SUPERINTENDENCIA FINANCIERA DE COLOMBIA

RESOLUCIÓN NÚMERO 1891

(24 SET. 2010)

Por la cual se impone una sanción

EL SUPERINTENDENTE DELEGADO PARA RIESGOS OPERATIVOS

En ejercicio de sus facultades legales, en especial las que le confieren: ***(i)*** el numeral 2° del artículo 11.2.1.4.18 y el artículo 11.2.1.4.26 del Decreto 2555 de 2010, ***(ii)*** el numeral 4° del artículo 208 y el artículo 211 del Estatuto Orgánico del Sistema Financiero, y ***(iii)*** la Resolución No. 1685 de 6 de noviembre de 2009, mediante la cual se delegaron en el Superintendente Delegado para Riesgos Operativos las facultades para el ejercicio de la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y de terceros países, sujetos a la inspección de la Superintendencia Financiera de Colombia, de que tratan los numerales 2 al 6 del artículo 17 de la Ley 1266 de 2008, en cuanto a la actividad de administración de datos personales regulada en la misma disposición.

CONSIDERANDO:

PRIMERO: Que el **Banco de Bogotá S.A.** se encuentra sometido a la inspección y vigilancia de la Superintendencia Financiera de Colombia de conformidad con lo previsto en el artículo 11.2.1.6.1. del Decreto 2555 de 2010.

SEGUNDO: Que el 21 de septiembre de 2009 la Delegatura para Riesgos Operativos se enteró, por medio de un correo, sobre la venta de bases de datos con información confidencial de presuntos clientes financieros en el sitio Web www.youtube.com, videos en los cuales se observan archivos con registros que podrían corresponder a clientes y productos de Banco de Bogotá S.A.

TERCERO: Que la Superintendencia Financiera, por intermedio de la Delegatura para Riesgos Operativos, mediante oficio con número de radicación 2009072805 del 21 de septiembre de 2009, solicitó al Banco adelantar una investigación sobre la divulgación de videos a través del sitio Web http://www.youtube.com/watch?v=wpqHZOgbG6w en el cual se ofrecía información de clientes del sistema financiero colombiano con datos como: nombre, producto, sucursal, cupo y referencias personales.

La investigación solicitada tenía como propósito determinar si la información divulgada en dichos videos correspondía a clientes de la entidad y de ser cierto, indicar las causas, así como las medidas que adoptarían en relación con dichos clientes y los controles que se implementarían para evitar que casos como éste se vuelvan a presentar.

El Banco de Bogotá, mediante comunicación radicada con el número 2009072805-001 del 24 de septiembre de 2009, manifestó que: "(...) *Se encontró un número pequeño de coincidencias con clientes o exclientes del banco; algunos por tarjetas de crédito y otros por cuentas del pasivo* (...) "

CUARTO: Que, de otra parte, este Organismo, a través de la Delegatura para Intermediarios Financieros, mediante oficio con número de radicación 2009074329-000 del 28 de septiembre de 2009, solicitó al representante legal convocar a una reunión de la Junta Directiva, con el fin de que en dicha sesión el máximo órgano de administración analizara los efectos de la situación presentada y remitiera una copia del acta con las decisiones y pronunciamientos requeridos, a más tardar el 2 de octubre de 2009.

QUINTO: Mediante oficio No. 2009075365 del 1 de octubre de 2009, el Superintendente Delegado para Riesgos Operativos informó de una visita de inspección al Representante Legal del Banco de Bogotá S.A., la cual se realizó del 2 al 7 de octubre de 2009.

El propósito de la inspección se dirigió a:

5.1. Determinar si la información divulgada en www.youtube.com corresponde a clientes de la entidad y puede haberse originado en las bases de datos del Banco.

5.2. Evaluar el proceso de Cobranzas en lo que respecta al manejo de la información de los clientes en cuanto a: (i) generación en los aplicativos que soportan los préstamos, (ii) el envío, (iii) uso y administración y (iv) destrucción o devolución de dicha información en las casas de cobranzas contratadas para adelantar la recuperación de la cartera.

5.3. Evaluar que en el proceso mencionado se esté dando cumplimiento a los requerimientos mínimos de seguridad en el manejo de información confidencial de clientes de la entidad: ***(i)*** respecto de los registros almacenados, para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento, dentro de las facultades conferidas a esta Superintendencia por el numeral 3 del artículo 17 de la Ley 1266 de 2008 (Ley de Habeas Data), así como ***(ii)*** la aplicabilidad de los numerales 3.1.1. y 3.2.5. de la Circular Externa Básica Jurídica 007 de 1996 Titulo I, Capitulo XII, frente a los terceros que, en desarrollo de su actividad, tienen acceso a la referida información.

SEXTO: Que el Banco de Bogotá, mediante comunicación radicada con el número 2009074329-001 del 2 de octubre de 2009, manifestó:

> *"(...) Al recibir el martes 29 de septiembre su comunicación de la referencia, la Junta Directiva se encontraba reunida en sesión ordinaria. Inmediatamente se trató este tema, los Directores recibieron la información correspondiente y dieron las orientaciones contenidas en el extracto del Acta No. 959, correspondiente a dicha reunión.*

(...) Con base en estos cruces, el resultado fue: total registros de youtube como del Banco de Bogotá: 96; de esos, 34 cédulas coinciden con las de clientes del Banco de Bogotá,

(...) Sólo un caso había sido gestionado por casas de cobranzas externas. Finalmente, coincidencia de cédula, nombre, tenencia de tarjeta de crédito y teléfono sólo encontramos en 19 casos. (...)"

SÉPTIMO: Que mediante oficio radicado con el número 2009075365-006-000 del 1° de diciembre de 2009, se formularon cargos institucionales a **Banco de Bogotá S.A.**, concediéndole un plazo improrrogable de treinta (30) días hábiles[1] para rendir explicaciones por los hechos y razones de derecho que allí se expusieron, de conformidad con lo dispuesto por los literales g) y h) del numeral 4° del artículo 208 del Estatuto Orgánico del Sistema Financiero.

OCTAVO: Que mediante comunicación radicada bajo el número 2009075365-011-000 del 28 de enero de 2009, **Banco de Bogotá S.A.,** actuando por conducto de su representante legal, doctor Alberto Pérez Vélez, rindió explicaciones de carácter institucional dentro del término establecido para el efecto.

NOVENO: Que las pruebas de la actuación administrativa son las indicadas en el acápite III del pliego de cargos citado en el considerando SEGUNDO anterior, toda vez que la entidad no solicitó ni allegó pruebas junto con su escrito de descargos.

DÉCIMO: Que, de acuerdo con lo establecido en el artículo 35 del Código Contencioso Administrativo en concordancia con el numeral 4 del artículo 208 del Estatuto Orgánico del Sistema Financiero, una vez vencido el término de traslado y agotada la etapa probatoria es procedente adoptar una decisión de fondo en la presente diligencia, esto es, determinar la procedencia de la sanción a que haya lugar o el archivo de la actuación si fuera del caso.

DÉCIMO PRIMERO: Que la imputación formulada al **Banco de Bogotá S.A.** se encuentra sustentada en los siguientes hechos:

11.1. SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN

11.1.1. a) Verificación de la información publicada en Internet

La entidad manifestó que la información que aparece publicada en Internet, en el sitio www.youtube.com, no guarda relación con las bases de datos del Banco. La Comisión de Inspección efectuó consulta a las tablas maestras de la base de datos de producción y a la de ICS (que maneja la Gerencia Nacional de Cobranzas), contra los registros del video publicado.

A continuación se presentan los resultados obtenidos por el Banco y por la Comisión, en los que se observan algunas diferencias:

---

[1] Contados a partir de la fecha de recibo de la comunicación, esto es, del 14 de diciembre de 2009.

Concepto	Banco	Visita
Registros del video anunciados como clientes del banco	96	96
Registros del video que existen como clientes del banco en la BD de producción (consulta por CC) (*)	34	33
Coincidencia de información (CC y nombre) del video y la BD de producción	19	33
Coincidencia de información (CC, nombre, TC y tel.) del video y la BD de producción	19	29
Clientes existentes en la BD de producción y en la BD de ICS, de los anunciados en el video	-	24 de 96
Clientes del banco que aparecen en el video, enviados a casas de cobranza (según consultas a la BD de ICS)	16	17
Clientes del banco que aparecen en el video, enviados al call center (según consultas a la BD de ICS)	-	7

(*) El Banco hizo la consulta mediante sus aplicativos, mientras que la comisión de inspección lo hizo con SQL sobre la tabla maestra de la base de datos de producción.

De los cruces de información realizados es importante destacar las siguientes situaciones:

- Los números de identificación aparecen con el digito 1 antepuesto, tanto en la BD de producción, en la BD de ICS, como en el video. Para el Banco este dígito corresponde al tipo de documento (cédula de ciudadanía).

- La forma en que aparecen registrados los nombres y apellidos en el video y la tabla maestra de clientes de la base de datos de producción del banco, es igual. Por ejemplo: PATIÑO GONZALEZ PEDRO, PENA LEON OSCAR MAURICIO Y MUNOZ QUEZADA CARLOS ARTURO. En estos tres casos los nombres están en mayúscula sostenida, PATIÑO está escrito con Ñ mientras que PENA y MUNOZ están escritos con N.

Por lo tanto, teniendo en cuenta la similitud en los parámetros, luego del cotejo, la Comisión de Inspección concluye que la información publicada en los videos anunciados en Internet puede haberse originado de las bases de datos del Banco.

b) Atención a clientes morosos en Oficinas del Banco de Bogotá

El Banco ha dispuesto en dos de sus oficinas (Bogotá y Barranquilla) la atención a clientes morosos, en las que cuenta con la participación de personal de las casas de cobranza.

La comunicación del personal de las casas de cobranza que se encuentra en estos puntos de atención se realiza a través de una Vlan - segmento virtual de red, el cual está conformado por un switch Cisco 2950, un firewall (appliance Check Point) y un switch 4503 nivel 3 (nodo principal). Estos dispositivos están conectados físicamente con cable UTP. El primer switch se usa para enlazar los PC´s usuarios (casa de cobranza) con el firewall.

El Firewall valida la IP de origen y destino; una vez autorizado, el paquete pasa al segundo switch encargado de crear el segmento de red entre la oficina y el centro de cómputo del Banco, para lo cual utiliza fibra óptica oscura (proveedor ETB – iluminada y administrada por el Banco).

Al respecto, la Comisión evidenció que la información transportada entre los PC (clientes - casa de cobranzas), ubicados en las oficinas del Banco, y el nodo principal de la misma (switch 4503), no es cifrada y que el canal por el que viaja no cuenta con mecanismos que garanticen su seguridad.

La anterior situación se torna de alto impacto, ya que se puede ver comprometida la confidencialidad de la información, teniendo en cuenta que el Banco, además, excluye de cifrado el tráfico de telefonía IP, voz IP y control de enrutadores, elementos utilizados en los puntos de atención del personal de las casas de cobranza y en las oficinas externas en las que éstas realizan su gestión.

c) Administración del Aplicativo ICS (Internet Colection System) - Sistema de información de Cobranzas para Cartera Vencida

Mediante esta herramienta la Gerencia Nacional de Cobranzas (GNC) administra la cartera vencida del Banco. La base de datos que maneja, contiene la información histórica de los clientes que presentan vencimientos a partir de un día en cualquiera de los productos.

Este aplicativo es administrado por dos funcionarios de la Gerencia Nacional de Cobranzas y dentro de las actividades desarrolladas por ellos se encuentran la de perfilar, asignar y autorizar a los usuarios del mismo.

Sobre el particular, la comisión de inspección evidenció que se llevan a cabo procedimientos que afectan la seguridad y calidad de la información, a saber:

- El funcionario a cargo del perfilamiento y asignación de usuarios cuenta además con privilegios para realizar consultas directas a la base de datos, actividad que ejecuta con la herramienta "SQL*PLUS Worksheet".

- El aplicativo está parametrizado para que siete clientes (asesores de las casas de cobranzas) utilicen el mismo usuario y clave de acceso.

11.1.2. Gestión de Cobranzas: El Banco de Bogotá realiza en su Call Center la cobranza de la cartera vencida que presenta una altura de mora de 1 a 90 días y contrata los servicios de abogados externos y de casas de cobranza para la recuperación de la cartera con un vencimiento superior.

La Comisión de Inspección efectuó visitas in-situ a los procesos que se realizan en el Call Center y en la casa de cobranza Colcartera EU.

a) Casa de Cobranza "Colcartera EU": Está clasificada como "Agencia Extrajurídico" y tiene asignada cartera con un vencimiento superior a 210 días que no puede ser judicializada. Al 30 de septiembre de 2009 tenía asignados 2.504 clientes de la ciudad de Bogotá que adeudaban $3.851 millones aproximadamente.

Esta empresa ocupa el sexto lugar entre las 18 casas de cobranza ubicadas en Bogotá, de acuerdo con el número de clientes asignados. En la inspección in-situ realizada, la comisión observó lo siguiente:

- En los PC´s de los supervisores a cargo de la campaña del Banco de Bogotá se encontraron instalados los aplicativos de MS-Office: Outlook, (sin restricciones), Excel y Word; el Reproductor de MS-Windows Media, Oracle for Windows NT, Internet Explorer, entre otros. Estos aplicativos no son necesarios para la labor que realizan dichos funcionarios.

- Las funcionarias de la casa de cobranza "Colcartera EU" tienen como práctica bajar información del Aplicativo ICS a MS-Excel con el fin de controlar la gestión que realizan. Dicha información corresponde a los siguientes campos: CED_SIN_DIG, CEDULA, NOMBRES, GRUPO, ESTADO, COBERTURA, REGION_MAX_MORA, OFIC_MORA_Q_PROD, SALDO_CL, RANGO_SALDO, MORA_CL, PAGOMIN_CL, DIAS_CL, RANGOS_CL, FRANJA, ESTADO_CLIENTE, ENTIDAD_CL, ABOGADO, CONDICION, X, ETAPA, CAMPAÑA, NUEVO_GRUPO, AGENCIA_DEF y OBS_ICS; evidenciando de esta manera que cuentan con la posibilidad de copiar o enviar por correo esta información a personas no autorizadas.

- El contrato suscrito entre Colcartera EU y la cooperativa de trabajo asociado que suministra el personal, no cuenta con cláusulas de confidencialidad, ni tampoco los contratos celebrados entre dicha cooperativa y cada uno de sus empleados, a pesar de lo convenido entre el Banco y esta casa de cobranza en el "Acuerdo de Confidencialidad" (anexo 4) en el cual se cita: "*mantener en confidencia la Información Confidencial y Documentos de la Parte Dueña de la Información, tomando en este sentido las mismas medidas de seguridad y ejerciendo los mismos cuidados que los aplicados por la Parte Receptora a su propia información confidencial; la Parte Receptora garantiza, además, que estas medidas y cuidados ofrecen una protección adecuada contra la*

divulgación, reproducción o utilización no autorizadas" compromiso que se ratifica en el respectivo reglamento.

Así mismo, se observó que en el "Acuerdo de Confidencialidad" no se incluyeron las políticas y procedimientos de seguridad informática que se deben aplicar en el uso del sistema de información ICS, puesto a disposición de las casas de cobranza.

Adicionalmente, el Banco no había realizado seguimiento o monitoreo a los mecanismos adoptados por la casa de cobranza para guardar y mantener la reserva y confidencialidad de la información, conforme a lo acordado en el "Reglamento casas de cobranzas externas Banco de Bogotá". Lo anterior, a pesar de que la entidad realiza visitas a las casas de cobranza por parte de personal de la Gerencia Nacional de Cobranza, ya que éstas se relacionan únicamente con la verificación de la gestión que realizan, según lo manifestado por la Gerente Nacional de Cobranzas en entrevista efectuada el 2 de octubre de 2009.

b) Call Center: En el Call Center de Cobranza del Banco se definieron tres tipos de roles para los funcionarios que utilizan el Aplicativo ICS: Gerente, Supervisor y Asesor; del seguimiento realizado se observó que la Entidad estableció como política que los Supervisores cuenten con el aplicativo MS-Outlook; sin embargo, se evidenció que no se han implementado controles que permitan restringir el envío de información a personas ajenas al Banco, situación que puede afectar la confidencialidad en el manejo de la información teniendo en cuenta que dicho Supervisor tiene a cargo tanto el monitoreo en línea de las actividades realizadas por los Asesores en el aplicativo ICS, como la gestión telefónica de éstos.

11.2. HABEAS DATA: Información confidencial de clientes de la entidad fue ofrecida en la página www.youtube.com, en el cual se encontraba disponible para su consulta pública e ilimitada.

El banco reconoció coincidencia de información por número de cédula de 34 registros y por cédula, nombre, producto (TC) y teléfono de 19 registros de sus clientes, involucrados en la base de datos que se encontraba en venta.

11.3. SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO (SARO):

a) Identificación de riesgos e implementación de controles: La entidad estableció cinco fallas o insuficiencias originadoras del riesgo "Divulgar o filtrar información de clientes a través de personal de la GNC, Megalínea, agencias o abogados externos", las cuales hacen referencia a errores, desconocimiento o falta de motivación, entre otros, tal y como se puede observar en la matriz de riesgos del proceso "Cobranzas PMP".

Sin embargo, dichas fallas o insuficiencias no contemplan otras causas de riesgo tales como la utilización indebida de información en beneficio de un funcionario de la entidad o de un tercero.

Para el riesgo mencionado el Banco estableció dos controles: uno hace referencia a la firma de cláusulas de confidencialidad en los contratos y el otro se relaciona con las restricciones para el uso de dispositivos (USB, CD) en el Call Center.

En consecuencia, no se han identificado fallas o insuficiencias ni se han implementado controles que permitan mitigar los riesgos que se originan en la indebida utilización de la información, que podrían presentarse en alguna de las actividades del proceso de cobranza.

b) Monitoreo: Una vez revisados los procesos a cargo de la Gerencia de Cobranzas, incluyendo el callcenter, las casas de cobranza (outsourcing) y la caracterización del proceso de Seguridad de la Información, la Comisión de Inspección no evidenció la existencia de indicadores de riesgo ni la implementación del esquema de autocontrol para realizar el monitoreo sobre las actividades que adelantan sus terceros, tal como lo establece el Banco en su Manual de Riesgo Operativo, debilidades que a pesar de haber sido detectadas en la Visita realizada en abril de 2009 por esta Superintendencia, aún se encuentran en implementación los correctivos.

Al respecto, la Gerencia de Riesgos manifestó que el monitoreo del SARO se lleva a cabo solamente con la revisión de los eventos de riesgo materializados, el comportamiento de los registros de eventos en el estado de resultados y con visitas a los Gestores para detectar posibles cambios en los procesos y/o en los riesgos.

Sobre el particular, se revisó la documentación que contiene la caracterización de los procesos de Cobranza, de Servicio de Cobranza Prejurídica y Jurídica, de Outsourcing y de Seguridad de la Información sin que se lograra evidenciar que para el monitoreo se utilicen indicadores de riesgos que permitan garantizar seguimiento efectivo de los riesgos asociados a la información administrada por los terceros.

c) Capacitación: A la fecha de la visita de inspección, el Banco no había adelantado durante el 2008 ni tenía programado adelantar capacitación sobre el SARO para el 2009, al personal de las casas de cobranza que vienen desarrollando las actividades de recaudo de cartera vencida del Banco.

DÉCIMO SEGUNDO: Que con base en los hechos descritos en el considerando anterior, esta Superintendencia formuló al **Banco de Bogotá S.A.** los siguientes cargos institucionales:

12.1. PRIMER CARGO – SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN:

12.1.1. A los hechos del numeral 2.1.1. del pliego de cargos: el Banco no ha dispuesto de los recursos tecnológicos y los controles suficientes que le permitan garantizar que la información confidencial de sus clientes, utilizada en el proceso de cobranzas, es administrada en condiciones de seguridad y calidad, dado que:

- No se han implementado los procedimientos y controles necesarios que mitiguen el riesgo de fuga de información para fines no autorizados, como lo exige el subnumeral 3.1.1 del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996.

- No se ha dispuesto de mecanismos de seguridad en el hardware y equipos de telecomunicaciones utilizados para que los funcionarios de las casas de cobranza, ubicados en las Oficinas del Banco, se conecten con el Centro de Cómputo; conforme lo señala el subnumeral 3.1.4. en concordancia con el subnumeral 4.1.5 del Título I Capítulo XII de la citada Circular.

- No se han definido roles funcionales independientes para la administración de usuarios y de la base de datos del aplicativo ICS, como lo indica el subnumeral 3.1.6 del Título I Capítulo XII de la misma Circular.

- No han implementado controles para evitar el uso compartido de los nombres de identificación de usuario y las claves para ingresar al aplicativo ICS, por los terceros que llevan acabo el proceso de cobranzas, como lo establece el subnumeral 3.1.6 del Título I Capítulo XII de la Circular en comento.

12.1.2. Gestión de Cobranzas:

- Pese a que el Banco suscribió acuerdos de confidencialidad con las casas de cobranza, no ha realizado seguimiento al cumplimiento que éstas deben dar en relación con la seguridad de la información, como lo exige la letra d) del subnumeral 3.2.1 del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996.

- El Banco no ha incluido en sus cláusulas lo concerniente a las políticas de control y seguridad (normas de seguridad informática y física) sobre las herramientas tecnológicas que pone a disposición de las casas de cobranza, como lo requiere la letra e) del subnumeral 3.2.1 del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996.

- El Banco no ha implementado restricciones de uso para el recibo y envío de correo electrónico para los supervisores del Call Center, en presunto incumplimiento del subnumeral 4.7.5. del Título I Capítulo XII de la misma circular.

NORMAS PRESUNTAMENTE INCUMPLIDAS:

12.1.3. A los hechos del numeral 2.1.1. del presente documento: Circular Básica Jurídica 007 de 1996, Título I Capítulo XII Numeral 3.1 Seguridad y Calidad, Subnumerales 3.1.1, 3.1.4 y 3.1.6. en concordancia con el Subnumeral 4.1.5:

"En desarrollo de los criterios de seguridad y calidad, y considerando los canales de distribución utilizados, las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

3.1.1. Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.

(...)

3.1.4 Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

(...)

3.1.6 Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada."

(...)

"4.1 Oficinas

Para las oficinas donde se realicen transacciones las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

(...)

4.1.5 La información que viaja entre las oficinas y los sitios centrales de las entidades deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los Establecimientos de Crédito el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados."

12.1.4. Gestión de Cobranzas: Circular Básica Jurídica 007 de 1996, Título I, Capítulo XII, Numerales 3.2 Tercerización – outsourcing y 4.7 Centro de Atención Telefónica (Call Center, Contact Center).

"3.2 Tercerización – Outsourcing

Las entidades que contraten bajo la modalidad de outsourcing o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información confidencial de la entidad o de sus clientes, deberán cumplir, como mínimo, con los siguientes requerimientos: (Subrayado fuera del texto original).

3.2.1. Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capitulo, por lo menos, los siguientes aspectos:

(...)

a) Restricciones sobre el software empleado.
b) Normas de seguridad informática y física a ser aplicadas."

(...)

4.7 Centro de Atención Telefónica

(...)

4.7.5 "En los equipos usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información (...)".

12.2. SEGUNDO CARGO - HABEAS DATA: ***(i)*** se presentó fuga de información confidencial de clientes de la entidad, la cual fue divulgada por Internet, en la página de YouTube, encontrándose entonces disponible para su consulta pública e ilimitada, ***(ii)*** el Banco corroboró que en los videos existía información de sus clientes, ***(iii)*** la materialización del incidente denota que la entidad, en su doble condición de fuente y usuaria de la información, no estaría garantizando la seguridad de los registros individuales de sus clientes, toda vez que no ha evitado su consulta o uso no autorizado, teniendo en cuenta que, tanto el Banco, como los terceros que éste contrata en la modalidad de outsourcing y que tienen acceso a información confidencial de sus clientes, están obligados a garantizar la reserva de la información de los datos personales de los clientes que no tengan la naturaleza de públicos, como nombres asociados a productos.

NORMA PRESUNTAMENTE INCUMPLIDA: HABEAS DATA: Ley 1266 de 2008: (i) literales c), f) y g) del artículo 4° y (ii) numerales 1 y 3 del artículo 9°; en desarrollo de la función de vigilancia conferida a esta

Superintendencia por el numeral 3 del artículo 17 de la misma:

"**Artículo 4°. Principios de la administración de datos.** En el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

(...)

c) Principio de circulación restringida. (...) Los datos personales, salvo información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;

(...)

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma."

"**Artículo 9°. Deberes de los usuarios.** Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los usuarios de la información deberán:

1. Guardar reserva sobre la información que les sea suministrada por los operadores de los bancos de datos, por las fuentes o los titulares de la información y utilizar la información únicamente para los fines para los que le fue entregada, en los términos de la presente ley.
(...)

3. Conservar con las debidas seguridades la información recibida, para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento."

"Artículo 17: Función de vigilancia.

(...)

3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley."

12.3. TERCER CARGO – SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO (SARO):

- El Banco no ha identificado la totalidad de los riesgos inherentes al proceso de Cobranzas que vienen desarrollando los terceros, por lo que no se evidenciaron los controles suficientes para garantizar la confidencialidad e integridad de la información utilizada en las casas de cobranza. Así mismo, no se han establecido indicadores descriptivos y/o prospectivos que permitan realizar un monitoreo que asegure que los controles operan en forma oportuna, efectiva y eficiente.

- Es posible extraer información confidencial de los clientes por medio del correo electrónico de la casa de cobranza "Colcartera E.U.", sin que se genere algún tipo de alerta en el banco.

- La entidad no ha involucrado en su programación anual de capacitación, además de todos sus funcionarios, a los terceros que desempeñan funciones de la entidad.

- De conformidad con lo anterior, se considera que el Banco de Bogotá estaría presuntamente incumpliendo el literal c) del numeral 3.1.1, el literal b) del numeral 3.1.3, los literales a), b) y c) del numeral 3.1.4 y los literales a), c), d) y e) del numeral 3.2.9 del Capítulo XXIII Reglas Relativas a la Administración del Riesgo Operativo de la Circular Externa 100 de 1995 de la Superintendencia Financiera de Colombia.

NORMA PRESUNTAMENTE INCUMPLIDA: Circular Externa 100 de 1995 de la Superintendencia Financiera de Colombia (Circular Básica Contable y Financiera), Capítulo XXIII Reglas Relativas a la Administración del Riesgo Operativo, Subnumerales 3.1. y 3.2.9.:

"3.1. Etapas de la Administración del Riesgo Operativo

"En la administración del riesgo operativo, las entidades deben desarrollar las siguientes etapas:

3.1.1. Identificación

En desarrollo del SARO las entidades deben identificar los riesgos operativos a que se ven expuestas, teniendo en cuenta los factores de riesgo definidos en este capítulo.

Para identificar el riesgo las entidades deben como mínimo.

(...)

c) Con base en las metodologías establecidas en desarrollo del literal b) del numeral 3.1.1 del presente capítulo, identificar los riesgos operativos, potenciales y ocurridos, en cada uno de los procesos.

(...)

3.1.3. Control

Las entidades deben tomar medidas para controlar los riesgos inherentes a que se ven expuestas con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen.

Durante esta etapa las entidades deben como mínimo:

(...)

b) De acuerdo con la metodología establecida en desarrollo del literal a) del numeral 3.1.3 del presente capítulo, implementar las medidas de control sobre cada uno de los riesgos operativos.

(...)

3.1.4. Monitoreo

Las entidades deben hacer un monitoreo periódico del perfil de riesgo y de la exposición a pérdidas.

Para el efecto, éstas deben cumplir, como mínimo, con los siguientes requisitos:

a) Desarrollar un proceso de seguimiento efectivo, que facilite la rápida detección y corrección de las deficiencias en **el** SARO. Dicho seguimiento debe tener una periodicidad acorde con los **riesgos operativos** potenciales y ocurridos, así como con la frecuencia y naturaleza de los cambios en el entorno operativo. En cualquier caso, el seguimiento debe realizarse con una periodicidad mínima semestral.

b) Establecer indicadores descriptivos y/o prospectivos que evidencien los potenciales riesgos operativos.

c) Asegurar que los controles estén funcionando en forma oportuna, efectiva y eficiente.

(...)

3.2.9. Capacitación

Las entidades deben diseñar, programar y coordinar planes de capacitación sobre el SARO dirigidos a todas las áreas y funcionarios.
Tales programas deben, cuando menos cumplir con las siguientes condiciones:

a) Periodicidad anual.

(...)

c) Ser impartidos a los terceros siempre que exista una relación contractual con éstos y desempeñen funciones de la entidad.

d) Ser constantemente revisados y actualizados.

e) Contar con los mecanismos de evaluación de los resultados obtenidos con el fin de determinar la eficacia de dichos programas y el alcance de los objetivos propuestos."

DÉCIMO TERCERO: Que los argumentos de defensa propuestos por el **Banco de Bogotá S.A.** en el escrito de descargos se resumen a continuación:

13.1. SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN: luego de transcribir los apartes correspondientes del pliego de cargos, el Banco se refiere a cada una de las normas citadas como presuntamente infringidas, así como al concepto de violación, en los siguientes términos:

13.1.1. Subnumeral 3.1.1. del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996: el Banco manifiesta que considera no estar incumpliendo la citada norma, teniendo en cuenta las acciones que ha venido tomando desde hace ya varios años, tendientes a manejar la información de los clientes en condiciones de seguridad y calidad, de acuerdo con las políticas establecidas por el Banco y según lo estipulado en la Circular 052 de 2007, citando, entre otras, las siguientes:

i. Señala que adoptó un modelo de seguridad que ha tenido como marco de referencia para su definición el estándar ISO27001, en el que se encuentran documentadas las políticas y controles necesarios para garantizar una adecuada gestión de la seguridad de la información, con un enfoque claro sobre temas de seguridad y evaluación de los riesgos a los que se encuentra sometida la información del Banco.

   Manifiesta que, con la adopción del modelo de seguridad de la información, simultáneamente se implementó un proceso continuo de concientización y divulgación del mismo al interior del Banco a través de conferencias presenciales, capacitación virtual, publicaciones en medios de comunicación, como la Intranet, boletines, revista interna, pagina interna de seguridad de la información, circulares y procedimientos, entre otros.

ii. Comenta que implementó los elementos de seguridad perimetral que le permiten controlar el acceso a los recursos del sistema que se encuentran a

disposición de los clientes tanto externos como internos. Menciona que, entre estos elementos, está el *hardware* y los equipos de comunicaciones de propósito especifico tales como *switches, routers*, equipos de cifrado de información para canales de oficina, *firewalls* y una red de canales privados para la comunicación entre las oficinas y las sedes administrativas, así como los elementos del software de propósito específico, tales como los detectores de intrusos (IDS), filtros de contenido, anti-virus, anti-*spyware* y anti-*malware*, control de dispositivos de almacenamiento no autorizados por el Banco, entre otros.

Añade que todos los elementos de *hardware, software* y equipos de comunicaciones han sido instalados y son continuamente monitoreados y actualizados, con el fin de garantizar que el manejo de la información se haga en las condiciones de seguridad y con la calidad adecuadas.

iii. Menciona que cuenta con un Sistema de monitoreo y gestión de red de comunicaciones y equipo de cómputo.

iv. Indica que cuenta con un Sistema de control de inventarios y licenciamiento para supervisar el *software y el hardware* que se instala en los equipos del Banco.

v. Informa que cuenta con un Sistema de análisis de vulnerabilidades informáticas basado en *hardware* de propósito especifico (*appliance*), con el cual se efectúan periódicamente procesos de revisión del esquema de seguridad, para garantizar así la continuidad en la aplicación de las políticas de seguridad del Banco.

vi. Añade que cuenta con un recurso humano calificado que se encuentra en constante proceso de capacitación, con el cual se realiza la gestión y el monitoreo de los sistemas de información, con participación del personal de las áreas de tecnología, así como de las áreas de seguridad del Banco.

13.1.2. Subnumeral 3.1.4. en concordancia con el subnumeral 4.1.5. del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996: afirma que ha venido tomando y tiene vigentes una serie de medidas para garantizar la seguridad de la información confidencial y lista las siguientes:

i. Todas las aplicaciones que funcionan en los equipos y redes de la entidad cuentan con un sistema de seguridad de acceso basado en usuarios y claves.

ii. Las consultas que se efectúan sobre la información confidencial de los clientes a través de las diferentes aplicaciones del Banco, quedan registradas en una auditoria que permite establecer, entre otras cosas, quien hizo la consulta, a qué hora se hizo y desde que dispositivo, con lo cual se establecen los controles para evitar accesos no autorizados.

iii. Con referencia al acceso directo a la información de los clientes, realizado mediante herramientas de exploración de bases de datos externas a las aplicaciones, el Banco viene adelantando desde comienzos del 2009 un proyecto con el cual, mediante la implementación de una herramienta (*appliance*) que se coloca de frente a las bases de datos, con un esquema de solución tipo *firewall* (solución de IMPER VA) y unos agentes que se instalan en la base de datos, se controla el acceso a los recursos informáticos corporativos, dejando rastros de las consultas realizadas, permitiendo así controlar de manera proactiva accesos no autorizados a la información.

Comenta que, no obstante lo anterior, y conciente de que las medidas tomadas respecto de la seguridad de la información confidencial están enfocadas fundamentalmente a proteger el acceso a la información estructurada que se encuentra en diferentes sistemas de información del Banco, y aunque no esta previsto en la norma, viene adelantando un proyecto en asocio con Microsoft para implementar el producto ADRMS (Active Directory Rigths Management Services), que establece la posibilidad de definir derechos de uso y acceso a la información almacenada en archivos en formato Excel, Word, Powerpoint o PDF, con lo cual se dará un nivel de protección contra el acceso no autorizado a la información que se encuentra almacenada en formatos no estructurados. Sobre el particular, afirma que ya adelantó las labores correspondientes a la evaluación del producto y la prueba de concepto con el equipo de trabajo de Microsoft, en las cuales se estableció que es posible definir niveles de autorización de lectura, impresión, copiado y visualización, entre otros. Añade que la Gerencia de Tecnología se encuentra adelantando las labores preliminares de actualización de la plataforma de servicio de correo del Banco, que permitirá hacer uso de la versión actualizada del producto, lo cual se tiene previsto para el Primer Semestre del año en curso.

Sobre el numeral 4.1.5. de la Circular 052, el Banco manifiesta que tiene en operación desde el mes de enero de 2009 la solución de cifrado para toda la información que viaja entre las oficinas y los sitios centrales, utilizando para ello un *hardware* de propósito especifico, adquirió 306 tarjetas encriptoras que se acondicionaron a los enrutadores de las oficinas y se reemplazaron un total de 409 enrutadores a los que no se les podían adecuar las tarjetas de encripción. Indica que la aplicación de la norma se hizo en un todo de acuerdo con las definiciones que se establecieron en la misma Circular 052, citando y transcribiendo el encabezamiento del numeral 2 y los subnumerales 2.3., 2.8. y 4.1. del citado instructivo.

Manifiesta que, de acuerdo con las definiciones establecidas en el texto de la norma, se estableció que las oficinas a las que se hace referencia para la aplicación del numeral 4.1.5, dentro del alcance de la circular en mención, son aquellos sitios en los que se realizan transacciones, es decir, los sitios en los que se efectúan operaciones que implican o conllevan movimiento de dinero, por ejemplo: retiros, transferencias, depósitos, pagos etc.

Con base en lo expuesto y teniendo en cuenta que los lugares que ha dispuesto en Bogota y en Barranquilla para la atención de clientes morosos corresponden a oficinas administrativas en las que no se realizan transacciones (sólo se adelantan trámites administrativos de cobro que derivan en acuerdos de pago que se perfeccionan posteriormente, esos si sobre oficinas bancarias -Oficinas transaccionales- del Banco, diferentes a aquellas en las que se realizaron los acuerdos), considera que a la información que viaja entre estos sitios y el sistema central, no le es aplicable el alcance de la norma y, por lo tanto, no requiere estar cifrada.

No obstante lo anterior, resalta que cada uno de los sitios dispuestos para la atención a clientes morosos cuenta con las medidas de seguridad y las adecuaciones de infraestructura necesarias para garantizar la confidencialidad y la integridad de la información que viaja entre estos sitios y el central, de acuerdo con lo que se describe a continuación:

i. En el sitio de *Atención* de la Calle 26:

- Un esquema de comunicación que asegura la comunicación entre los PCs usuarios (casa de cobranza) con el *Firewall*.
- Reglas de validación en el *Firewall*.
- Conexión por fibra oscura del proveedor ETB, iluminada y administrada por el Banco.

Añade que, en consideración a los temas relacionados por la Superintendencia en el informe, el Banco trabajó con ETEK, el proveedor del *Firewall*, para cifrar la comunicación entre el sitio de atención ubicado en la Calle 26 y el sitio central. Comenta que estableció una VPN (Red Privada Virtual) entre el *FIREWALL VPNJ Edge* de la Calle 26 y el *Firewall* VSX del sitio Central.

ii. En el sitio de atención de Barranquilla, ubicado en el segundo piso de la Oficina Bancaria:

- Un esquema de comunicación que asegura la comunicación entre los PCs usuarios (casa de cobranza) con el *Firewall*.
- Reglas de validación en el *Firewall*.
- Aislamiento del tráfico de red de la Oficina Bancaria y la red del sitio de atención,
- La información, al pasar por el enrutador de la Oficina, queda cobijada por el cifrado de la comunicación entre la red de la Oficina y el sitio central a través de un canal seguro.

13.1.3. Subnumeral 3.1.6. del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996: trascribe la norma y expone que en la misma no se establece la obligatoriedad de definir roles funcionales independientes para la

administración de usuarios y de las bases de datos, por lo que considera que este concepto de violación no aplica.

Indica que, dada la cantidad de aplicaciones, áreas y usuarios que tiene el Banco, que hacen compleja la aplicación efectiva de las normas establecidas en este sentido, el Banco acaba de aprobar la ejecución del proyecto de administración de identidades IDM, con el cual, mediante la definición de un modelo de gobierno de seguridad de usuarios, la implementación de una infraestructura y unas herramientas tecnológicas y la definición de unas políticas y procedimientos adecuados de gestión de usuarios y control de acceso, se dará atención de manera efectiva al tema de claves de acceso a los sistemas de información.

Manifiesta que la solución de administración de identidades contempla:

i. La gestión de Identidades

- Aprovisionamiento de cuentas
- Automatización del flujo de trabajo de asignación de usuarios
- Administración centralizada remota
- Sincronización de contraseñas
- Reemplazo automático de contraseñas

ii. El control de acceso

- Políticas de control de acceso
- *Single Sign-On*
- *Web Single Sign On*
- *Reduced Sign On*

iii. Servicios de directorio

- Repositorio de identidades (servicios de directorio para la administración de los atributos de cuentas de usuario)

En relación con el control para evitar el uso compartido de usuarios y claves, menciona que el Banco tiene definidas las políticas y los procedimientos que protegen las claves de acceso a los sistemas de información en las que se establece la prohibición de compartir las claves o permitir su uso por parte de grupos de personas.

Indica que si bien el aplicativo ICS (Internet Collection System), usado para la gestión de cobro, permitía tener varias sesiones habilitadas por usuario, dando la posibilidad a los usuarios de conectarse con un mismo usuario compartido a la aplicación, se tenia previsto que era necesario crear usuarios por persona y dejar en "1" las sesiones permitidas por usuario, y que esta labor estaba prevista para el cambio de versión del aplicativo, como en efecto se cumplió. Señala que se realizó la creación de 170 usuarios personalizados para cada uno de los funcionarios de

las casas de cobranzas que utilizaban usuarios compartidos y que los usuarios compartidos fueron inactivados de acuerdo con el procedimiento establecido para la aplicación.

Añade que, terminada la labor de creación, activación y entrega de los usuarios por persona, el parámetro de cantidad de sesiones por usuario se cambió a "1". Es decir, con cada usuario sólo se puede abrir una sesión de trabajo.

Concluye indicando que, en resumen, en las Oficinas Bancarias transaccionales del banco no existen funcionarios de las casas de cobranza y por ende éstos no tienen acceso a información confidencial de los clientes a través de las aplicaciones disponibles en las oficinas del Banco

13.2. GESTIÓN DE COBRANZAS: luego de transcribir la norma presuntamente infringida el concepto de violación indicados en el pliego de cargos, manifiesta que, al revisar el subnumeral 3.2.1, Titulo I, Capitulo XII de la citada Circular, no encuentra la existencia del literal d). Afirma que este subnumeral establece "Definir criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos.". Señala que tampoco encuentra en dicha Circular anotación alguna sobre la obligatoriedad del Banco de hacer seguimiento a las casas de cobranzas sobre el cumplimiento de la seguridad de la información.

Comenta que en el numeral 3.2.2, Titulo I, Capitulo XII de la citada Circular, si existe la letra d) y que este subnumeral establece "Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capitulo, por lo menos, los siguientes aspectos:", pero el literal d) habla sobre "Restricciones sobre el software empleado" y reitera que no hay ningún literal que haga referencia al seguimiento que debe realizar el Banco al cumplimiento que deben dar las casas de cobranzas sobre la seguridad de la información.

Sin embargo, procede a detallar las actividades que se han emprendido a fin de fortalecer aún más el cabal cumplimiento al numeral 3.2. Tercerización Outsourcing del Titulo I - Capitulo XII de la Circular 052 de 2007, que se transcriben a continuación:

"

- El 21 de diciembre de 2009 se inició un plan de trabajo para evaluar los contratos actuales de los entes externos y definir si es necesario modificarlos, con el fin de incluirles las cláusulas relativas al numeral 3.2. Tercerización Outsourcing del Titulo I - Capitulo XII de la Circular 052 de 2007, específicamente las señaladas en el numeral 3.2.2., y realizar los ajustes correspondientes.

- El 4 de diciembre de 2009 se llevó a cabo el II Encuentro de Entes Externos de La Gerencia Nacional de Cobranzas, y dentro del programa se incluyó la capacitación relacionada con el Sistema de Riesgo Operativo, Continuidad del Negocio y Seguridad de la Información a los agentes de cobranzas

externos, de la cual se levantó el acta de asistencia correspondiente. En la mencionada capacitación se hizo especial énfasis en la importancia del cumplimiento estricto del numeral 3.2. Tercerización Outsourcing del Titulo I - Capitulo XII de la Circular 052 de 2007.

- El 2 de diciembre de 2009 se remitieron a todos los entes externos de la Gerencia Nacional de Cobranzas unas encuestas que buscaban evaluar el grado de cumplimiento de los mismos con los modelos de Seguridad de la Información y Continuidad del Negocio del Banco. Tan pronto se tabulen y analicen estas encuestas, compartiremos de manera individual con cada ente externo los resultados de las mismas, e iniciaremos el plan de trabajo correspondiente y se efectuarán los ajustes a que haya lugar.

- En octubre de 2009 se presentó la propuesta de contratación del servicio de capacitación para la "Profesionalización de las Casas externas de Cobro" y el "Programa de Auditoria" a las mismas con una firma consultora, la cual fue aprobada en diciembre de 2009 y se llevará a cabo a partir de enero de 2010, con el fin de garantizar el cumplimiento por parte de éstas de las circulares 048 y 052 de la Superintendencia Financiera.

- En diciembre de 2009 la Gerencia Nacional de Cobranzas, en conjunto con las áreas de Contraloría de la Dirección General, de Sistemas y del Departamento de Seguridad del Banco, inició un plan de trabajo con el fin de establecer el alcance y periodicidad de las visitas de auditoria a las casas de cobranzas por parte de cada una de las áreas mencionadas."

Respecto del concepto de violación, que transcribe: *"El Banco no ha incluido en sus cláusulas lo concerniente a las políticas de control y seguridad (normas de seguridad informática física) sobre las herramientas tecnológicas que pone a disposición de las casas de cobranza, como lo requiere la letra e) del subnumeral 3.2.1 del Titulo I Capitulo XII de la citada Circular"*, comenta que sí existe una cláusula (Décima Segunda) en el Acuerdo de Confidencialidad, que hace referencia a la obligatoriedad sobre el uso divulgación guarda y custodia de los documentos e información que el Banco le entregue. Transcribe la mencionada cláusula:

"DECIMA SEGUNDA. ACUERDO DE CONFIDENCIALIDAD: LA CASA DE COBRANZAS EXTERNA se compromete a guardar y a custodiar los documentos y a mantener toda aquella información que tenga carácter reservado y que sea legalmente protegida y la que EL BANCO califique como tal, que sea recibida y conocida por LA CASA DE COBRANZAS EXTERNA con motivo ó con ocasión de la celebración y/o ejecución del presente contrato, y tomará las medidas de seguridad necesarias para impedir cualquier uso y/o divulgación indebida de dichos documentos e información, a menos que la divulgación sea necesaria para la ejecución y fines del contrato. LA CASA DE COBRANZAS EXTERNA autoriza irrevocablemente a EL BANCO para inspeccionar los mecanismos adoptados por esta para guardar y mantener la reserva y confidencialidad de los documentos e información que le sean suministrados, y pondrá en práctica las recomendaciones

que formule sobre ese particular. En consecuencia, LA CASA DE COBRANZAS EXTERNA indemnizará a EL BANCO y/o a terceros todos los perjuicios que sean causados con ocasión de la divulgación, uso indebido, no autorizado y aprovechamiento ilegitimo de la citada información, que resulten del incumplimiento de la obligación de guarda y custodia aquí pactada. Para los efectos de ésta cláusula, en caso de violación de la misma se establece una multa a favor de EL BANCO y a cargo de LA CASA DE COBRANZAS EXTERNA por valor de un mil (1000) salarios mínimos legales mensuales vigentes, sin perjuicio de las acciones ordinarias en cabeza de EL BANCO para obtener la indemnización total de los perjuicios que sufriere con ocasión del incumplimiento de la obligación prevista en esta cláusula".

Añade que el 21 de diciembre de 2009 se inició un plan de trabajo para evaluar los contratos actuales de los entes externos y definir si es necesario modificarlos con el fin de incluirles las cláusulas relativas al numeral 3.2. Tercerización Outsourcing del Titulo I - Capitulo XII de la Circular 052 de 2007, específicamente las señaladas en la letra e) del subnumeral 3.2.2., y realizar los ajustes correspondientes.

En relación con el subnumeral 4.7.5. del Título I Capítulo XII de la Circular Básica Jurídica 007 de 1996, luego de transcribir la norma y el concepto de violación, el banco manifiesta que no está de acuerdo con este concepto de violación, y que, por el contrario, considera que sí ha dispuesto las restricciones de uso para el recibo y envío de correo electrónico para los supervisores del Call Center. Explica que la entidad puede permitir la navegación por Internet o el envío de correo electrónico, siempre y cuando se cuente con un sistema de registro de información enviada y recibida.

Añade que, para tales efectos, el Banco ha tornado las siguientes acciones:

"

- Habilitar la funcionalidad del servicio de *Journaling* que provee el producto de mensajería Microsoft Exchange, con lo cual a las bases de datos definidas en forma exclusiva para los buzones de correo del Call Center se les configuró el registro en el Journaling de todos los mensajes enviados y recibidos por parte de los supervisores.
- Mantener una copia centralizada de los mensajes gestionados en dichos buzones.
- Se implemento *(sic)* adicionalmente la herramienta de *Quest Software*, llamada "*Archive Manager*", que permite realizar consultas sobre los registros mantenidos en el *Journaling*, la cual se conserva por tres años.
- Internamente el Banco ha formalizado la normatividad relacionada con el envío y recepción de correo electrónico externo en el Manual de Servicios Administrativos, Titulo IV Capitulo 5 "Normas y Procedimientos para el Uso de Internet", numeral 5.1, en la actualización de fecha 6 de noviembre de 2009.
- No obstante que en nuestro sentir el Banco viene dando cumplimiento a la normatividad aplicable, se está implementando un control adicional a nivel

central, para restringir el envío de correos externos únicamente a direcciones autorizadas previamente, por parte de los Supervisores del *Call Center*. Para esto se configurará el servidor de mensajería Microsoft Exchange con reglas de transporte, para que el Supervisor pueda enviar correo a cualquier persona dentro de la organización y únicamente a los usuarios de la lista de distribución de destinos autorizados; para todos los demás dominios y cuentas en Internet no podrá enviar mensajes. Esta actividad está programada para el mes de febrero de 2010."

Añade que se modificó la matriz de perfiles para que a los supervisores del *Call Center* se les restrinja el uso de correo externo, solo para envío de información a las direcciones de mail corporativas especificas que requieren en su trabajo.

13.3. HABEAS DATA

Luego de transcribir la norma citada como presuntamente incumplida y el concepto de la violación del pliego de cargos, puntualiza que el dato financiero no tiene la calidad de privado y, en consecuencia, frente a él no existe la obligación de reserva. Complementa indicando que, en este asunto, por referirse a la reglamentación de una norma constitucional, el único medio para su regulación, reglamentación, etc., es a través de una Ley estatutaria, como lo evidencia la expedición de la ley de Habeas Data, y manifiesta que también, como se dirá más adelante, el Banco sí ha tomado la precaución de firmar cláusulas de confidencialidad.

13.4. SISTEMA DE ADMINISTRACION DE RIESGO OPERATIVO (SARO): una vez transcrita la norma citada como presuntamente incumplida y el concepto de la violación indicados en el pliego de cargos, manifiesta que:

"

- El proceso de identificación de riesgos se realizó para todos los procesos misionales y habilitantes del Banco, siguiendo las instrucciones impartidas en la Circular 041 de 2007.

  En el proceso de Cobranzas se identificaron 12 riesgos, dentro de los cuales se consideró el riesgo de "Divulgar o filtrar información de clientes a través de personal de la Gerencia Nacional de Cobranzas, Megalínea, Agencias o Abogados externos, etc.", el cual puede ser causado por 5 fallas:

  - Desconocimiento de políticas de seguridad de información
  - Definición inadecuada de información a entregar para la gestión de cobro
  - Definición inadecuada de perfiles de acceso a información de los clientes
  - Falta de motivación y compromiso del personal
  - Errores en la remisión de documentación entregada

  Igualmente, los controles asociados son:

- El departamento de Seguridad y la Gerencia Jurídica, para la vinculación de empleados, agencias y abogados al Banco, tiene establecido como control la firma de contratos con cláusulas de confidencialidad.
- Las herramientas utilizadas por las personas que se desempeñan en el *Call Center* del Banco cuentan con restricciones en el uso de puertos, USB, inhabilidad para el uso de CD, diskette, lo que impide la fuga de información del aplicativo utilizado.

Añade que actualmente se está revisando la documentación de riesgos y controles para establecer los requerimientos de información necesarios, con el objeto de generar los Indicadores que permitan hacer un monitoreo oportuno, como el sugerido.

- Comenta que, respecto de la posibilidad de extracción de información confidencial de los clientes por medio del correo electrónico de las casas de cobranza, se está haciendo seguimiento a las medidas de mejoramiento a adoptar para mitigar el riesgo.

- Afirma que durante el 2008 se realizó la capacitación a proveedores de acuerdo con el grado de contratación que se tuviera y que a los más grandes se les hizo capacitación conceptual en los temas relacionados con SARO y Plan de Continuidad de Negocio.

- Manifiesta que durante el 2009, dado el nivel de contratación de servicios con Megalínea, se hicieron sesiones de capacitación en la metodología adoptada para SARO, a fin de que la entidad tuviera un mapa de riesgos y empezara a integrar los conceptos de administración de riesgos en la estructura administrativa de la entidad. Indica que también se presentó el curso virtual de SARO para todos los funcionarios del *Call Center* el cual incluye un examen de validación de conceptos.

- Señala que en diciembre 4 de 2009, la Gerencia Nacional de Cobranzas celebró el "Encuentro de Agencias Externas de Cobranza" en el cual se presentó una actualización de los temas de SARO y Plan de Continuidad de Negocio del Banco.

- Añade que para el 2010, se tiene previsto continuar y reforzar la divulgación de SARO a las agencias de cobranza (127), y a los abogados externos, plan que va desde Febrero hasta Abril.

Concluye manifestando que, de acuerdo con lo anterior, el Banco considera que no está incumpliendo las normas mencionadas, sino que, dado su tamaño y la magnitud de proveedores, el cubrimiento de los numerales mencionados se hizo con base en priorización de los mismos, y una visión macroproceso para iniciar y tener una base de implantación de SARO, y que también considera que son susceptibles de mejoramiento algunos de los aspectos comentados, por lo cual se está adelantando una revisión detallada, añadiendo que, para este año (2010)

contará con la siguiente ficha técnica para cada uno de los procesos, la cual comprende la actualización de los correspondientes documentos, así:

- Caracterización del proceso
- Diagrama de actividades (flujo del proceso con identificación gráfica de riesgos)
- Matriz de responsabilidades (cargos involucrados en el proceso)
- Matriz de activos de información
- Matriz de Riesgos y Controles teniendo en cuenta además de los riesgos operativos los riesgos tecnológicos, de continuidad de negocio, de seguridad de la información y de registro contable.

13.5. CONSIDERACIONES GENERALES SOBRE LOS PUNTOS ANTERIORES: bajo este acápite el Banco deja sentadas algunas premisas de carácter general, replicables a todas las glosas, los hechos y las citas que esta Superintendencia hace de violación de resoluciones o instrucciones:

"En materia de protección de datos[2], el primer antecedente de proyecto legislativo existente se sucedió en el año de 1986 con el proyecto de ley 73, "Por medio de la cual se crea el Estatuto para la protección de la intimidad de las personas frente a los sistemas de información y los bancos de datos", proyecto que fue finalmente archivado por el Congreso de la República.

Posteriormente, después de algunas iniciativas presentadas, mediante sentencia C-008 de 1995, la Corte Constitucional declaró inconstitucional el proyecto de ley estatutaria relativo a la materia, por padecer de vicios de forma. Así las cosas, con anterioridad y durante la vigencia de la Constitución de 1991 hasta el año 2008, en Colombia no se habían expedido normas especiales en materia de protección de datos o habeas data recolectados por personas especializadas, por lo cual lo aplicable para estos casos eran las disposiciones que consagraban la reserva a la correspondencia, libros y papeles de las personas naturales y además de los libros y papeles del comerciante.

En lo que respecta al dato económico o financiero, debe advertirse que sólo con la expedición de la ley 1266 de 2008 es que el tema fue regulado por el legislador, en el articulo 3 literal g), en donde fue catalogado como **dato semiprivado**, entendido por este como aquél ***"que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley"***[3] (subrayado fuera del texto original). Cabe recordar que la precitada ley fue expedida el 31 de diciembre de 2008, otorgándose en su articulo 21 un periodo de transición de seis (6) meses.

---

[2] Tal como se narra en el libro *Autodeterminación informática y habeas data en Colombia*, del Dr. José Miguel de la Calle Restrepo.

[3] Ley 1266 de 2008, artículo 3, literal g).

Se destaca que con anterioridad a la precitada ley ninguna norma legal había reglamentado lo pertinente a la naturaleza, tratamiento, manejo, recopilación, revelación, suministro y reserva sobre los datos personales económicos. Sin embargo, a través de distintos fallos de la Corte Constitucional, se establecieron ciertos precedentes y conceptos sobre los cuales conviene destacar los siguientes:

1. En sentencia T-261 de 1995, la Corte Constitucional afirmó, en lo que respecta a la naturaleza del dato económico y sobre el carácter público de la dirección y el teléfono, entre otras:

> *"En el campo que interesa para los fines del proceso, el de las relaciones de carácter financiero, éstas exigen necesariamente de quien acude a los servicios que prestan las instituciones del sector, los cuales incorporan como elemento fundamental el del crédito, el suministro de datos personales sobre aspectos económicos, que, como ya lo dijo esta Corte en sentencias de unificación números SU-082 y SU-089 del 1 de marzo de 1995 (M.P.: Dr. Jorge Arango Mejia), no pertenecen forzosamente al dominio de la intimidad"*
>
> *"De tal modo hay datos personales que específicamente son íntimos y gozan, en consecuencia, de la garantía constitucional en cuanto tocan con un derecho fundamental e inalienable de la persona y de su familia, al paso que otros, no obstante ser personales, carecen del calificativo específico de privados, toda vez que no únicamente interesan al individuo y al circulo cerrado de su parentela, sino que, en mayor o menor medida, según la materia de que se trate, tienen importancia para grupos humanos más amplios (colegio, universidad, empresa) e inclusive para la generalidad de los asociados, evento en el cual son públicos, y si ello es así, están cobijados por otro derecho, también de rango constitucional fundamental, como es el derecho a la información (Articulo 20 C.P.)"*
>
> *"El conocimiento acerca de la dirección de un individuo es algo que, por el mismo desenvolvimiento de las actividades en el seno de la sociedad y aun por razones físicas de vecindad, no puede mantenerse en secreto"*
>
> *"Así, por regla general, toda persona natural o jurídica titular de una línea telefónica aparece en el directorio telefónico de la respectiva ciudad y allí, para conocimiento público, son registrados los datos en referencia, a menos que el sujeto incluido en la publicación se dirija en forma expresa a la entidad responsable de la misma para que, hacia el futuro, se suprima tal registro."*

2. En el mismo sentido, es decir, sobre la naturaleza del dato económico, la Corte Constitucional en la sentencia SU-082 de 1995, afirmó que:

"Cuando el articulo 15 de la Constitución consagra el derecho a la intimidad personal y familiar, es evidente que ampara, en primer lugar, aquello que atañe solamente al individuo, como su salud, sus hábitos o inclinaciones sexuales, su origen familiar e racial, sus convicciones políticas y religiosas. Ampara, además, la esfera familiar, lo que acontece en el seno de la familia, que no rebasa el ámbito doméstico."

"Entendidas así la intimidad personal y familiar, es claro que resulta exagerado colocar en su mismo plano el comportamiento de una persona en materia crediticia (...) quien obtiene un crédito de una entidad dedicada a esta actividad y abierta al público, no puede pretender que todo lo relacionado exclusivamente con el crédito, y en especial la forma como él cumpla sus obligaciones, quede amparado por el secreto como si se tratara de algo perteneciente a su intimidad"

3. Finalmente -por su relevancia- valga poner de presente el fallo T-729 de 2002, en el cual la Corte Constitucional reiteró la ausencia de regulación en materia de habeas data, instó al Congreso de la República para impulsar un proyecto de ley al respecto, y realizó la siguiente categorización en materia de datos, a saber:

"(...) En este sentido la Sala encuentra cuatro grandes tipos: la información pública o de dominio público, la información semi-privada, la información privada y la información reservada o secreta.

Así, la información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada e personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.

La información semi-privada, será aquella que por versar sobre información personal e impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de la seguridad social o de los datos relativos al comportamiento financiero de las personas.

La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede

ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

Finalmente, encontramos la información reservada, que por versar igualmente sobre información personal y sobretodo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabria mencionar aquí la información genética, y los llamados "dates sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc."

Recalca el Banco en que [a pesar de][4] la ausencia normativa en materia de protección de datos, de antaño en los fallos de la Corte Constitucional ha habido consenso en cuanto a la naturaleza del dato económico, el cual, concluye, no es privado ni intimo, así como de los datos relativos al estado civil de las personas, su dirección y demás datos demográficos, los cuales ostentan el carácter de públicos, por las razones anotadas por la misma Corte Constitucional en jurisprudencia reiterada.

Frente a las glosas realizadas por la Superintendencia, efectúa las siguientes observaciones:

Insiste en que el dato financiero no es reservado y, por ende, no hay obligación de confidencialidad, de lo cual concluye que no puede ser censurada la conducta de una persona por el hecho de que tal información sea conocida por terceros, por cualquier medio y, con mayor razón, cuando no hay evidencia de que el Banco la haya suministrado o facilitado los medios al respecto.

Comenta que la mayoría de las citas que se hacen de la ley de habeas data están dirigidas, dado el objeto de la citada regulación, a las bases de datos manejadas por sociedades recolectoras, siendo éste un estatuto que regula el tema de manera parcial y sólo frente a los administradores de bases de información, tal como lo afirmó la Corte Constitucional. El Banco no es una base de datos y, por tal razón, no puede en materia sancionatoria, sin violarse el principio de tipicidad y de legalidad, pretender extender deberes o aplicarlos de manera analógica a personas diferentes a las que están dirigidas tales disposiciones.

Manifiesta que, en este caso concreto, se dice que noventa y seis (96) personas relacionadas son clientes del Banco, lo que confrontado sus bases, no es preciso. Añade que de las noventa y seis (96) se agrega que treinta y tres (33) son clientes en concreto del producto de tarjeta de crédito, lo que tampoco es acertado. Indica que de estos treinta y tres (33), veintinueve (29) si tienen o tuvieron tarjeta pero en la información sólo aparece el nombre, la dirección y la cédula, datos estos últimos

[4] Nota de quien resume.

-nombre, dirección y cédula- que como lo ha aclarado la jurisprudencia constitucional atrás citada tienen el carácter de públicos o semiprivados. En cuanto al producto, no se indica el número de la tarjeta, las compras, los saldos, movimientos, transacciones, comportamiento crediticio o cualquier otro tipo de información que esté sujeta a reserva bancaria y que exclusivamente debiera estar en poder del Banco de Bogota, ni ninguna información relativa al comportamiento o relación comercial de estas personas con el Banco, lo cual a su vez no permite concluir que evidentemente tales terceros posean la información de los mencionados veintinueve (29) clientes. Añade que, si se toma en cuenta el consolidado de los clientes que tiene el Banco por cuenta de ahorros, cuenta corriente, CDTs, cartera, tarjeta débito, tarjeta crédito, etc. que suman aproximadamente tres millones (3.000.000) de clientes, se puede afirmar que no reviste ninguna materialidad por su aspecto cuantitativo y mucho menos por el contenido incompleto de la información.

Señala que, como quiera que los datos contenidos en las bases ofrecidas por terceros no obran exclusivamente en bases de datos del Banco de Bogotá, sino que por el carácter público del dato, pueden bien estar en cualquier otra base de datos, como directorios telefónicos, bases de datos de organismos públicos -por ejemplo: Registraduría Nacional del Estado Civil, SISBEN. FOSYGA, Secretaria de Salud del Distrito, Procuraduría General de la Nación, Policía Nacional SIDEX- o la de cualquier otra entidad, no es posible afirmar con el simple cruce de información que la información contenida en las bases ofrecidas por terceros haya sido recopilada con ocasión de una conducta del Banco de Bogota, sus empleados o contratistas.

De otro lado, comenta que en el pliego de cargos se da a entender que el Banco incurre en violación en la medida en que, entre otras cosas, no ha celebrado pactos de confidencialidad con terceros, con las oficinas de cobranza, con sus empleados, para obligarlos a guardar reserva o a no hacer uso de la información y aplicativos para fines personales y sobre el particular se deben hacer las siguientes reflexiones:

Insiste en que el deber de reserva o confidencialidad sólo es aplicable a la información que tiene que ver con la intimidad o dato intimo de las personas, carácter que no tiene el dato comercial.

Afirma que tal deber de sigilo lo deben guardar las personas, no como consecuencia de la celebración de un contrato, convenio o cláusula particular, sino que en la medida en que está prevista en la Constitución tal protección, todas las personas están obligadas a guardar dicha reserva, por lo cual no puede constituirse en un hecho censurable la no celebración de contratos o acuerdos puntuales sobre el particular, fuera de que el Banco si los ha celebrado y ha incluido las cláusulas pertinentes en los mismos.

En lo que tiene que ver con los trabajadores o los empleados, resalta que la Constitución Nacional consagra en su articulo 15 el derecho a la intimidad y al buen nombre, así mismo el articulo 74 prevé el secreto profesional y la reserva de

los documentos privados, normas éstas que sumadas a la presunción de buena fe prevista en el articulo 84 consagran una obligación const.tucional a cargo de los empleados y contratantes de mantener reserva respecto de todos aquellos asuntos que tenga conocimiento en desarrollo de las labores encomendadas. Añade que, en lo que respecta a las relaciones laborales, el artículo 55 del C.S.T. establece la obligación a cargo de las partes -empleados y empleadores- de ejecutar los contratos de buena fe, estableciendo que ellos obligan **no sólo a lo que en el se expresa sino a todas las cosas que emanan precisamente de la naturaleza de la relación jurídica**, y que el articulo 56 del C.S.T establece, a su turno, una obligación de fidelidad y obediencia para con el patrono. Tal obligación general de fidelidad encuentra mayor especificidad en la obligación especial contenida en el numeral 2 del articulo 58 del mismo código, en donde le es imperativo al trabajador "***no comunicar con terceros, salvo autorización expresa,.las informaciones que tenga sobre su trabajo, especialmente sobre las cosas que sean de naturaleza reservada o cuya divulgación pueda ocasionar perjuicios al patrono***".

Destaca que para los empleados, la obligación no es sólo de guardar reserva sino de no utilizar las herramientas, información, útiles y demás elementos que se le suministran para objeto distinto del desempeño de sus funciones, lo cual tampoco requiere de un pacto o cláusula contractual, porque tal deber se consagra de manera expresa en el articulo 60 del C.S.T., pero además, si se revisa el contrato de trabajo y el reglamento de trabajo aprobado por el Ministerio de la Protección Social igualmente se encuentran consignados tales deberes, de lo cual concluye que no se le puede endilgar al Banco incuria por este aspecto, fuera de que como lo prevé el articulo 1603 del C.C.C. *(sic)* es obligación de las personas ejecutar los contratos de buena fe, obligándose los contratantes a ***todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por ley pertenecen a ella***. (El subrayado, negrillas y cursiva son del texto en comento).

Formula a continuación observaciones o descargos en relación con las casas de cobranza y, en general, a los profesionales del derecho que adelantan la tarea de iniciar los procesos de cobro:

Manifiesta que son personas externas que actúan en nombre del Banco, a tarifa, en la gestión de recuperación de la cartera, de los cuales no tiene información que utilicen los datos de los clientes para fines distintos al de la cobranza.

Indica que la información que se le suministra es esencial para el ejercicio de la labor encomendada y que la información a que tienen acceso, por ser comercial contenida en títulos de deuda y además estar destinada a ir a procesos, no tiene el carácter de íntima o de reservada. Pero aclara que tampoco tales profesionales o casas están autorizadas por el Banco para darles cualquier uso, porque están comprometidas con el Banco a través de un contrato donde se han incluido cláusulas sobre la obligación de obrar con lealtad, honradez, a guardar el secreto profesional, incluso después de la cesación en la prestación de sus servicios. Y añade que a este tipo de personas o prestadoras de servicios legales, les son aplicables las normas generales contenidas en la Constitución y en la ley de

guardar secreto frente no sólo a la información intima o privada de las personas que llegue a su conocimiento. Puntualiza que la ley 1123 de 2007 -Código Disciplinario del Abogado- incluye iguales deberes, en concordancia con el Código de Procedimiento Civil e incluso el Código Penal, hasta el punto de que para garantizar la guarda del secreto profesional, los exime del deber de declarar.

Con fundamento en estos argumentos, concluye que no puede ser objeto de censura que el Banco no haya celebrado, como si lo ha hecho, contratos con tales "terceros" para garantizar la confidencialidad y menos se le censure por no hacerle visitas o inspecciones a tales servidores, cuya obligación de realizarlas no está en ninguna norma y cuya legalidad, por lo demás, es completamente discutible, precisamente por el secreto profesional con que la Constitución y la ley los protege *erga omnes* (art. 74 C.N.).

Insiste en que las obligaciones de sigilo, secreto, confidencialidad o reserva, emanan primigeniamente de la Constitución y la ley, a través de normas de orden público que rigen todas la[s][5] relaciones jurídicas y que por ende su eficacia no pende de acuerdos de voluntades privados. En tal sentido, no resulta acertado afirmar que deban existir indefectiblemente cláusulas contractuales de confidencialidad en las convenciones civiles, comerciales o laborales, para obligar a los contratantes a guardar reserva sobre la información suministrada o de la que llegaren a tener conocimiento en desarrollo de sus labores; insistiendo en que tales obligaciones son inherentes a cualquier negocio jurídico, cualquiera que sea su naturaleza, habida cuenta de la existencia de normas imperativas de mayor jerarquía que así lo consagran. Ahora bien, sin perjuicio de lo anterior, lo cierto es que los contratos de trabajo que celebra el Banco de Bogota con sus empleados, el reglamento interno de trabajo, así como los contratos civiles o comerciales para la prestación de servicios profesionales, **reiteran la obligación constitucional y legal de reserva y confidencialidad a cargo de los contratantes**, constituyendo una fuente adicional de dicha obligación de sigilo y reserva. (Las negrillas son del texto que se comenta).

Finalmente, advierte que el Banco ha contemplado y documentado en sus Manuales, políticas de manejo de la información, con el fin de garantizar su **confidencialidad, integridad, disponibilidad, auditabilidad y privacidad**, y que para ello ha establecido un conjunto de principios, políticas, normas, procedimientos, estándares y herramientas dentro del denominado Modelo de Seguridad de la Información, dentro de lo que se destaca un área especializada y encargada del manejo de dichos asuntos. Añade que, en relación con la seguridad de la información, el Banco tiene las siguientes políticas, entre otras:

"

- Categorización y establecimiento de perfiles de usuarios, a efectos de asignar los recursos informáticos y otorgar los privilegios para el acceso a la información.
- Procedimientos de destrucción de información confidencial.

---

[5] Nota de quien resume.

- Programas de capacitación en materia de seguridad de la información.
- Remoción de drives para la extracción de información a través de medios portátiles, como diskettes o CDs.
- Bloqueo de puertos USB y monitoreo de uso en áreas especiales (Call Center, tarjetas, procesamiento etc.)
- Celebración de acuerdos adicionales al contrato de trabajo con aquellos empleados que requieren la utilización de aplicativos del Banco de manera remota.
- Manejo y confidencialidad de contraseñas.
- Uso de barreras de comunicaciones y autenticación de conexiones a redes del Banco.
- Prohibición del uso de módems para la conexión a Internet a través de proveedores distintos del Banco.
- Prohibición de uso de celulares en determinadas áreas del Banco."

DÉCIMO CUARTO: Establecidos de esta forma los antecedentes de la presente actuación y con el fin de analizar los argumentos expuestos en su defensa por el **Banco de Bogotá S.A.** para este Despacho son pertinentes las consideraciones que pasan a exponerse:

14.1. PRIMER CARGO – SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN: se encuentra llamado a prosperar, con las salvedades que se indican en los literales a) y c) del numeral 14.1.1. del presente acápite, por las razones que se indican a continuación:

14.1.1. a) Verificación de la información publicada en Internet: aunque el Banco no realiza pronunciamiento alguno que permita desvirtuar el hallazgo efectuado durante la visita inspección al consultar las tablas maestras de la base de datos de producción y a la de ICS (que maneja la Gerencia Nacional de Cobranzas), contra los registros del video publicado, en relación con la similitud de los parámetros de los registros, centrando su defensa en describir las medidas que ha implementado, de manera general, para dar cumplimiento a la Circular 052 de 2007; esta Superintendencia no puede concluir, sin lugar a dudas, que los datos divulgados en el incidente que motivó la visita provinieron del Banco de Bogotá S.A. o de sus contratistas.

No obstante, tanto de las cifras suministradas por la entidad, verificadas *in situ* por este organismo de vigilancia, como de lo manifestado en los descargos, se concluye que la información de 29 clientes de la entidad estuvo comprometida en el incidente que originó la presente actuación administrativa. Cabe anotar que los hechos que motivaron la apertura de este expediente[6] fueron oportunamente puestos en conocimiento de las autoridades competentes, que adelantan las actuaciones policivas y penales del caso.

---

[6] Divulgación de videos a través del sitio Web http://www.youtube.com/watch?v=wpqhzogbg6w, a través del cual se ofrecía información de clientes de diferentes entidades financieras.

Mal podría este organismo de vigilancia dejar de considerar los hallazgos de que da cuenta el pliego de cargos formulado al no demostrarse que los mismos fueron la causa eficiente de la mencionada divulgación, ya que corresponde a esta entidad preservar la confianza pública y la estabilidad del sistema financiero, marco dentro del cual ejerce sus funciones administrativas, encaminadas justamente a advertir de las debilidades detectadas con ocasión de su labor de supervisión y sancionar, si es del caso, acciones u omisiones que impliquen riesgos de pérdida o divulgación no autorizada de datos personales de los clientes de las entidades vigiladas, para referirnos a este caso concreto. Bajo este presupuesto, se continúa con el estudio de los demás cargos y descargos que obran en la presente actuación.

b) Atención a clientes morosos en Oficinas del Banco de Bogotá: en sus descargos sobre este particular, el Banco describe la configuración de la conexión de la oficina con el sitio central, tal como ésta había sido evidenciada durante la visita de inspección por esta Superintendencia. Sin embargo, no se pronuncia en relación con los hallazgos detectados, ni desvirtúa el hecho de que la información transportada entre los PC (clientes – casa de cobranzas), ubicados en las oficinas del Banco y el nodo principal de la misma (switch 4503) no es cifrada, y que el canal por el que viaja no cuenta con mecanismos que garanticen su seguridad.

Cabe destacar que los dos sitios a los que se hace referencia en el pliego de cargos se encuentran físicamente ubicados en oficinas transaccionales del Banco. Adicionalmente, la información que viajaba entre los PC del personal de las casas de cobranza y el Banco no estaba integrada a la plataforma de seguridad implementada para la totalidad de los servicios que se prestan, motivo por el cual se concluye que, para la época de la visita, la Entidad no contaba con mecanismos que garantizaran la confidencialidad de dicha información.

Lo anterior, evidencia los riesgos de acceso no autorizado (factores internos o externos) y de fraude, debido a que ese segmento de la red permanecía vulnerable a la época de la visita, esto último teniendo en cuenta que la entidad informó en su respuesta que adoptó las medidas para subsanar esta debilidad (posteriores a la visita) que de ser implementadas, le permitirán resolver las debilidades detectadas por la comisión de visita sobre este particular, por todo lo cual, prospera el cargo formulado, sobre este particular.

c) Administración del Aplicativo ICS (Internet Colection System) – Sistema de información de Cobranzas para Cartera Vencida: el cargo no prospera a este respecto, toda vez que, como lo indica la entidad, el requerimiento citado como presuntamente incumplido[7] "no establece la obligatoriedad de definir roles funcionales independientes para la administración de usuarios y de las bases de datos".

[7] Subnumeral 3.1.6. del numeral 3.1., Capítulo XII, Título I de la Circular Básica Jurídica 007 de 1996.

14.1.2. Gestión de Cobranzas:

a) Casa de Cobranza "Colcartera EU": pese al error cometido, tanto en el informe de visita como en el pliego de cargos, consistente en citar el subnumeral 3.2.1. del Capítulo XII, Título I de la Circular Básica Jurídica 007 de 1996 como norma presuntamente incumplida, transcribiendo los literales d) y e) del subnumeral 3.2.2. de la misma disposición; al analizar los descargos, encuentra esta Superintendencia que: ***(i)*** el Banco se pronunció expresamente sobre los referidos literales d) y e) del subnumeral 3.2.2., lo lleva a concluir que, pese a la mencionada equivocación, no se está vulnerando su derecho a la defensa, ***(ii)*** que a pesar de contar con la cláusula de confidencialidad relacionada con el uso, divulgación, guarda y custodia de los documentos e información que el Banco le entrega al tercero, éste no venía haciendo seguimiento y monitoreo a sus políticas, definidas en el "Reglamento casa de cobranzas externas Banco de Bogotá" referente a la inclusión de cláusulas de confidencialidad suscritas entre las casas de cobranza y la cooperativa de trabajo asociado que suministra el personal, ni entre esta última y cada uno de los empleados. El Banco de Bogotá S.A. describe las medidas que viene adoptando a partir de octubre de 2009 (con posterioridad a la visita) para fortalecer el cumplimiento del numeral 3.2. del Título I, Capítulo XII de la Circular Básica Jurídica 007 de 1996, lo que lleva a esta Superintendencia ha concluir que el Banco se encuentra adoptando correctivos en relación con las debilidades advertidas durante el proceso de inspección. Cabe mencionar que los terceros a cargo de procesos del Banco, que tienen acceso a información confidencial, de la entidad o de sus clientes, deben asumir el manejo de dicha información con los criterios de seguridad y calidad requeridos en el citado instructivo, de manera que las entidades vigiladas por esta Superintendencia puedan garantizar que sus actividades se orienten a proteger la confidencialidad de dicha información, y ***(iii)*** que con posterioridad a la visita, la entidad se encuentra evaluando los contratos celebrados con entes externos y definiendo si es preciso modificarlos, para dar cumplimiento de lo requerido por el subnumeral 3.2.2. del Título I, Capítulo XII de la precitada Circular, actividad que correspondía a la primera etapa de implementación de la disposición en comento, que regía a partir del 1° de julio de 2008. Por las razones expuestas, prospera el cargo formulado, en relación con el tema en cuestión.

b) Call Center: analizados los argumentos expuestos por la entidad en sus descargos, encuentra esta Superintendencia que el Banco: ***(i)*** ha dispuesto las restricciones de uso para el recibo y envío de correo electrónico para los supervisores del Call Center, pero éstas no se han implementado efectivamente, tal como pudo verificarlo esta Superintendencia, ***(ii)*** indica acciones adoptadas en relación con los hallazgos de este organismo de vigilancia, pero no señala la fecha a partir de la cual se implementaron, en su mayoría, y en las que hay referencia, ésta es posterior a la época de la visita, y ***(iii)*** manifiesta que modificó la matriz de perfiles para que a los supervisores del *Call Center* "se les restrinja el uso de correo externo sólo para envío de información a las dirección de mail corporativas específicas que requieren en su trabajo", sin señalar la fecha en que se efectuó tal modificación, ni allegar prueba de ello. Por lo anterior, el cargo formulado, a este respecto, se encuentra llamado a prosperar.

14.2. SEGUNDO CARGO – HABEAS DATA:

14.2.1. Aunque nos referiremos en extenso a este tema en el numeral 14.4. del presente acto administrativo, resulta pertinente aclarar que, contrariamente a lo manifestado por el Banco en sus descargos[8], el dato financiero está catalogado por la Ley 1266 de 2008[9] como **semiprivado**, en los siguientes términos: "Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley".

14.3.2. La connotación de **semiprivado** que la ley de Hábeas Data otorga al dato financiero, ha sido desarrollada por la Corte Constitucional en Sentencia C-1011/08[10], en los siguientes términos:

> "La información semiprivada es aquel dato personal o impersonal que, al no pertenecer a la categoría de información pública, sí requiere de algún grado de limitación para su acceso, incorporación a bases de datos y divulgación. Por ende, se trata de información que sólo puede accederse por orden de autoridad judicial o administrativa y para los fines propios de sus funciones, o a través del cumplimiento de los principios de administración de datos personales antes analizados. Ejemplo de estos datos son la información relacionada con el comportamiento financiero, comercial y crediticio y los datos sobre la seguridad social distintos a aquellos que tienen que ver con las condiciones médicas de los usuarios." (Subrayado fuera de texto original)

En otro de sus apartes sobre este mismo tema, la misma sentencia puntualiza que:

> "En contrario, los datos semiprivados y privados, habida cuenta la naturaleza de la información que contienen, se les adscriben restricciones progresivas en su legítima posibilidad de divulgación, que

---

[8] "... desde ahora queremos puntualizar que el dato financiero no tiene la calidad de privado y, en consecuencia, frente a él no existe la obligación de reserva", y "...De esos treinta y tres (33), veintinueve (29) sí tienen o tuvieron tarjeta pero en la información sólo aparece el nombre, la dirección y la cédula, datos estos últimos – nombre, dirección y cédula – que como lo ha aclarado la jurisprudencia constitucional tienen el carácter de públicos o semiprivados". Esta Superintendencia aclara que si bien el dato financiero no es privado, tampoco es público y es considerado por la Ley y la jurisprudencia de la Corte Constitucional como **semiprivado**, conceptos todos que encuentran definición y desarrollos en las mismas fuentes citadas.

[9] Literal g) del Artículo 3°.

[10] Revisión de constitucionalidad del Proyecto de Ley Estatutaria No. 27/06 Senado – 221/07 Cámara (Acum. 05/06 Senado) "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.". Expediente PE-029. Magistrado Ponente: Dr. Jaime Córdoba Triviño.

> se aumentan en tanto más se acerquen a las prerrogativas propias del derecho a la intimidad. De esta forma, el dato financiero, comercial y crediticio, si bien no es público ni tampoco íntimo, puede ser accedido legítimamente previa orden judicial o administrativa o a través de procedimientos de gestión de datos personales, en todo caso respetuosos de los derechos fundamentales interferidos por esos procesos, especialmente el derecho al hábeas data financiero." (El subrayado es nuestro).

Y más adelante añade que:

> "Precisamente, el objeto general del Proyecto de Ley es establecer las reglas que permitan que la utilización de esa información semiprivada resulte respetuosa de los derechos y libertades predicables de los procesos de recolección, tratamiento y circulación de datos personales."

Posteriormente aclara que:

> "(...) debe tenerse en cuenta que para los efectos de la regulación sectorial que se predica del Proyecto de Ley, el legislador estatutario ha previsto que la información financiera, comercial y crediticia es una modalidad de información semiprivada. En consecuencia, no será válido que en la aplicación de las reglas contenidas en la iniciativa, que como se ha insistido, solo resultan aplicables a la administración de datos personales de contenido comercial y crediticio, se establezca que dicha información tiene carácter público, puesto que existe un mandato legal que establece, de forma expresa, lo contrario." (Subrayado extratextual)

14.3.3. Hecha la anterior precisión y pese a que la entidad suscribió cláusulas de confidencialidad con sus agentes de cobranza externos; por las razones expuestas en el numeral 14.1. de este acto administrativo, concluye esta Superintendencia que, para la época de la visita, el **Banco de Bogotá S.A.** no se encontraba observando a cabalidad el principio de seguridad, de que trata el literal f) del artículo 4° de la Ley 1266 de 2008, el cual debe concretarse en esquemas de monitoreo y control permanentes sobre los protocolos de seguridad y calidad definidos con todos los terceros que apoyan la prestación de los servicios autorizados y que por virtud de esa relación acceden a información semiprivada, cuya administración está a cargo del Banco y que como tal, es el único responsable de su manejo. Dichas acciones y resultados deberán ser debidamente probados y estar a disposición de este Organismo cuando sean requeridos, dentro del seguimiento que el tema merece. Por lo expuesto, el cargo formulado se encuentra llamado a prosperar, en relación exclusivamente con el principio de seguridad a que acá se alude.

14.3.4. No prospera el cargo formulado respecto de los principios de circulación restringida y de confidencialidad, teniendo en cuenta que esta

Superintendencia no puede concluir, sin lugar a dudas, que los datos divulgados en el incidente que motivó la visita provinieron de **Banco de Bogotá S.A.** o de sus contratistas.

14.3. TERCER CARGO – SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO (SARO): El cargo formulado se encuentra llamado a prosperar, por las razones que se indican a continuación:

a) Identificación de riesgos e implementación de controles: la entidad no desvirtúa en sus descargos el hallazgo de la Superintendencia sobre este particular, ni allega prueba alguna para controvertir la conclusión plasmada en el pliego de cargos, derivada de las matrices de riesgos de los procesos de cobranza puestas a disposición de la comisión de inspección en un CD, al cual se refiere el numeral 3.2.1. del acápite de pruebas del pliego formulado.

b) Monitoreo: el Banco no controvierte los hallazgos de esta Superintendencia sobre el particular y, por el contrario, manifiesta que se encuentra "revisando la documentación de riesgos y controles para establecer los requerimientos de información necesarios, con el objeto de generar los indicadores que permitan hacer un monitoreo oportuno, como el sugerido".

c) Capacitación: el Banco no desvirtúa los hallazgos de esta Superintendencia sobre el particular y en su respuesta manifiesta que, con posterioridad a la época de la visita, ha tomado medidas correctivas para impartir capacitación al personal de las casas de cobranza que vienen desarrollando las actividades de recaudo de su cartera vencida. Debe tenerse en cuenta que, de conformidad con lo previsto en la norma citada como presuntamente incumplida, a más tardar el 1° de julio de 2008 la entidad debió haber efectuado la capacitación a la totalidad de sus terceros y que los programas correspondientes deben ser constantemente revisados y actualizados.

14.4. EN RELACIÓN CON EL ACÁPITE DEL ESCRITO DE DESCARGOS DENOMINADO "CONSIDERACIONES GENERALES SOBRE LOS PUNTOS ANTERIORES" – A TODOS LOS CARGOS: sobre los argumentos esgrimidos por la entidad respecto de los cargos formulados, en su conjunto, esta Superintendencia efectúa los siguientes comentarios:

14.4.1. El 31 de diciembre de 2008 se publicó en el Diario Oficial la Ley 1266, "por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

14.4.2. Tal como se expuso en el numeral 14.2 del presente acto administrativo, el dato financiero está catalogado por la Ley 1266 de 2008 como **semiprivado.** En tal virtud, el mismo no puede tener el tratamiento de público y su tratamiento debe ser respetuoso de los derechos fundamentales interferidos por esos procesos, especialmente el derecho fundamental al hábeas data financiero.

14.4.3. El régimen de transición de que trata el artículo 21 de la Ley 1266 de 2008, establecido para que las personas que, a la fecha de su entrada en vigencia ejercieran alguna de las actividades por ella reguladas adecuaran su funcionamiento a las disposiciones de la ley, venció el 1° de julio de 2009, esto es, con anterioridad a la época de los hechos que motivaron la presente actuación administrativa y a la de la visita.

14.4.4. En cuanto a las citas jurisprudenciales efectuadas por el Banco, conviene efectuar las siguientes precisiones:

a) Los precedentes citados son anteriores a la Ley de Hábeas Data que, como se dijo, regula integralmente el tema de la administración de datos personales de contenido comercial y crediticio;

b) La **sentencia T-261 de 1995**[11] se refiere al caso de la entidad financiera que administraba la tarjeta de crédito del accionante y que suministró a firmas comerciales datos sobre la dirección y el teléfono de quien incoa la tutela, sin su autorización. Como se aprecia, no se trata del mismo supuesto de hecho de que se trata en esta actuación administrativa, toda vez que: ***(i)*** no se ha establecido en este caso que la entidad financiera haya suministrado la información al tercero que la estaba comercializando, como si se determinó en el caso de la tutela en cuestión, ***(ii)*** la información divulgada en el caso que nos ocupa, no solamente comprendía dirección, teléfono, estado civil "y demás datos demográficos" (a los que se refiere el Banco de Bogotá en sus descargos), sino que también se asociaba al documento de identidad de cada uno de los titulares del producto tarjeta de crédito (TC), hecho que no fue desvirtuado por el Banco, y ***(iii)*** los datos a los que se refiere la sentencia no fueron expuestos a una consulta pública a través de Internet.

c) El aparte de la **sentencia SU-082 de 1995** de la Corte Constitucional, trascrito por el Banco en sus descargos, tampoco resulta aplicable a este caso concreto, por cuanto se refiere específicamente la información que las instituciones de crédito reportan a los bancos de datos, en relación con la forma en que el sujeto concernido cumple sus obligaciones económicas. En tal caso, media la autorización previa para efectuar tales reportes, lo cual no ocurrió con la publicación efectuada a través de Internet, a que se refiere la presente actuación administrativa.

d) Finalmente, en **sentencia T-729 de 2002** la Corte Constitucional clasificó la información en cuatro tipos (pública o de dominio público, semi-privada, privada y reservada o secreta), ante la ausencia de regulación en materia de

[11] Acción de tutela instaurada por GERMAN HUMBERTO RINCON PERFETTI contra SISTEMA PRONTA S.A. DE TARJETAS DE CREDITO, PRONTA S.A. COMPAÑIA DE FINANCIAMIENTO COMERCIAL y la REVISTA LATINOAMERICANA INTERNACIONAL. Magistrado Ponente Dr. JOSE GREGORIO HERNANDEZ GALINDO.

hábeas data para la época (2002). Sin embargo, en el año 2008 se expidió la Ley 1266, la cual, retomando en gran parte la jurisprudencia de la citada Corte sobre la materia, definió los tipos de información (artículo 3°) y estableció los principios para la administración de los datos (artículo 4°), entre otras disposiciones. Es bajo estos parámetros legales que esta Superintendencia formuló los cargos respectivos, analizó los descargos de la entidad y profiere el presente acto administrativo. Y considerando que la mencionada Corte es la intérprete final y autorizada de la Constitución, la Ley de Hábeas Data se ha analizado por parte de esta Superintendencia, para efectos del presente acto administrativo, a la luz de la Sentencia C-1011/08.

14.4.5. Desconoce esta Superintendencia los fundamentos de la afirmación del Banco según la cual la Ley de Hábeas Data solamente regula el tema frente a los "administradores de bases de información". Sobre el particular, resultan pertinentes los siguientes comentarios: ***(i)*** Si bien es cierto que la ley 1266 de 2008 regula la materia parcialmente, como se afirma en los descargos, cabe aclarar que dicha especialidad se refiere específicamente a la **información financiera, crediticia, comercial, de servicios y la proveniente de terceros países** y no a que la norma solamente sea aplicable únicamente a los operadores de bancos de datos de este tipo de información, y ***(ii)*** en la mencionada ley se establecen derechos de los titulares de la información frente a las fuentes y usuarios de la misma (artículo 6°) - doble condición que ostenta el Banco de Bogotá S.A. Así mismo, se establecen deberes de las fuentes (artículo 8°) y de los usuarios (artículo 9°) de la información. Además regula lo relacionado con las peticiones, consultas y reclamos que los titulares de la información pueden presentar directamente ante las fuentes (artículo 16) y además, se define lo relacionado con la vigilancia de los destinatarios de la ley, indicando que "en los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia, está ejercerá la vigilancia e impondrá las sanciones correspondientes, de conformidad con las facultades que le son propias, según lo establecido en el Estatuto Orgánico del Sistema Financiero y demás normas pertinentes y las establecidas en la presente ley." (artículo 17 - Subrayado fuera de texto original).

14.4.5. Respecto de las consideraciones referidas a la obligatoriedad que se predica de "todas las personas" de guardar la reserva o confidencialidad de la información, por tratarse de un derecho constitucional, que permiten concluir al Banco que "no puede constituirse en un hecho censurable la no celebración de contratos o acuerdos puntuales sobre el particular", conviene precisar que la misma afirmación podría hacerse respecto de todos los derechos fundamentales que aparecen relacionados en la Carta Política, óptica bajo la cual, no se haría necesaria la expedición de leyes, decretos, reglamentos y otras regulaciones, toda vez que bastaría con observar los postulados (genéricos) de la Constitución Política para que todos los asociados cumpliéramos el contrato social. En opinión de esta Superintendencia, el deber de "todas las personas", entre ellos los contratistas del Banco, de observar las disposiciones constitucionales en cita, no exonera a la entidad vigilada de cumplir con los instructivos que rigen su actividad (puntualmente, con las Circulares citadas como presuntamente incumplidas en el

pliego de cargos formulado, en las cuales se establecen parámetros mínimos, con fundamento en los cuales los vigilados gestionan sus riesgos operativos).

g) En cuanto a la argumentación referida a los trabajadores y empleados del Banco, así como a las previsiones contenidas en los contratos de trabajo de los mismos, cabe resaltar que esta Superintendencia tiene claro que los terceros (casas de cobranza) no son empleados del Banco y que las debilidades operativas a las que se refieren los cargos formulados, no se relacionan con relaciones laborales. El Banco remite a documentos tales como "el contrato de trabajo y el reglamento de trabajo aprobado por el Ministerio de la Protección Social", indicando que en los mismos aparece consignada la obligación de guardar reserva y otras relacionadas, documentos que no allega y que, además, por lo expresado, poco contribuirían a esclarecer la posición del Banco en relación con los cargos formulados en el pliego correspondiente.

e) Sobre las relaciones contractuales con terceros (casas de cobranza), este Organismo no cuestiona que se comparta con ellos la información que "es esencial para el ejercicio de la labor encomendada". Lo que ha merecido reparo son las condiciones de seguridad bajo las cuales el Banco gestiona dicho intercambio, a la luz de la normatividad vigente y citada como presuntamente incumplida en el pliego de cargos, por cuya observancia corresponde velar a esta Superintendencia.

El Banco insiste en que todas las personas están obligadas a observar la constitución y la ley, especialmente si éstos son abogados, por lo cual no se haría necesario incluir cláusulas de confidencialidad en los contratos celebrados con estos profesionales. Esta posición merece todo el respeto desde el punto de vista iusfilosófico, sin embargo, tanto los instructivos de esta Superintendencia como la Ley de Hábeas Data, que se citan como presuntamente incumplidos en el pliego de cargos, se encuentran vigentes y son de obligatoria observancia por parte de las entidades vigiladas, al tenor de lo dispuesto por el literal a), numeral 3 del artículo 326 del Estatuto Orgánico del Sistema Financiero y de la Ley 1266 de 2008, respectivamente.

f) Finalmente, el Banco relaciona algunas de las políticas que tiene en materia de seguridad de la información, pero sin allegar prueba alguna que desvirtúe los hallazgos de esta Superintendencia sobre ese particular, especialmente en cuanto se refiere al cargo proferido respecto de este tema en concreto (numeral 2.1. del pliego).

Por lo expuesto, las consideraciones efectuadas por la entidad "sobre los puntos anteriores", no desvirtúan los cargos formulados.

DÉCIMO QUINTO: PROCEDENCIA DE LA SANCIÓN: Teniendo en cuenta lo indicado anteriormente, en relación con la prosperidad de los cargos imputados por esta Superintendencia al Banco de Bogotá S.A., con las salvedades que se indican en los literales a) y c) del numeral 14.1.1. del presente acto administrativo, y teniendo en cuenta las circunstancias de atenuación de los mismos, consistentes

en la implementación *a posteriori* de medidas tendientes a subsanar las debilidades detectadas durante el proceso de inspección, la Superintendencia Financiera de Colombia

R E S U E L V E:

ARTÍCULO PRIMERO: Imponer al **Banco de Bogotá S.A.,** identificado con NIT 860002964-4, la sanción consistente en multa a favor del Tesoro Nacional por valor de TREINTA MILLONES DE PESOS MONEDA CORRIENTE ($30'000.000,oo) de conformidad con lo expuesto en la parte motiva de esta Resolución.

El pago de la multa que mediante esta resolución se impone se debe efectuar en el Banco de la República, cuenta corriente número 61012027, código de portafolio 151 a nombre de la Dirección del Tesoro nacional D.T.N. – Otras tasas y multas, mediante consignación en efectivo o cheque de gerencia.

El pago deberá efectuarse a más tardar el día hábil siguiente al de la fecha de ejecutoría de la presente resolución. A partir de esa fecha y hasta el día de su pago se causará un interés equivalente a una y media veces (1.5) el interés bancario corriente certificado por la Superintendencia Financiera de Colombia para el respectivo periodo sobre el valor insoluto de la sanción. La consignación deberá acreditarse ante la Subdirección Administrativa y Financiera de esta entidad dentro de los diez (10) días hábiles siguientes a la fecha de la ejecutoría.

ARTÍCULO SEGUNDO: Notifíquese personalmente el contenido de la presente Resolución al doctor ALEJANDRO AUGUSTO FIGUEROA JARAMILLO, representante legal del **Banco de Bogotá S.A.,** o quien haga sus veces; acto en el cual deberá entregársele copia de la misma y advertírsele que contra ella procede únicamente el recurso de apelación ante el Superintendente Financiero de Colombia, dentro de los cinco (5) días hábiles siguientes a la fecha de su notificación, de acuerdo con lo establecido en el literal l) del numeral 4 del artículo 208 del Estatuto Orgánico del Sistema Financiero.

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., 24 SET. 2010

MIGUEL ÁNGEL VILLALOBOS HERNÁNDEZ
Superintendente Delegado para Riesgos Operativos
240000

Notificar Personalmente:
Doctor ALEJANDRO AUGUSTO FIGUEROA JARAMILLO
Representante Legal
Banco de Bogotá S.A.
Calle 36 No. 7 – 47
Bogotá, D.C.