MANUAL DE BUENAS PRÁCTICAS
PARA EL MANEJO DE LOS DATOS PERSONALES
DE LOS CLIENTES DE LOS SERVICIOS FINANCIEROS

I) OBJETO

El presente Manual tiene como objeto promover, asesorar y proteger la autodeterminación informativa de los clientes de las entidades financieras con el objetivo de que puedan conocer los datos que tenga la entidad financiera respectiva; los fines para los cuales esos datos están destinados; que estos sean empleados solamente para el fin permitido por el ordenamiento jurídico; y además, que los datos sean rectificados, actualizados, complementados o suprimidos si son incorrectos o inexactos, o si están siendo utilizados para un fin distinto del que legítimamente pueden cumplir.

II) DEFINICIONES

A efectos del presente Manual se entenderá como:

a) **Entidad Financiera**: Cada uno de los bancos estatales, públicos o privados, financieras, cooperativas, mutuales o cualesquiera otro intermediario financiero que integre o llegue a integrar legítimamente el Sistema Financiero Nacional.

b) **Base de datos interna, personal o doméstica**: Cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales públicos o privados, mantenidos por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando éstas no sean vendidas o de cualquier otra manera comercializadas.

c) **Datos personales:** Cualquier dato relativo a una persona física identificada o identificable.

d) **Datos sensibles**: Se trata de información relativa al fuero íntimo de la persona, que no conciernen más que a su titular y a quienes éste quiera participar de ellos, tales como su orientación ideológica, fe religiosa o espirituales, condición socioeconómica, preferencias sexuales, raza, opinión pública, información biomédica o genética, es decir, aquellos aspectos propios de su personalidad. No siendo permitido el acceso de terceros sin su consentimiento expreso.

e) **Datos personales de acceso restringido:** Aquellas informaciones que, aún formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Por ejemplo: Datos que consten en la Caja Costarricense del Seguro Social, Ministerio de Hacienda, SICVCA, entre otros.

f) **Datos personales de acceso irrestricto:** los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados. Por ejemplo: Datos del Registro Público Nacional, Datos del Registro Civil, entre otros.

g) **Cliente:** persona física, titular de los datos que sean objeto del tratamiento automatizado o manual.

h) **Consentimiento informado del titular de los datos personales**: Toda manifestación de voluntad, expresa, libre, inequívoca, informada y específica que se otorgue por escrito por medio físico o electrónico, para un fin determinado, mediante la cual el titular de los datos personales o su representante, consienta el tratamiento de sus datos personales.

i) **Tratamiento de datos personales:** cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por

transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros.

III) LEGISLACIONES

El contenido del presente Manual es concordante con las disposiciones establecidas tanto por la legislación y normativa vigente emitida por los órganos reguladores aplicable a los bancos o instituciones financieras, incluyendo pero sin limitarse a las siguientes:

- Ley Orgánica del Sistema Bancario Nacional
- Ley Orgánica del Banco Central de Costa Rica
- Ley 5044 (de empresas financieras).
- Ley General de Administración Pública
- Ley 8204 sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de uso no Autorizado, Actividades Conexas, Legitimación de Capitales y Financiamiento al Terrorismo y su Normativa Conexa.
- Reglamento a la Ley 8204.
- Normativa Acuerdo SUGEF 12-10.
- Ley de Protección de la Persona frente al tratamiento de sus datos personales y su Reglamento.
- Reglamento de tarjetas de crédito y débito
- Acuerdo SUGEF 7-06 denominado "Reglamento del Centro de Información Crediticia"[1], vigente a partir del 13 de junio del 2006.

[11] Proyecto de Modificación al Acuerdo SUGEF 7-06 enviado en consulta al Sector Bancario y Financiero, mediante oficio CNS-1123/11. Éste último está precisamente en período de consulta, por lo que aún estas modificaciones no han sido aprobadas.

- Acuerdo SUGEF 14-09 “Reglamento sobre la Gestión de la tecnología de la información”.

En caso de discrepancia entre las disposiciones establecidas en el presente Manual y las señaladas por la legislación y normativa vigente y/o futura, prevalecerá lo que éstas últimas dispongan.

IV) PRINCIPIOS

El presente Manual pretende responder a los siguientes principios, así como también implementar acciones que se deriven de la puesta en práctica de estos:

a) Principio de confidencialidad

La entidad financiera deberá guardar secreto de todos los datos que manejen de sus clientes salvo que se encuentre dentro de las excepciones estipuladas en la Ley. Este deber se extiende a cualquier persona o entidad que intervenga en cualquiera de las fases de tratamiento de la información, aun cuando haya terminado su relación con la entidad financiera.

El personal de las entidades financieras deberá guardar la confidencialidad con ocasión de ejercicio de las facultades propias de su función, principalmente cuando se acceda a información sobre datos personales y sensibles. Esta obligación perdurará aun después de finalizada la relación con la entidad.

Las entidades financieras deberán proteger y utilizar adecuadamente cualquier dato o información confidencial que les suministren sus clientes. Ésta deberá ser utilizada de manera exclusiva para el propósito por el cual fue requerida, salvo los casos que la ley lo permita o cuando el cliente lo autorice para otros fines.

b) Principio de finalidad de la información:

Se recopilarán aquellos datos personales que sean adecuados y pertinentes en relación con la finalidad que persigan para su recopilación. Los datos sensibles serán utilizados para el fin para el cual fueron recopilados. Una vez recopilados deberán mantenerse exactos y actualizados por

el cliente de forma que correspondan a la situación actual de su titular. Además se le garantizará al titular de los datos su derecho de acceso cuando lo considere oportuno.

c) Derecho de información:

Cada entidad financiera deberá, a la hora de solicitar al cliente información, indicarle el fin para el cual está siendo recopilada y el tratamiento que se le va a dar. Se le indicará su derecho de acceso y rectificación, cancelación o eliminación, salvo las excepciones establecidas en la ley.

d) Consentimiento informado:

Los datos de carácter personal serán tratados únicamente con el consentimiento de su titular, salvo que una ley disponga otra cosa.

e) Los datos especialmente protegidos:

Se deberá respetar el régimen de protección establecido en la ley para aquellos datos sensibles.

f) Principio de la seguridad de los datos:

Las bases de datos de las entidades financieras deberán adoptar las medidas técnicas y organizativas que sean viables para garantizar la seguridad de los datos.

g) Principio de comunicación de datos:

La entidad financiera deberá solicitar el permiso del titular para poder comunicar la información a cualquier tercero que así lo requiera en razón de su función y del fin para el cual fueron entregados los datos, salvo las excepciones de Ley.

V. OBLIGACIONES DE LAS ENTIDADES FINANCIERAS

a) Recursos humanos, físicos y tecnológicos:

Las entidades financieras deben proveer los recursos necesarios para recopilar y administrar los los datos de sus clientes, de conformidad con los principios de la Ley.

b) Deber de brindar información:

Las entidades financieras deben proporcionar a los titulares de los datos personales, la información sobre la finalidad para la que son recabados. Además deberán obtener su consentimiento para el tratamiento de los datos personales del cliente, salvo las excepciones de ley e informarle de la posibilidad de ejercitar los derechos de acceso y rectificación, cancelación o eliminación.

El texto informativo utilizado para este propósito será redactado de forma tal que sea lo más claro y legible posible y con un lenguaje que sea fácilmente comprensible.

c) Deber de utilizar los datos de los clientes según el fin para el cual fueron recopilados:

La entidad financiera se compromete a utilizar los datos que manejan de sus clientes según el fin para el cual fueron recopilados, salvo las excepciones de Ley.

d) Deber de secreto y seguridad:

La entidad financiera procurará utilizar los medios necesarios para el cumplimiento de los deberes de secreto y seguridad en el manejo de los datos de sus clientes.

e) Deber de veracidad y actualización:

Los datos manejados deben ser exactos y responder a la situación informada por el titular. Bajo esta premisa la entidad financiera se compromete a mantenerlos actualizados con la información que por su parte el cliente suministre y conservarlos durante el tiempo necesario para la finalidad para la que fueron recopilados.

f) Deber de permitir la consulta:

La entidad financiera le facilitará a su titular, cuando éste lo solicite, los datos que se tienen de éste en su base de datos.

~~g)~~ Respeto al Derecho de rectificación, cancelación o eliminación:

La entidad financiera respetará el derecho de rectificación, cancelación o eliminación de la información que se maneja del cliente siempre y cuando una Ley no establezca lo contrario. En el caso de la eliminación se le informarán los efectos de su solicitud.

Aprobado en sesión del Foro Interbancario Legal del 22 de mayo del 2015 y comunicado a los Bancos e Instituciones Financieras el 29 de mayo del 2015