CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

CÓDIGO
DE BUENAS PRÁCTICAS BANCARIAS
PARA LA PROTECCIÓN DE LOS SERVICIOS ELECTRÓNICOS

Versión revisada y aprobada por el Foro Interbancario de Seguridad en TI de la
Cámara de Bancos e Instituciones Financieras de Costa Rica
en sesión del 13 de noviembre del 2013

CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

El Foro Interbancario de Seguridad en TI recomienda a los Bancos e Instituciones Financieras adoptar el siguiente:

"CÓDIGO DE AUTORREGULACIÓN DE BUENAS PRÁCTICAS BANCARIAS PARA LA PROTECCIÓN DE LOS SERVICIOS ELECTRÓNICOS"

ARTÍCULO 1.- OBJETIVO.

El presente Código de Autorregulación de Buenas Prácticas Bancarias se aplicará a los servicios electrónicos que brindan las entidades bancarias y financieras a sus clientes.

ARTÍCULO 2.-DEFINICIONES.

A los efectos del presente Código de Autorregulación se entenderá por:

Servicio electrónico: Aquel que permite al cliente realizar transacciones tales como: consultas, transferencias, retiros, depósitos, pagos, entre otras; mediante sistemas electrónicos provistos por las entidades bancarias y financieras a través de redes privadas y públicas.

Autenticación: proceso de verificación de la identidad del cliente del servicio electrónico

Dispositivo de autenticación: medio o instrumento utilizado en el proceso de autenticación.

ARTÍCULO 3.-CLAÚSULAS CONTRACTUALES.

Los bancos e instituciones financieras sólo deberán permitir a sus clientes la utilización de servicios electrónicos, cuando cuenten con el consentimiento expreso de éstos, mediante los mecanismos legales establecidos por la entidad.

En la prestación de servicios electrónicos a sus clientes, será recomendable que los bancos e instituciones financieras establezcan en los reglamentos y contratos respectivos, de manera clara y precisa, lo siguiente:

a) Las operaciones que podrán realizarse mediante los servicios electrónicos.

b) Los mecanismos de identificación y autenticación del cliente requeridos para la utilización del servicio.

c) Los mecanismos de confirmación de las operaciones realizadas mediante los servicios electrónicos, de acuerdo con los medios que cada entidad determine.

d) Los derechos y obligaciones correspondientes al uso de los servicios electrónicos, tanto para los bancos e instituciones financieras, como para los clientes.

e) Al menos las siguientes obligaciones para los bancos e instituciones financieras, sin perjuicio de que en el contrato respectivo se pacten otras adicionales:

   i. Comunicar a los clientes los riesgos inherentes a la utilización de los servicios electrónicos y las recomendaciones para prevenirlos.

   ii. Comunicar a los clientes las recomendaciones para hacer un uso adecuado del servicio.

   iii. El compromiso de los bancos e instituciones financieras de proteger la información del cliente en su poder.

   iv. El compromiso de los bancos e instituciones financieras de no requerir información que comprometa la seguridad de sus mecanismos de autenticación.

f) Al menos las siguientes obligaciones del cliente, sin perjuicio de que en el contrato respectivo se pacten otras adicionales:

   i. El compromiso de los clientes de seguir las recomendaciones, instrucciones y procedimientos establecidos por los bancos e instituciones financieras para proteger su información confidencial.

   ii. Notificar de inmediato al banco o institución financiera cuando se presente alguna de las siguientes situaciones:

      - La pérdida o el robo de los dispositivos de autenticación entregados para el uso de los servicios electrónicos.

- transacciones no autorizadas, errores u otras anomalías.
- Cuando detecte o sospeche alguna irregularidad al utilizar los servicios electrónicos.

iii. No anotar en ningún lugar su número de identificación personal, clave, PIN u otro código, especialmente en el dispositivo de autenticación.

iv. Suministrar al banco o institución financiera correspondiente una dirección de correo electrónico para recibir notificaciones y mantenerlo actualizado.

g) Procedimientos de resolución alterna de conflictos, mediante los cuales las partes se comprometan a resolver en definitiva sus diferencias patrimoniales de naturaleza disponible, utilizando alguno de los mecanismos previstos en la Ley sobre la Resolución Alterna de Conflictos y Promoción de la Paz Social, el Reglamento de Arbitraje de los Centros de Conciliación y Arbitraje u otros existentes en el país.

h) La facultad de los bancos e instituciones financieras para solicitar a los clientes la información que estimen necesaria para la prestación del servicio electrónico, así como los medios y procedimientos por los cuales se les solicitará dicha información.

i) La facultad de los bancos o instituciones financieras para que, en caso de que detecten eventos que se aparten del uso habitual del cliente, puedan suspender temporalmente los servicios electrónicos hasta tanto puedan ser verificadospor las partes.

ARTÍCULO 4.-

Es recomendable que en los servicios electrónicos ofrecidos a sus clientes, los bancos e instituciones financieras, cumplan como mínimo con lo siguiente:

a) Cifrar la transmisión de información, cuando se realice a través de redes públicas.

b) Establecer mecanismos para el proceso de generación y entrega de contraseñas, claves de acceso o dispositivos de autenticación, que aseguren que quien los reciba, sea únicamente el dueño o autorizado de la cuenta.

c) Realizar las acciones necesarias para que los clientes no utilicen como clave de acceso, PIN o contraseña, datos fácilmente identificables tales como:

i. Datos personales del cliente como su cédula o su nombre.

ii. El nombre del banco o institución financiera.

iii. El identificador del cliente dado por el Banco o Institución Financiera.

iv. Secuencias ni repeticiones numéricas

d) La longitud de las contraseñas o claves de acceso deberá ser de al menos ocho caracteres.

e) Las contraseñas o claves de acceso deberán incluir mayúsculas, minúsculas, números y caracteres especiales

f) La vigencia máxima de las contraseñas o claves de acceso será de 90 días naturales.

g) Las contraseñas o claves de acceso deberán almacenarse utilizando un algoritmo estándar de cifrado de no reversión.

h) Implementar controles para evitar la lectura de los caracteres que componen las contraseñas o claves de acceso digitadas por el cliente en la pantalla del medio electrónico de acceso.

i) Establecer mecanismos para que, en caso de que exista inactividad en una sesión por parte de un cliente, por un lapso que determine el banco o institución financiera, la sesión se dé por terminada en forma automática.

j) En el evento de que en el sitio web o aplicación del Banco o institución financiera se incluyan enlaces (links) a sitios de terceros, se deberá comunicar al cliente que está abandonando el sitio del banco o institución financiera, cuya seguridad no depende, ni es responsabilidad del banco o institución financiera.

k) Establecer esquemas de bloqueo automático de contraseñas o claves de acceso, al menos para los casos siguientes:

i. Cuando se intente ingresar a los servicios electrónicos utilizando contraseñas o claves de acceso incorrectas. En ningún caso los intentos de acceso fallidos deberían exceder de tres ocasiones consecutivas sin que se genere el bloqueo automático.

ii. Cuando el cliente no utilice los servicios electrónicos por un periodo que determine cada banco o institución financiera.

iii. La institución deberá prever procedimientos para el restablecimiento del acceso al servicio, que aseguren que el cliente correspondiente sea quien lo restablezca. En el caso de que se utilicen preguntas secretas, o mecanismos similares, las respuestas respectivas serán almacenadas en forma cifrada.

l) Evitar el acceso en forma simultánea mediante la utilización de un mismo Identificador del cliente, a los servicios electrónicos del banco o institución financiera.

m) Realizar campañas de difusión de recomendaciones de seguridad dirigidas a sus clientes, para la correcta utilización de los servicios electrónicos.

ARTÍCULO 5.-

Los bancos e instituciones financieras no solicitarán a los clientes, a través de sus colaboradores o terceros, sus contraseñas o claves de acceso.

ARTÍCULO 6.-

En caso de que la operación de los servicios electrónicos o su mantenimiento sean tercerizados, el banco o institución financiera deberá establecer los Contratos de Confidencialidad idóneos, para procurar la seguridad de la información.

ARTÍCULO 7.-

Es recomendable que los bancos e instituciones financieras establezcan los medios, canales y procedimientos mediante los cuales se les solicitará, notificará y actualizará la información a los clientes.

ARTÍCULO 8.-

Es recomendable que los bancos e instituciones financieras establezcan los controles mínimos que a continuación se mencionan para la utilización de los servicios electrónicos:

a) Implementar mecanismos de autenticación de doble factor.

b) Establecer los mecanismos de control para el registro de cuentas destino y de ser necesario establecer un período de tiempo para que dichas cuentas queden habilitadas .

c) Establecer límites de monto para operaciones monetarias. En caso de que el cliente desee variar el límite preestablecido, cada banco e institución financiera determinará los medios y procedimientos para ese fin.

ARTÍCULO 9.-

Los bancos e instituciones financieras que pongan al alcance de los clientes, en sus instalaciones o en áreas de acceso al público, equipos para el uso de los servicios electrónicos, deberán adoptar controles de seguridad de orden físico y lógico, que impidan el acceso o la captura de la información.

ARTÍCULO 10.-

Es recomendable que los bancos e instituciones financieras mantengan mecanismos de control para la detección de las transacciones que se aparten de los parámetros de uso habitual del cliente, a efecto de que tomen las acciones de protección pertinentes.

ARTÍCULO 11.-

Los bancos e instituciones financieras deberán contar con bitácoras que permitan la trazabilidad de las transacciones realizadas. Se recomienda registrar al menos la siguiente información:

a) Los datos de la conexión y desconexión al servicio electrónico: fecha, hora exacta, dirección origen (IP) así como la identificación del usuario.

b) Los datos de la transacción: tipo de transacción, fecha, hora exacta, cuentas relacionadas (origen y destino), monto y moneda.

Las bitácoras deberán ser almacenadas de forma segura y contemplar mecanismos de sólo lectura, así como mantener procedimientos de control interno para su acceso y disponibilidad.

ARTÍCULO12.-

Los bancos e instituciones financieras deberán establecer las políticas y procedimientos para la gestión de incidentes de seguridad de información que se puedan suscitar durante la prestación de los servicios electrónicos.