o por correo en la Calle 21 # 68D – 08, Bogotá D.C., Colombia de la ciudad de Bogotá D.C.