DOCUMENTO DE SEGURIDAD
LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL LEY 1581/2012

Bogotá, Colombia, noviembre 2018.

Por la presente, **B&C Corporation** sociedad legalmente registrada y autorizada bajo las leyes de La República de Colombia (en adelante "**B&CC**" o "la compañía"), como Responsable de Tratamiento de datos de carácter personal, cuyos archivos han sido inscritos en el Registro Nacional de Base de Datos (RNBD) de la Superintendencia de Industria y Comercio de Colombia (SIC), y en cumplimiento de la normativa vigente de protección de datos, en especial lo establecido en el Artículo 15 de la Constitución Política de Colombia ("habeas data"), la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas que la modifican, adicionan, complementan o desarrollan, aprueba la presente versión de política interna sobre tratamiento de datos personales (en adelante la "Política"), junto con los procedimientos de índole técnica y organizativa que lo desarrollan.

La política interna sobre tratamiento de datos personales es de acceso público, sin embargo, los procedimientos de índole técnica y organizativa que la desarrollan son de acceso restringido a las personas que a continuación se detallan y a los cuales se distribuye dicho documento y solo se distribuirán de conformidad con el procedimiento previsto para su requerimiento de conformidad con lo establecido en presente documento.

El Documento de Seguridad está restringido a las personas indicadas y está prohibida la redistribución de este.

TABLA DE CONTENIDOS

1.INTRODUCCION 5
2. DEFINICIONES 6
3. ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD 7
4. MEDIDAS DE SEGURIDAD APLICABLES A ARCHIVOS Y TRATAMIENTOS AUTOMATIZADOS Y NO AUTOMATIZADOS 9
5. MEDIDAS DE SEGURIDAD APLICABLES A ARCHIVOS Y SISTEMAS AUTOMATIZADOS 9
5.1. MEDIDAS DE NIVEL BÁSICO 9
5.1.1. Identificación y autenticación 9
5.1.2. Control de Acceso 10
5.1.3. Archivos Temporales 10
5.1.4. Gestión de Soportes 10
5.1.5. Copias de Respaldo. Procedimientos de generación y recuperación de copias de seguridad. 11
5.1.6. Tratamiento de datos fuera de los locales 11
5.1.7. Registro de Incidencias 12
5.1.MEDIDAS DE NIVEL BÁSICO 12
5.2.1. Responsable de Seguridad 12
5.2.2. Auditoría 12
5.2.3. Identificación y Autenticación 13
5.2.4. Control de Acceso Físico 13
5.2.5. Gestión de Soportes 13
5.2.6. Registro de Incidencias 13
5.2.MEDIDAS DE NIVEL MEDIO 13
5.3.1. Distribución de soportes 13
5.3.2. Registro de Accesos 14
5.3.3. Copias de respaldo y recuperación 14
5.3.4. Telecomunicaciones 14
5.3.MEDIDAS DE NIVEL ALTO 14
6. MEDIDAS DE SEGURIDAD APLICABLES A BASES DE DATOS Y SISTEMAS NO AUTOMATIZADOS 14
6.1. MEDIDAS DE NIVEL BÁSICO 15
6.1.1. Criterios de archivo 15
6.1.2. Dispositivos de almacenamiento 15
6.1.3. Custodia de los soportes 15
6.1.MEDIDAS DE NIVEL BASICO 15
6.2. MEDIDAS DE NIVEL MEDIO 15
6.2.1. Responsable de Seguridad 15
6.2.2. Auditoría 15
6.3. MEDIDAS DE NIVEL ALTO 16
6.3.1. Almacenamiento de la información 16
6.3.2. Copia o reproducción 16
6.3.3. Acceso a la documentación 16
6.3.4. Traslado de documentación 17
7. DERECHOS, FUNCIONES Y OBLIGACIONES DE LOS USUARIOS 17
7.1. OBLIGACIONES GENERALES 17
7.1.1. Identificación de responsables 18

7.1.2. Uso y finalidad de la Información personal. 19
7.1.3. Actualización de la información personal 21
7.1.4. Cumplimiento de indicaciones de otros departamentos 21
7.1.5. Obligaciones Como Responsable de la información 22
7.1.6. Obligaciones Como Encargado de la información 22
7.1.7. Derechos del titular 22
7.1.8. Procedimiento Para El Ejercicio De Los Derechos Del Titular 23
7.1.8.1. Contactos: 23
7.1.8.2. Procedimiento de Consulta de la Información 23
7.1.8.3. Procedimiento de Reclamación 23
8. CREACIÓN, MODIFICACIÓN O BAJA DE ARCHIVOS 24
8.1.CREACIÓN DE NUEVOS ARCHIVOS 24
8.2. MODIFICACION DE ESTA POLITICA 25
9. PROCEDIMIENTO DE DIVULGACIÓN 25
10. PERMANENCIA DE LAS BASES DE DATOS: 25
11. CONFIDENCIALIDAD Y SEGURIDAD 25
11.1. Evaluacion de impacto de proteccion de datos 25
12. VIGENCIA ..... 25.

1. INTRODUCCIÓN

El artículo 17 de la Ley Estatutaria 1581/2012, de 17 de octubre, de Protección de Datos de Carácter personal, establece que:

"Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad (…) K) 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"

El objetivo del presente Documento de Seguridad es describir e Informar al Titular sobre el uso, destinación y finalidad del tratamiento de la información personal y los derechos que le asisten, así como las medidas de índole técnica y organizativas existentes en **B&C Corporation**., (en adelante "**B&CC**" o la "Entidad"), en lo que se refiere a la seguridad de los archivos, automatizados o no automatizados, centros de tratamiento, locales, equipos, sistemas, sistemas de almacenamiento, programas y personas que intervienen en el tratamiento de los datos de carácter personal, con el objetivo de garantizar la seguridad, confidencialidad e integridad de los mismos y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

El Documento de Seguridad surge como adecuación a las disposiciones vigentes en materia de seguridad de los datos de carácter personal, correspondiente a el Artículo 15 de la Constitución Política de Colombia ("habeas data"), la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas que la modifican, adicionan, complementan o desarrollan. Las principales disposiciones a la citada ley se corresponden con las siguientes:

- EL Artículo 15 de la Constitución Política de Colombia ("habeas data")
- La Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.**,** aprobado en el Congreso de la Republica de Colombia el 17 de octubre de 2012.
- El Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012 aprobado por el presidente de la Republica de Colombia el 27 de julio de 2013

El presente documento recoge todas las medidas, normas, procedimientos, reglas y estándares adoptados por **B&CC**, encaminados a garantizar los niveles de seguridad exigidos por la Ley 1581 de 2012 y el Decreto 1377 de 2013, así como una relación de los datos de carácter personal, descripción de los sistemas de información y documentos que contienen dichos datos, así como los sistemas que los tratan de identificación de las funciones y obligaciones del personal con acceso a los mismos. Este documento y sus procedimientos Anexos (disponibles en la Intranet de B&C Corporation - https://www.bccorporation.org -) están, redactados en cumplimiento de lo dispuesto en Ley 1581 de 2012 y el Decreto 1377 de 2013 y recogen, por tanto, las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento. Asimismo, tiene como finalidad la de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado. Es por ello imprescindible, definir las medidas, normas, políticas y procedimientos de seguridad que permitan obtener y mantener el nivel de seguridad de la información adecuada a la criticidad de los datos y procesos que se almacenan y gestionan en **B&CC**.

Las personas con acceso a los datos de carácter personal y a los sistemas de información de **B&CC**, deben ser conscientes de la necesidad de preservar la información y de las consecuencias que acciones inapropiadas en este sentido pueden ocasionar a la Entidad. Es por ello, que el personal con acceso a los datos de carácter personal y a los sistemas de información de **B&CC**, es informado periódicamente de todas las normas de seguridad que afectan al desarrollo de sus funciones, así como de las consecuencias en caso de incumplimiento.

Las normas de seguridad contenidas en este documento afectan a todas las estructuras organizativas de **B&CC** y deben ser cumplidas y observadas por todo el personal con acceso a los datos de carácter personal y a los sistemas de información de la Entidad. Cualquier violación de estas medidas, normas y procedimientos podrá conllevar una acción disciplinaria consecuente con la infracción, así como las acciones legales oportunas.

Con el objetivo de divulgar el conocimiento de las normas de seguridad, a las que hace referencia este documento, se ha elaborado y difundido una notificación tal y como se establecen el Apartado 8 del presente documento.

Este documento deberá mantenerse permanente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de estos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión del presente documento y, si procede, su modificación total o parcial

2. DEFINICIONES

A los efectos del presente documento se entenderá por:

a) **Datos de carácter personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables.
b) **Datos sensibles:** Aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación.
c) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
d) **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento en razón de una relación comercial o jurídica con la compañía, sea cliente, proveedor, empleado, o cualquier tercero.
e) **Cliente:** Toda persona para quien la compañía presta un servicio o con quien sostiene una relación contractual/obligacional.
f) **Proveedor:** Toda persona natural o jurídica que preste algún servicio a la compañía, en virtud de una relación contractual/obligacional.
g) **Tratamiento de datos**: Cualquier operación, o conjunto de operaciones, que se realice sobre datos personales, tales como recolección, almacenamiento, uso, circulación, supresión, operaciones y procedimientos técnicos de carácter automatizado o no, grabación, elaboración, modificación, consulta, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
h) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida solo o conjuntamente sobre la finalidad sobre la base de datos y/o el tratamiento de los datos (El "Responsable) El Responsable de la base de datos será **B&CC** y el Encargado del Tratamiento la persona física designada por **B&CC** para llevar a cabo las funciones del Responsable del Archivo.
i) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, que por cuenta del responsable realice el tratamiento de datos personales, como Responsable de los datos (el "Encargado").
j) **Transferencia:** Es cuando el Responsable y/o el 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.

k) **Trasmisión:** 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.
l) **Centros de tratamiento**. Dentro de este concepto se engloban los distintos recursos (locales, equipos, sistemas, comunicaciones, etc.) que intervienen en el tratamiento de los datos de carácter personal.
m) **Copia de seguridad, copia de respaldo o *backup***. Copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida
n) **Documento.** Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
o) **Archivo**: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
p) **Base de datos no automatizada:** Todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.
q) **Personas**: todas aquellas personas, pertenecientes o no a la Compañía, que intervienen en el tratamiento y gestión de los datos de carácter personal.
r) **Perfil de usuario**: accesos autorizados a un grupo de usuarios.
s) **Programas y aplicaciones**: relación de aplicaciones que intervienen en el tratamiento de los datos de carácter personal de la Entidad.
t) **Recurso protegido:** cualquier parte componente de un sistema de información, ya sea éste automatizado o no
u) **Responsable de Seguridad**: persona o personas a las que el responsable del archivo ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
v) **Sistemas de tratamiento**: Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
w) **Usuario**: Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.
x) **Leyes de protección de datos**: significa en relación con los datos personales que se procesan en cumplimiento del acuerdo de servicio, el Reglamento general de protección de datos (UE) 2016/679 ("GDPR") junto con todas las leyes de implementación y cualquier otra protección de datos aplicable, leyes de privacidad o regulaciones de privacidad;
y) **Subprocesador:** significa cualquier procesador de datos designado por el Responsable del Tratamiento para procesar Datos Personales en nombre del titular.

Para el resto de los términos utilizados, se estará a lo establecido en las definiciones de la Ley 1581 de 2012, los decretos que la reglamentan, y a la política general de tratamiento de datos de la compañía respectivamente.

3. ÁMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD

En este capítulo se determina el ámbito de aplicación del presente documento con especificación de los recursos protegidos que dan soporte a los sistemas de información de **B&CC**. Por ello, para determinar los recursos protegidos de la Compañía se han tenido en cuenta los siguientes componentes, definidos en el apartado anterior del presente documento:

- Datos De Carácter Personal
- Base de datos no automatizada

- Documento
- Programas y aplicaciones
- Sistemas de tratamiento
- Tratamiento de datos
- Centros de tratamiento
- Personas
- Perfil de usuario
- Responsable del tratamiento

Estos recursos protegidos pueden ser englobados dentro de tres ámbitos de aplicabilidad del Documento de Seguridad:

- Ámbito Jurídico: Determina la Entidad Jurídica a la que aplican las medidas descritas en el presente documento.
- Ámbito Personal: Incluye el recurso protegido definido como personas.
- Ámbito Material: Comprendido por todos aquellos archivos, programas y aplicaciones que los materializan, así como los centros de tratamiento de los archivos.

El ámbito de aplicación abarca, por tanto, los sistemas que de alguna forma participan en el almacenamiento o tratamiento de la información de **B&CC**. Además, se tienen en cuenta las instalaciones que dan soporte a los sistemas de información.

Ámbito jurídico

Este documento se aplicará a B&C Corporation.

Ámbito personal

El presente Documento de Seguridad, incluyendo sus procedimientos anexos, es de obligado cumplimiento para todo el personal de la Entidad, incluido el personal externo que presta servicios en las oficinas e instalaciones de **B&CC** y con acceso a datos de carácter personal. Las normas internas contenidas en los Apartados 3, 4, 5 y 6 del presente documento se han puesto en conocimiento de todo el personal de la Entidad con el objeto de dar debido cumplimiento a la obligación contenida en la Ley 1581 de 2012.

El personal Encargado del Tratamiento de archivos con datos de carácter personal que presta sus servicios mediante conexiones remotas o bien realiza el tratamiento de los archivos en sus locales, será responsable del cumplimiento de las medidas de seguridad y los aspectos de índole jurídica en el ámbito de la protección de datos, según se recoge en los correspondientes contratos de encargos de tratamiento, y descritos en el presente Documento de Seguridad. Así mismo, en el Apartado 6 del presente documento, se describen de manera detallada las funciones y obligaciones por parte de terceros con acceso a datos de carácter personal.

Ámbito material

Es de aplicación a todos los archivos físicos que contengan datos de carácter personal en poder de **B&CC**. En el Anexo 25, del presente capítulo, puede consultarse la relación de estos. Las medidas establecidas en él son de obligado cumplimiento para el personal directivo y para los empleados de **B&CC.**

Legislación aplicable:

- EL Artículo 15 de la Constitución Política de Colombia ("habeas data")
- La Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.**,** aprobado en el Congreso de la Republica de Colombia el 17 de octubre de 2012.
- El Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012 aprobado por el presidente de la Republica de Colombia el 27 de julio de 2013

4. MEDIDAS DE SEGURIDAD APLICABLES A ARCHIVOS Y TRATAMIENTOS AUTOMATIZADOS Y NO AUTOMATIZADOS

Las medidas de seguridad que se contemplan en el artículo 19 del el Decreto 1377 de 2013 en concordancia con las categorías especiales previstas en la Ley 1581 de 2012, se han establecido atendiendo a la naturaleza de la información tratada. El carácter de la información obliga a establecer medidas en consonancia con su clasificación. Así, se considera:

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

El Responsable de Seguridad de cada Base de Datos supervisará el desarrollo, para cada uno de los archivos existentes, de tal forma que se recogerá el nombre del archivo, su estructura, el nivel de seguridad que le corresponde, los departamentos o áreas que tienen acceso a la información, así como el detalle de cuanta información sea necesaria para el cumplimiento de la legislación vigente.

Con el objeto de dar debido cumplimiento a lo establecido en el Artículo 15 de la Constitución Política de Colombia ("habeas data"), Ley 1581 de 2012 y El Decreto 1377 de 2013, **B&CC** ha establecido las siguientes medidas de seguridad, que deberán ser conocidas, aceptadas y respetadas por todo el personal. Para el efectivo cumplimiento de las medidas de seguridad, es necesario cumplir además con las políticas establecidas en los Apartados 4 y 5 del presente documento.

Con el fin de garantizar el cumplimiento de las medidas de seguridad relativas al tratamiento de la información el Anexo 8 se describe la periodicidad de cada uno de los controles que se realizan.

5. MEDIDAS DE SEGURIDAD APLICABLES A ARCHIVOS Y SISTEMAS AUTOMATIZADOS

5.1. MEDIDAS DE NIVEL BÁSICO

5.1.1. Identificación y autenticación

Dada la importancia de los accesos de los usuarios a los sistemas de información, **B&CC** posee un mecanismo que permite la identificación de forma inequívoca y personalizada de todo aquel usuario que intenta acceder a los sistemas de información y verifica que éste está autorizado.

El mecanismo de identificación se basa en la asignación de identificadores a cada uno de los usuarios que acceden a los sistemas de información.

El mecanismo de autenticación de usuarios a los sistemas de información de **B&CC** se basa en la existencia de contraseñas. Para algunos casos, códigos de confirmación (firma) confidenciales.

Con el objetivo de garantizar la confidencialidad e integridad de las contraseñas, así como de la información residente en los sistemas de información de la Entidad, a la que podría tenerse acceso a través de dichas contraseñas, se han definido y establecido procedimientos de asignación, distribución y almacenamiento de las claves que permiten el acceso de usuarios a los sistemas. Estos procedimientos obligan a cambiar con una determinada periodicidad, siempre inferior al año, las contraseñas de acceso y mientras están vigentes quedan almacenadas de forma ininteligible. El detalle del procedimiento de asignación, distribución y almacenamiento de contraseñas se detalla en el Anexo 3 del presente documento.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado de identificación y autenticación de usuarios y asignación de privilegios de acceso pueden encontrarse en el Anexo 2, Procedimiento de Identificación y autenticación, del presente documento.

5.1.2. Control de Acceso

Dada la importancia de los accesos de los usuarios a los sistemas de información, **B&CC** posee los mecanismos necesarios para obtener una relación actualizada de los usuarios y perfiles que tienen acceso autorizado a los sistemas de información de la Entidad.

El personal subcontratado que realiza tratamiento sobre archivos con datos de carácter personal tendrá las mismas obligaciones y condiciones que los empleados de **B&CC**.

El acceso lógico y operativo de los usuarios a los recursos de **B&CC** está permitido exclusivamente en función de las necesidades derivadas de la actividad profesional que realizan. Adicionalmente, existen mecanismos para evitar accesos de usuarios a recursos con derechos distintos de los autorizados.

Única y exclusivamente el personal que gestiona los sistemas podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable o encargado de tratamiento de cada uno de los archivos de carácter personal.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 4 "Procedimiento de Control de Acceso" de este Documento.

5.1.3. Archivos Temporales

Los archivos temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo al tipo de información que contengan. De este modo, deberán exigírseles las mismas medidas de seguridad que a los archivos de datos que se generarán a lo largo del ciclo de vida de los procesos.

Todo archivo temporal (automatizado o no automatizado) deberá ser borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Los procedimientos de seguridad que permiten a **B&CC** cumplir el nivel de seguridad definido sobre los archivos temporales se describen en el Anexo 5 "Procedimiento de tratamiento de archivos temporales" de este Documento.

5.1.4. Gestión de Soportes

B&CC dispone de un procedimiento, tal y como se recoge en el Anexo 6 "Gestión de soportes" de este documento, por el cual se permite controlar los soportes informáticos y documentos que contengan datos de carácter personal mediante mecanismos que permitan la identificación y la gestión del inventario de estos.

Adicionalmente, **B&CC** ha establecido los mecanismos necesarios que garanticen que únicamente el personal autorizado tiene acceso a los soportes que contienen información con datos de carácter personal.

Quedan fuera del procedimiento de inventario de soportes la gestión de los correos electrónicos con archivos adjuntos que contienen datos de carácter personal por parte del personal autorizado para el desempeño de sus funciones.

La salida de soportes que contienen datos de carácter personal fuera de los locales del responsable del archivo será convenientemente autorizada por **B&CC**. Asimismo, en el traslado de la documentación con datos de carácter personal se establecerán las medidas necesarias para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 6 "Gestión de soportes" de este Documento.

En cuanto a aquellos soportes que vayan a ser desechados o reutilizados, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en ellos, previamente a que se proceda a su baja en el inventario.

En los soportes que vayan a salir fuera de los locales del Responsable del Archivo como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

5.1.5. Copias de Respaldo. Procedimientos de generación y recuperación de copias de seguridad.

Considerándose en **B&CC** la información como un activo estratégico para la organización, se han definido procedimientos para la realización de Copias de Respaldo y la recuperación de datos de carácter personal.

En dichos procedimientos se detallan la periodicidad de estas, la identificación de los soportes y la custodia de éstos. Así mismo, dichos procedimientos garantizan la reconstrucción de los datos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción de estos.

El Responsable del Tratamiento o el Encargado del Tratamiento de cada archivo, cuando esta función esté externalizada, se encargarán de verificar la definición, funcionamiento y correcta aplicación de los procedimientos de Copia de Respaldo y recuperación, con una periodicidad no superior a los seis meses.

Dentro de las políticas existentes en lo que se refiere a la realización de Copias de Respaldo se ha establecido la obligatoriedad de realizar una Copia de Respaldo semanal como mínimo. Ésta y otras políticas, normas y procedimientos se describen en el Anexo 7 "Copias de seguridad" de este documento.

En **B&CC** se establecerán las políticas, normas, medidas y procedimientos que se estime necesario para que las pruebas anteriores a la implantación o modificación de los sistemas de información que traten archivos con datos de carácter personal no se realicen con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de archivo tratado. En caso de ser necesario llevar a cabo pruebas con datos reales, previamente será realizada una copia de seguridad de los archivos con datos de carácter personal afectados.

En el Anexo 11 "Protección de datos reales en el entorno de pruebas" de este documento se describen los procedimientos seguidos en la Entidad para la realización de pruebas.

5.1.6. Tratamiento de datos fuera de los locales

En aquellas ocasiones en las que se está realizando un tratamiento de la información fuera de los locales del Responsable de Archivo, ésta debe realizarse tras disponer de la correspondiente autorización para poder llevar a cabo la ejecución del citado tratamiento.

En los casos no habituales de tratamiento de datos fuera de los locales **B&CC**, será necesario contar con la autorización expresa del Responsable de Tratamiento.

De forma adicional, deberá garantizarse que las medidas de seguridad de los sistemas en los que dicha información va a ser tratada se ajustan a las medidas correspondientes al tipo de información tratada atendiendo a lo establecido en la ley, Ley 1581 de 2012 y El Decreto 1377 de 2013.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 12 "Tratamiento de datos fuera de los locales de la Entidad" de este documento.

5.1.7. Registro de Incidencias

Considerando como un tipo de incidencia cualquier anomalía que pudiese afectar a la seguridad de los datos de carácter personal, **B&CC** ha establecido un procedimiento para la notificación y gestión de dichas incidencias.

Este procedimiento permite registrar de cada incidencia notificada el tipo y objeto, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica, el estado, la prioridad y los efectos derivados de la misma, así como las medidas correctoras aplicadas para su resolución. En aquellos casos en que no sea posible la determinación del momento en que se produjo, se registrará el momento de su detección.

En el Anexo 15 "Procedimiento de Notificación, gestión y respuesta ante las incidencias" de este documento se describe en detalle el procedimiento de notificación, gestión y respuesta ante las incidencias.

5.2. MEDIDAS DE NIVEL MEDIO

5.2.1. Responsable de Seguridad

B&CC, como Responsable de los Archivos de datos de carácter personal, designará uno o varios Responsables de Seguridad, encargados de coordinar y controlar las medidas de seguridad definidas en este documento.

En ningún caso esta designación del Responsable de Seguridad supone una delegación de la responsabilidad que corresponde a **B&CC** como persona jurídica responsable del archivo.

En el Apartado 7 del presente Documento de Seguridad, se incluye una relación de las funciones del Responsable de Seguridad.

5.2.2. Auditoría

Los sistemas de información e instalaciones de tratamiento de datos se someterán periódicamente a una auditoría interna o externa, encargada de verificar el cumplimiento de la Ley 1581 de 2012 y El Decreto 1377 de 2013 y de los procedimientos e instrucciones vigentes en materia de seguridad de los datos.

La periodicidad de estas auditorías será fijada por **B&CC**, pero no será nunca superior a dos años. Asimismo, en caso de se produzcan cambios significativos en los sistemas de información, se realizará una auditoria de carácter extraordinario tras la finalización de los procesos de cambio.

Los informes de auditoría resultantes de las revisiones realizadas por los auditores deberán dictaminar sobre la adecuación a la Ley 1581 de 2012 y El Decreto 1377 de 2013 de las medidas y controles existentes en la Entidad, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias. Dichos informes deberán aportar la evidencia necesaria (datos, hechos, observaciones, etc.) que soporte los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de auditoría serán analizados por el Responsable de Seguridad competente, que elevará las conclusiones para que **B&CC**, adopte las medidas correctoras adecuadas.

5.2.3. Identificación y Autenticación

Para los archivos automatizados con datos de carácter personal de nivel medio, el mecanismo de identificación y autenticación de usuarios limita la posibilidad de intentar reiteradamente el acceso no autorizado a los sistemas de información.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse dentro del Anexo 2 "Procedimiento de identificación y autenticación de usuarios" de este documento.

5.2.4. Control de Acceso Físico

Única y exclusivamente el personal autorizado podrá tener acceso a los locales donde se encuentran ubicados los sistemas de información con datos de carácter personal.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 9 "Procedimiento de control de Acceso de Acceso Físico al Centro de Procesamiento de Datos (CPD)" y el Anexo 10 "Procedimiento de Control de Acceso a Edificios" de este documento.

5.2.5. Gestión de Soportes

En lo que se refiere a la gestión de soportes informáticos o de otra índole que pudieren contener datos de carácter personal, el registro sobre la entrada y/o salida de los mismos, es gestionado y actualizado por el Área de IT Systems, y debe adaptarse para permitir conocer, de forma directa o indirecta, la siguiente información: tipo de soporte, la fecha y hora de entrada, el emisor, el número de soportes o documentos, el tipo de información que contiene el soporte, la forma de envío y la persona responsable de la recepción y envío que deberá estar debidamente autorizada.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 6 "Gestión de soportes y documentos" de este documento.

5.2.6. Registro de Incidencias

En el registro de incidencias existente en **B&CC**, deberán consignarse los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, los datos que haya sido necesario grabar manualmente en el proceso de recuperación.

Adicionalmente, será necesaria la autorización expresa del Responsable del Archivo para la ejecución de los procedimientos de recuperación de los datos.

En el Anexo 15 "Procedimiento de Notificación, gestión y respuesta ante las incidencias" de este documento se describe en detalle el procedimiento de notificación y gestión de incidencias existente.

5.3. MEDIDAS DE NIVEL ALTO

5.3.1. Distribución de soportes

La identificación de los soportes se realizará empleando sistemas de etiquetado comprensibles y siguiendo una nomenclatura tal que permita la identificación al personal con acceso autorizado a dichos soportes y documentos, pero sea desconocida y dificulte su acceso al resto de personas.

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien, utilizando mecanismos que garanticen la ininteligibilidad y la no manipulación de la información durante su transporte.

Asimismo, los dispositivos portátiles serán cifrados cuando éstos sean empleados para el tratamiento de datos de carácter personal fuera de las instalaciones de **B&CC**. En aquellos casos en los que no sea posible el cifrado de los datos, dada la naturaleza de los dispositivos, será autorizado por parte del Responsable del Archivo el uso de los mismos fuera de los locales, así como analizados los riesgos y necesidades del uso de los mismos para el desempeño de las funciones. En cualquier caso, el usuario será responsable de vigilar y salvaguardar dichos dispositivos en todo momento.

5.3.2. Registro de Accesos

Para aquellos archivos de nivel alto sobre los que se realizan accesos múltiples, es decir, por parte de varios usuarios, el registro de acceso a datos de carácter personal considerados de nivel alto por su naturaleza, incorporará las siguientes características:

- De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó el acceso, el archivo accedido, el tipo de acceso y si ha sido autorizado o denegado.
- En caso de acceso autorizado, se guardará aquella información que permita identificar el registro accedido.
- Los mecanismos que permiten el registro de los datos detallados en los dos puntos anteriores estarán bajo el control directo del Responsable de Seguridad competente sin ser permisible, en ningún caso, la desactivación de estos.
- El periodo mínimo de conservación del registro de accesos será de dos años.

- El Responsable de Seguridad competente se encargará de realizar revisiones, con una periodicidad mínima mensual, de la información de control registrada elaborando un informe de las revisiones realizadas y los problemas detectados.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 13 "Registro de acceso a archivos de nivel alto" de este documento.

5.3.3. Copias de respaldo y recuperación

Para aquellos datos que, por su naturaleza, sean considerados de nivel alto, se realizarán las correspondientes Copias de Respaldo según los criterios establecidos por la Entidad. Adicionalmente, deberá conservarse una Copia de Respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso con las medidas de seguridad exigidas en este documento y en la Ley 1581 de 2012 y El Decreto 1377 de 2013.

En caso de no sea posible el almacenamiento de una Copia de Respaldo externa (fuera de la ubicación habitual de los sistemas informáticos), se garantizarán las medidas de seguridad para garantizar la integridad de las copias y procedimientos durante su almacenamiento, con el fin de permitir posibles recuperaciones futuras.

5.3.4. Telecomunicaciones

Para aquellos datos que, por su naturaleza, sean considerados de nivel alto, la transmisión de estos a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

6. MEDIDAS DE SEGURIDAD APLICABLES A BASES DE DATOS Y SISTEMAS NO AUTOMATIZADOS

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 18 "Criterios de Archivos no automatizado" de este documento.

6.1. MEDIDAS DE NIVEL BASICO

6.1.1. Criterios de archivo

El archivo de los soportes o documentos se realizará en archivos que garanticen la correcta conservación de los documentos, la localización y consulta de la información y posibilite el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación, cancelación y oposición al tratamiento.

6.1.2. Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal dispondrán de mecanismos que obstaculicen su apertura.

Para aquellos casos en los que los dispositivos no permitan garantizar el cumplimiento de esta norma, el Responsable del Tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 6 "Gestión de soportes y documentos" de este documento.

6.1.3. Custodia de los soportes

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de esta custodiará dichos documentos e impedirá en todo momento que pueda ser accedida por persona no autorizada.

Las políticas, normas y procedimientos que **B&CC** posee en relación con este apartado pueden encontrarse en el Anexo 17 "Custodia de archivos no automatizados" de este documento.

6.2. MEDIDAS DE NIVEL MEDIO

6.2.1. Responsable de Seguridad

B&CC, como Responsable de los Archivos de datos de carácter personal, designará uno o varios Responsables de Seguridad, encargados de coordinar y controlar las medidas de seguridad definidas en este documento.

En ningún caso esta designación del Responsable de Seguridad supone una delegación de la responsabilidad, que corresponde a **B&CC** como persona jurídica responsable del archivo.

En el Apartado 7 del presente Documento de Seguridad, se incluye una relación de las funciones del Responsable de Seguridad.

6.2.2. Auditoría

Los sistemas de información e instalaciones de tratamiento de datos se someterán periódicamente a una auditoría interna o externa, encargada de verificar el cumplimiento de la Ley 1581 de 2012 y El Decreto 1377 de 2013 en relación con los procedimientos e instrucciones vigentes en materia de seguridad de los datos.

La periodicidad de estas auditorías será fijada por **B&CC**, pero no será nunca superior a dos años. Asimismo, en caso de se produzcan cambios significativos en los sistemas de almacenamiento de archivos no automatizados, se realizará una auditoria de carácter extraordinario tras la finalización de los procesos de cambio.

Los informes de auditoría resultado de las revisiones realizadas por los auditores deberán dictaminar sobre la adecuación a lo establecido en la Ley 1581 de 2012 y El Decreto 1377 de 2013 de las medidas y controles existentes en la Entidad, identificando sus deficiencias y proponiendo las medidas correctoras o complementarias necesarias. Dichos informes deberán aportar la evidencia necesaria (datos, hechos, observaciones, etc.) que soporte los dictámenes alcanzados y las recomendaciones propuestas.

Los informes de auditoría serán analizados por el Responsable de Seguridad competente, que elevará las conclusiones para que **B&CC** adopte las medidas correctoras adecuadas. Estos informes quedarán a disposición de la Superintendencia de Industria y Comercio.

6.3. MEDIDAS DE NIVEL ALTO

6.3.1. Almacenamiento de la información

Los armarios, archivadores u otros elementos en los que se puedan almacenar archivos no automatizados con datos de carácter personal se encuentran en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas permanecen cerradas cuando no sea preciso el acceso a los documentos incluidos en el archivo.

Para aquellas áreas en las que no es posible garantizar el acceso restringido mediante mecanismos que impidan el acceso libre, se establecerán las medidas alternativas que garanticen el acceso restringido a dichas áreas únicamente al personal autorizado a dichos archivos.

6.3.2. Copia o reproducción

La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado en el Anexo 7 del presente documento.

Para aquellos casos en los que se generen copias para el tratamiento de los usuarios con de carácter temporal, una vez realizado el tratamiento de la información de los archivos o sus copias, se procederá a la destrucción de las copias o reproducciones que ya no sean necesarias de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

En el anexo 19 "Destrucción de archivos no automatizados" de este documento, se especifica la forma de proceder para la destrucción de archivos no automatizados que contengan datos de carácter personal.

En aquellos casos en los que sea necesario almacenar durante un tiempo los documentos o sus copias, una vez empleados éstos serán almacenados siguiendo los criterios de seguridad descritos en el presente documento.

En el anexo 20 "Copia de archivos no automatizados" de este documento, se indica la forma de proceder ante la necesidad de realizar copia de archivos no automatizados.

6.3.3. Acceso a la documentación

En caso de que existan archivos de nivel alto no automatizados, **B&CC** limitará el acceso a la documentación que contenga datos de carácter personal de nivel alto, únicamente al personal autorizado a tal efecto. En aquellos casos en los que sea necesario acceder por parte de terceros no autorizados a tal efecto, se establecerán los mecanismos necesarios para registrar dichos accesos.

Asimismo, en aquellos casos en los que sea necesario acceder a los documentos con datos de carácter personal de nivel alto por parte de múltiples usuarios, se establecerán los mecanismos necesarios para identificar los accesos realizados por cada uno de los usuarios.

Aunque **B&CC** no dispone de archivos no automatizados de nivel alto, en el anexo 21 "Acceso a archivos no automatizados" de este documento, se describen las directrices para el acceso a la información.

6.3.4. Traslado de documentación

Siempre que se proceda al traslado físico de la documentación contenida en un archivo, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado

7. DERECHOS, FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

7.1. OBLIGACIONES GENERALES

Con el objeto de dar debido cumplimiento a lo establecido en la Ley 1581 de 2012 y El Decreto 1377 de 2013, **B&CC** impone a su personal el cumplimiento de las obligaciones detalladas a continuación, las cuales deberán ser conocidas, aceptadas y respetadas por todo el personal.

Las figuras intervinientes en el cumplimiento de Derechos, Funciones y Obligaciones son las que se mencionan a continuación:

- Responsable del Tratamiento
- Encargado del tratamiento
- Titular de la Información
- Responsable de Seguridad
- Usuario

B&CC, dentro de los *Security Standards* de la Información publicado en la Intranet de la Entidad, incluye las directrices en las que se definen las obligaciones y responsabilidades de todas las personas con acceso a la información de carácter personal en particular y a los sistemas de información que posee la Entidad donde se albergan dichos datos. Estas políticas son de obligado cumplimiento para toda la organización. El departamento de Recursos Humanos será el encargado de informar al personal de la obligación en el cumplimiento de estos.

Todos los empleados de **B&CC** cumplirán con la normativa en vigor aplicable en cada momento, así como con las normas y procedimientos internos de la Entidad relacionados con el tratamiento y protección de datos de carácter personal.

Cualquier infracción a la normativa referida deberá ser comunicada al área de Cumplimiento Normativo dentro del departamento de Compliance a través del canal de denuncias de la Entidad, siguiendo los cauces internos habituales. En caso de existir conflictos normativos, se acudirá al superior jerárquico para que éste disponga lo que proceda hacer, comunicándose el incidente al departamento que corresponda. Salvo en caso de urgencia, se pospondrá cualquier acción en que se dude acerca de si la misma puede vulnerar alguna normativa, sea del rango que sea.

Todo empleado aceptará las obligaciones mediante firma de dichas políticas y procedimientos tal y como se define en el procedimiento referenciado en el Anexo 22 del presente documento.

7.1.1. Identificación de responsables

A continuación, se identifican los responsables que se han asignado en **B&C Corporation**, relacionados con la Ley 1581 de 2012 y El Decreto 1377 de 2013

En cumplimiento con la Ley 1581 de 2012 y El Decreto 1377 de 2013, el Responsable del tratamiento autoriza a los Encargados de realizar las acciones en su nombre en virtud de la relación, legal, contractual y reglamentaria que los gobierna.

Archivo NÓMINAS	**RESPONSABLE**
RESPONSABLE DEL ARCHIVO	B&C Corporation
RESPONSABLE DEL TRATAMIENTO	Legal Manager
ENCARGADO DEL TRATAMIENTO	Ver Anexo 25 "*Encargados del tratamiento y prestación de servicios" del presente documento.* B&C Corporation Tratamiento archivos automatizados y no automatizados
RESPONSABLE DE SEGURIDAD	Security Officer
ENCARGADOS DE CONCEDER, ALTERAR O ANULAR EL ACCESO SOBRE DATOS Y RECURSOS	Ver procedimiento LOPD – 4 "*Control de Acceso"* referenciado en el Anexo 4 del presente documento.
ENCARGADOS DE GESTIONAR LA NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS	Departamento de Soporte de B&C Corporation Ver procedimiento 15 - LOPD "Notificación, gestión y respuesta ante las incidencias" referenciado en el Anexo 5 del presente documento.

Archivo PROVEEDORES	**RESPONSABLE**
RESPONSABLE DEL ARCHIVO	B&C Corporation
RESPONSABLE DEL TRATAMIENTO	Legal Manager
ENCARGADO DEL TRATAMIENTO	Ver Anexo 25 "*Encargados de tratamiento y prestación de servicios" del presente documento.* Tratamiento archivos automatizados y no automatizados
RESPONSABLE DE SEGURIDAD	Security Officer
ENCARGADOS DE CONCEDER, ALTERAR O ANULAR EL ACCESO SOBRE DATOS Y RECURSOS	Ver procedimiento LOPD – 4 "Control de Acceso" referenciado en el Anexo 4 del presente documento. Departamento de Soporte de B&C Corporation

ENCARGADOS DE GESTIONAR LA NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS	Ver procedimiento 15 - LOPD "Notificación, gestión y respuesta ante las incidencias" referenciado en el Anexo 15 del presente documento.

Archivo CANAL DE RECLAMACIONES CARGO	**RESPONSABLE**
RESPONSABLE DEL ARCHIVO	B&C Corporation
RESPONSABLE DEL TRATAMIENTO	Director of Customer Service
ENCARGADO DEL TRATAMIENTO	Ver Anexo 25 "*Encargados de tratamiento y prestación de servicios" del presente documento.* Tratamiento archivos automatizados
RESPONSABLE DE SEGURIDAD	Director of Customer Service
ENCARGADOS DE CONCEDER, ALTERAR O ANULAR EL ACCESO SOBRE DATOS Y RECURSOS	Ver procedimiento LOPD – 4 "Control de Acceso" referenciado en el Anexo 4 del presente documento. Departamento de Soporte de B&C Corporation.
ENCARGADOS DE GESTIONAR LA NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS	Ver procedimiento 15 - LOPD "Notificación, gestión y respuesta ante las incidencias" referenciado en el Anexo 15 del presente documento.

7.1.2. Uso y finalidad de la Información personal.

No se comunicará información personal a personas no autorizadas. En caso de que exista algún requerimiento por parte de la persona afectada por la información, se tomarán las medidas oportunas, dentro de lo establecido en los procedimientos operativos de la Entidad para verificar que la persona que lo solicita es quién dice ser. No se enviará esta información por teléfono o fax, salvo autorización expresa del interesado. Los archivos de información personal no podrán enviarse por medios inseguros. Las transmisiones se encriptarán de acuerdo con los niveles de seguridad exigidos y utilizando las herramientas previstas a tal fin.

La información personal no podrá utilizarse para fines distintos de aquellos para los que se recogió. Adicionalmente, no se utilizará para, a partir del análisis de esta información, llegar a una tercera o a varias.

La capacidad de acceso a la información personal no presupone la autorización. Ningún empleado accederá a información personal que no sea estrictamente necesaria para su trabajo. Si algún empleado tuviera acceso a información de carácter personal erróneamente, deberá comunicar su capacidad de acceso a al departamento de Soporte para que haga las correcciones oportunas.

7.1.2.1 Los datos personales serán tratados con el objeto de:

a. Ejecutar el objeto social de **B&C Corporation**.

b. Cumplir con las obligaciones legales de la compañía, en razón del desarrollo de su actividad comercial.

c. Gestionar datos relacionados con recursos humanos, análisis organizacional, desarrollo y manejo de reportes de desempeño de los contratos laborales, gestión de las relaciones laborales, procesamiento, gestión, pago de nómina y cumplimiento de las obligaciones legales.

d. Administrar los asuntos internos de la compañía, incluyendo, pero sin limitarse a la contabilidad, reportes financieros y de gestión, cálculo, presentación y pago de impuestos, otros registros y reportes de cumplimiento. Esta información incluye datos personales de directores y agentes de las afiliadas de la compañía.

e. Servicio y mercadeo: Para la prestación de los servicios al cliente y el mercadeo efectuado con una red de base de clientes.

f. Realizar el proceso de "Conozca a su cliente-KYC", que consiste en el conjunto de procedimientos para la identificación y aceptación de clientes.

g. Cumplir con obligaciones legales, tales como, las recomendaciones del "Grupo de Acción Financiera" (GAFI), la "Tercera Directriz Americana" 2005/60/EC, leyes nacionales sobre lavado de activos y financiación del terrorismo, servicios financieros y servicios de cumplimiento tributario y la opinión 14/2011 del Artículo 29 sobre la protección de datos relacionadas con la prevención del lavado de activos y financiación del terrorismo del "Grupo de Trabajo de Protección de Datos".

h. Gestionar las relaciones de socios comerciales: Aquellos que pertenecen a una red internacional o a un servidor internacional de base de clientes. Los socios comerciales también serán los subcontratistas que realicen servicios a los clientes.

i. Desarrollar los negocios de la compañía: Analizando el mercado de oportunidades, la competencia y la ejecución de estrategias, para mantener e incrementar el mercado en los territorios donde **B&CC** desarrolla operaciones.

j. Administrar los servicios contractuales prestados al cliente, incluyendo, pero sin limitarse a las tarifas.

k. Procesar, gestionar y enviar la información necesaria para el procesamiento de la nómina, los pagos, ingresos, registros, novedades y demás requerimientos del sistema de seguridad social de acuerdo a la legislación colombiana.

l. Negociar con prospectos de clientes. La información obtenida no será utilizada, ni vendida, ni usada para ninguna otra negociación u objeto.

m. Pagar las obligaciones contractuales y extracontractuales.

n. Enviar información a entidades gubernamentales o judiciales, por solicitud expresa de las mismas.

o. Apoyar procesos de auditoria externa/interna.

p. Registrar la información de los empleados y/o funcionarios de los clientes en la base de datos de la compañía.

q. Registrar la información de los proveedores en la base de datos de la compañía.

r. Contactar con clientes, empleados y/o proveedores para el envío de información relacionada con las relaciones contractuales, comerciales y legales a que haya lugar.

s. Con propósitos de seguridad, prevención, investigación y persecución del fraude.

t. Almacenar los datos que por cualquier medio y con la debida autorización haya recolectado la compañía.

u. Cualquier otra finalidad que resulte en el desarrollo de la firma, negociación y/o ejecución del contrato o cualquier tipo de relación, entre el titular de la información y la compañía.

7.1.2.2. B&C Corporation no venderá, traspasará o licenciará la información recibida salvo que (i) exista autorización expresa del Titular para hacerlo y (ii) esto sea requerido y/o permitido por ley.

7.1.2.3. B&C Corporation podrá subcontratar a terceros para el procesamiento de información. Cuando efectivamente la compañía subcontrate con terceros el procesamiento de la información personal, exigirá a dichos terceros la protección de la información personal con medidas de seguridad apropiadas, así mismo prohibirá el uso de la información personal para otros fines distintos a los contratados y la divulgación de la información personal a terceros.

7.1.2.4. B&C Corporation podrá transferir y/o transmitir la información del titular a otras compañías en el extranjero por razones de seguridad o eficiencia administrativa, de conformidad con las autorizaciones de cada uno de los Titulares.

7.1.2.5 Cuando el lugar al que se vaya a realizar la transferencia y/o transmisión de Datos esté ubicado fuera de Colombia, la compañía solicitará a la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio la declaración de conformidad para la transferencia de los datos.

7.1.2.6. Una vez cese la necesidad del tratamiento de los datos personales, los mismos podrán ser eliminados de las bases de datos de la compañía o archivados en términos seguros a efectos de que solamente sean divulgados cuando a ello hubiere lugar de acuerdo con la ley.

7.1.2.7. Funciones y obligaciones específicas

Todo empleado aceptará las obligaciones mediante firma de dichas políticas y procedimientos tal y como se define en el procedimiento "Notificación y Divulgación", referenciado en el Anexo 22 del presente Documento.

Las funciones y obligaciones de las figuras intervinientes se describen en el procedimiento "Funciones y Obligaciones del Personal".

7.1.3. Actualización de la información personal

Una vez recibida nueva información personal que modifique la existente, se actualizará lo antes posible.

Queda terminantemente prohibida la modificación de información personal de forma que altere los datos reales, cualquiera que sea el motivo de esta acción.

La información acerca de datos personales se obtendrá por medio de los procedimientos prescritos en las normas internas de la Entidad. No deberá adquirirse información por otros medios.

7.1.4. Cumplimiento de indicaciones de otros departamentos.

Todos los empleados cumplirán puntualmente con las indicaciones que se reciban de los departamentos de los que dependan.

7.1.5. Obligaciones como Responsable de la información

a. Cumplir e implementar las normas de protección de datos personales y la política de la compañía.

b. Informar al cliente que desde el inicio de la relación comercial se recolectará y tratará información susceptible de protección, por lo que deberá contar con la autorización del Titular de la información.

c. Solicitar de forma previa y expresa la autorización de tratamiento de la información a toda persona que por alguna relación contractual o extracontractual deba suministrar datos sensibles.

d. Mantener actualizada la Política de tratamiento de Datos y darla a conocer a sus empleados, clientes y/o proveedores.

7.1.6. Obligaciones Como Encargado de la información

a. Solicitar a sus clientes - Responsables de la información- la certificación en la que éstos aseguren haber obtenido autorización previa de los Titulares de la información para darle tratamiento a la misma.

b. Solicitar a los clientes, como Responsables de la información, el cumplimiento de las normas de protección de datos personales.

7.1.7. Derechos del titular

De conformidad con el Artículo 8 de la Ley 1581 de 2012, los derechos que le asisten a los titulares de la información, en relación con sus datos personales son:

a. Conocer, actualizar y rectificar sus datos personales, dentro de los parámetros legales.

b. Solicitar prueba de la autorización otorgada por el Titular de la información a la compañía, como Responsables del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento.

c. Solicitar a la compañía, como Responsable o Encargado del Tratamiento, información sobre el uso que se le ha dado a los datos personales.

d. Presentar quejas por infracciones a lo dispuesto en la ley y las normas que la modifiquen, adicionen o complementen, ante la Superintendencia de Industria y Comercio.

e. Revocar la autorización y/o solicitar la supresión de datos, cuando en el Tratamiento no se respeten los principios, derechos y/o garantías constitucionales y legales; siempre que no exista una obligación legal de conservación de dichos datos.

f. Acceder en forma gratuita exclusivamente a los datos personales que hayan sido objeto de Tratamiento y conocer de las actividades que se ejecutan con su información en ocasión a dicho tratamiento.

Parágrafo: Lo anterior no significa que se dará acceso a los procesos desarrollados en relación al tratamiento de datos personales desarrollados por la compañía.

7.1.8. Procedimiento Para El Ejercicio De Los Derechos Del Titular

7.1.8.1. Contactos:

En caso de preguntas acerca de esta Política, o cualquier inquietud o reclamo respecto a la administración de esta, comuníquese a través de:

- **Nombre:** Alejandro Irirarte Yepez
- **E-Mail:** Legal@bccorporation.org
- **Dirección:** Carrera 8 #12c-35 Oficina 402, Bogotá D.C. - Colombia
- **Tel.:** +57 319 658 6808
- **Área:** Legal

Las solicitudes de rectificación, queja, actualización, consulta, acceso o de sustracción de datos, deberá ser remitida a:

- **Nombre:** Alejandro Irirarte Yepez
- **E-Mail:** Legal@bccorporation.org
- **Dirección:** Carrera 8 #12c-35 Oficina 402, Bogotá D.C. - Colombia
- **Tel.:** +57 319 658 6808
- **Área:** Legal

7.1.8.2. Procedimiento de Consulta de la Información

Para realizar consultas de información sometida a tratamiento por la compañía, el titular de dicha información deberá:

1). Remitir al área encargada (indicada en el punto 7.1.8.1.) una solicitud escrita, firmada y con diligencia de presentación personal por el titular de la información o por los causahabientes, con copia del documento de identificación del solicitante.

En caso de ser los causahabientes del titular quienes soliciten la información, deberán anexar copia del registro civil de nacimiento o matrimonio, escritura pública de sucesión o copia auténtica de sentencia judicial de sucesión, según corresponda, junto con el registro civil de defunción del titular.

2). Las solicitudes o peticiones serán atendidas en un término máximo de diez (10) días hábiles desde el recibo de la solicitud o petición.

3). Si por algún motivo el área encargada no puede atender la solicitud o petición, se informará al interesado sobre los motivos de la demora, e indicando la fecha en la cual se atenderá la consulta. Esta fecha no puede exceder los cinco (5) días hábiles siguientes al vencimiento del primer término.

4) Si la solicitud resulta incompleta, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción de la solicitud para que subsane las fallas.

5) Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la solicitud, tal como está previsto en el artículo 17 de la ley 1755 de 2015.

7.1.8.3. Procedimiento de Reclamación

1). Remitir al área encargada (indicada en el punto 6.1.2), la queja o reclamo de manera escrita, firmada y con diligencia de presentación personal ante notario por el titular de la información o por los causahabientes junto con la copia de la cédula del solicitante.

En caso de ser los causahabientes del titular quienes soliciten la información deberán anexar copia del registro civil de nacimiento o matrimonio, según corresponda, junto con el registro civil de defunción del titular.

2). Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo 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.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

3). Una vez recibido el reclamo completo, el área encargada dentro de la compañía incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

4). El término máximo para que el área encargada en la compañía atienda el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

5). Cuando el encargado dentro de la compañía no pueda atender el reclamo dentro de dicho término, se informará al interesado 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.

8. CREACIÓN, MODIFICACIÓN O BAJA DE ARCHIVOS

8.1. CREACIÓN DE NUEVOS ARCHIVOS

La creación de un nuevo archivo debe ser solicitada por el director del departamento que será usuario de este. Para ello, cumplimentará el modelo de solicitud (ver procedimiento *23 – LOPD - Creación, modificación o baja de archivos*) que se remitirá al Responsable de Seguridad de **B&CC** y al departamento de Compliance para que evalúe la necesidad de inscribir un nuevo archivo o modificar uno ya existente en el Registro General de Protección de Datos de la Superintendencia de Industria y Comercio. El Responsable de Seguridad de **B&CC** podrá valorar junto con los Responsables de Seguridad de los archivos existentes si el archivo de nueva creación puede quedar englobado dentro de alguno de los archivos lógicos ya registrados y únicamente es necesario detallarlo en el presente documento, sus anexos y/o los procedimientos que los desarrollan.

De dichas reuniones o comunicaciones, se informará a los diferentes Responsables de Seguridad de los archivos existentes y al departamento de IT Systems, en caso de que aplicase, de la procedencia o improcedencia de la creación del nuevo archivo o la inclusión en alguno de los archivos lógicos ya existentes.

Posteriormente, en caso de que se decida que se trata de un nuevo archivo lógico, se procederá a la inscripción del nuevo archivo en el Registro General de Protección de Datos de la Superintendencia de industria y Comercio. Esta acción será desarrollada por el departamento de Compliance, cumplimentando las solicitudes de la propia Agencia.

El Responsable de Seguridad de ese nuevo archivo complementará posteriormente la ficha interna facilitada por el Responsable de Seguridad de **B&CC** con las características del archivo y las medidas de seguridad que le sean de aplicación.

La persona física encargada de la gestión del alta de los archivos ante la Superintendencia de Industria y comercio será el Responsable de Seguridad de **B&CC**.

8.2. **MODIFICACIÓN DE ESTA POLÍTICA**

Esta política puede ser modificada en cualquier momento, razón por la cual se recomienda a los titulares de la información revisar periódicamente en la página web https:// www.bccorporation.org /, o a través de la intranet, donde se les avisará del cambio y se pondrá a disposición la última versión de esta política o los mecanismos para obtener una copia de la misma.

9. PROCEDIMIENTO DE DIVULGACIÓN

El Responsable de Seguridad de **B&CC**, como garante de la correcta divulgación y del cumplimiento del contenido del Documento de Seguridad, ha de comunicar (a través del departamento de RRHH) a todos los empleados con acceso a los sistemas de información de **B&CC** o a documentación con datos de carácter personal, la existencia del Documento de Seguridad, las funciones y obligaciones que como usuarios de ésta han de llevar a cabo y la importancia de su participación en el conocimiento y cumplimiento de los estándares de seguridad detallados en el mismo, para garantizar la protección y confidencialidad de los datos de **B&CC**.

Para todos los empleados de **B&CC** se realizarán sesiones periódicas de formación, con entrega de las instrucciones y material referente en materia de seguridad de la LOPD. Así mismo, se verificará la realización de dichos cursos y su finalización exitosa. De esta forma, se asegura que tanto los antiguos empleados como las nuevas incorporaciones conozcan principios y conceptos relevantes en materia de protección de datos.

Adicionalmente, para los nuevos empleados, **B&CC** requerirá la lectura y conformidad de las cláusulas de confidencialidad y protección de datos mediante la firma de la carta de oferta o al tiempo de firmarse el contrato laboral.

10. PERMANENCIA DE LAS BASES DE DATOS:

La compañía conservará los datos personales al menos durante el tiempo que las normas especiales para cada caso lo establezcan; en los casos que la Ley no establezca un término de conservación, la compañía almacenará la información indefinidamente.

11. CONFIDENCIALIDAD Y SEGURIDAD

B&CC mantendrá la confidencialidad de los Datos personales e instruirá a su personal y a los Subprocesadores. **B&CC** implementará las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad de los Datos personales adecuado al riesgo requerido de conformidad con las Leyes de protección de datos aplicables y, cuando el tratamiento se refiera a datos personales de residentes de la UE, tomará todas las medidas requeridas de conformidad con el artículo 32 del GDPR. Al evaluar el nivel apropiado de seguridad, **B&CC** deberá tener en cuenta en particular los riesgos que presenta el tratamiento, en particular de la destrucción, pérdida, alteración, divulgación no autorizada o acceso no autorizado a los datos personales transmitidos, almacenados o tratados de otra manera.

11.1 Evaluación de impacto de protección de datos

B&CC brindará asistencia razonable al Cliente con cualquier evaluación de impacto de protección de datos que se requiera de conformidad con el Artículo 35 del GDPR y con cualquier consulta previa a cualquier Autoridad de Supervisión del Cliente que se requiera de conformidad con el Artículo 36 del GDPR, en cada caso en relación con el tratamiento de datos personales por parte de **B&CC** en nombre del cliente y teniendo en cuenta la naturaleza del tratamiento y la información disponible para **B&CC.**

12. VIGENCIA:

La versión de la presente política rige a partir del 01 de noviembre de 2018