



CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

**CÓDIGO DE AUTORREGULACIÓN
DE BUENAS PRÁCTICAS BANCARIAS PARA
LA PROTECCIÓN DE LAS TRANSACCIONES
EFECTUADAS MEDIANTE EL USO DE
INSTRUMENTOS ELECTRÓNICOS DE PAGO**



**Recomienda a las instituciones Bancarias y Financieras
adoptar el siguiente:**

**“CÓDIGO DE AUTORREGULACIÓN DE BUENAS
PRÁCTICAS BANCARIAS PARA LA PROTECCIÓN DE
LAS TRANSACCIONES EFECTUADAS MEDIANTE
INSTRUMENTOS ELECTRÓNICOS DE PAGO”**

ARTÍCULO 1.-

El presente Código de Autorregulación de Buenas Prácticas Bancarias se aplicará a las transacciones efectuadas por las entidades bancarias y financieras, mediante instrumentos electrónicos de pago.

ARTÍCULO 2.-

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

- a) «Instrumento electrónico de pago»: aquellos que permiten el acceso (a distancia) a la cuenta de un cliente, en particular las tarjetas de pago, y los servicios de telebanco (por teléfono y por computador), incluyendo pero sin limitarse a: las transferencias de fondos efectuadas mediante un instrumento electrónico de pago; el retiro de dinero en efectivo mediante un instrumento electrónico de pago; y la carga (y descarga) de un instrumento de dinero electrónico en dispositivos como cajeros automáticos.
- b) «Emisor»: La persona que, en desarrollo de su actividad profesional, pone a disposición de otra persona un instrumento electrónico de pago, en virtud de un contrato suscrito con él. Para los efectos de este Código se entenderá también como “emisor” la expresión “banco e institución financiera.”



CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

- c) «Titular»: La persona que, en virtud de un contrato suscrito con un emisor, posee un instrumento electrónico de pago. Para los efectos de este Código se entenderá también como “titular” la expresión “cliente”.

ARTÍCULO 3.-

En los casos en que bancos e instituciones financieras (emisores) pacten la prestación de servicios a sus clientes (titulares), mediante el uso de instrumentos electrónicos de pago, será recomendable que en los reglamentos y contratos respectivos establezcan de manera clara y precisa las bases para determinar:

- a) Las operaciones y servicios que podrán proporcionarse a través de instrumentos electrónicos de pago.
- b) Los mecanismos o procedimientos de identificación del cliente, así como las responsabilidades correspondientes al uso de los instrumentos electrónicos de pago, tanto para los bancos e instituciones financieras como para los clientes.
- c) Los medios por los que se haga constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate, incluyendo los métodos de autenticación tales como contraseñas, claves de acceso u otros.
- d) Los mecanismos de confirmación de la realización de las operaciones celebradas a través de cualquier instrumento electrónico de pago.
- e) El compromiso de los bancos e instituciones financieras de no requerir información confidencial que comprometa la seguridad de sus medios de autenticación, por medio de internet.



CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

- f) Acuerdo arbitral – de equidad o de derecho, según lo determine cada banco e institución financiera - mediante el cual las partes se comprometan a resolver en definitiva cualquier posible conflicto de intereses, utilizando alguno de los mecanismos previstos en el Reglamento de Arbitraje de alguno de los Centros de Conciliación y Arbitraje existentes en el país definido por las partes en los reglamentos y/o contratos, de acuerdo con lo establecido en la Ley 7727 sobre la Resolución Alternativa de Conflictos y Promoción de la Paz Social. En el momento en que se autorice el Centro de Conciliación y Arbitraje de la Cámara de Bancos e Instituciones Financieras, los bancos e instituciones financieras someterán sus conflictos de intereses con sus respectivos clientes, a los mecanismos previstos en el Reglamento de Arbitraje de este Centro.
- g) Al menos las siguientes obligaciones del cliente, sin perjuicio de que en el contrato respectivo se pacten otras adicionales:
- i. Utilizar el instrumento electrónico de pago en las condiciones aplicables a la emisión y utilización de tales instrumentos; en particular, tomar todas las medidas adecuadas para garantizar la seguridad de los medios electrónicos (computador, teléfono, etc.) y de los mecanismos (número de identificación personal u otro código), que permitan su utilización.
 - ii. Notificar sin demora al emisor: i) la pérdida o el robo del instrumento electrónico de pago o de los medios que permitan su utilización; ii) el registro en su cuenta de cualquier transacción no autorizada; iii) cualquier error u otra anomalía en la gestión de su cuenta por parte del emisor; iv) cuando se entere de la invasión de un programa tipo troyano, keylogger, o cualquier otro malware, al computador que normalmente utilice para sus transacciones.
 - iii. No anotar su número de identificación personal u otro código de forma fácilmente reconocible, especialmente en el instrumento electrónico de pago o en cualquier objeto que guarde o que lleve junto con el mismo.
 - iv. Suministrar al banco o institución financiera correspondiente un medio electrónico o digital para recibir notificaciones. Cada vez que el cliente realice una transacción, el banco o institución financiera podrá remitirle una confirmación, de acuerdo con los medios que cada entidad determine.



CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

- v. Los bancos e instituciones financieras sólo deberán permitir a sus clientes la utilización de instrumentos electrónicos de pago, cuando cuenten con el consentimiento expreso de éstos, otorgado mediante su firma original o digital, en este último caso cuando ésta esté disponible, previo al primer uso que hagan de dichos medios. A tales efectos los bancos e instituciones financieras deberán comunicar por escrito a los clientes los riesgos inherentes a la utilización de los instrumentos electrónicos de pago y las recomendaciones para prevenir la realización de operaciones irregulares o ilegales. A su vez, cada cliente deberá firmar – personal o digitalmente (cuando esté disponible) - una copia de la comunicación que le sea entregada por los bancos e instituciones financieras correspondientes, en señal de que ha recibido, conoce, consiente y acepta expresamente en el uso de los instrumentos electrónicos de pago de conformidad con las condiciones allí establecidas. Dichas condiciones serán de acatamiento obligatorio para todas las partes.

ARTÍCULO 4.-

Es recomendable que en la utilización de instrumentos electrónicos de pago para proporcionar servicios a sus clientes, los bancos e instituciones financieras cumplan como mínimo con lo siguiente:

- a) Encriptar la transmisión de información, cuando el medio electrónico utilizado para llevar a cabo consultas, operaciones monetarias y cualquier otro tipo de transacción bancaria, entre el banco o institución financiera y sus clientes, sea la red electrónica mundial denominada Internet.
- b) Establecer mecanismos para el proceso de generación y entrega de contraseñas o claves de acceso que aseguren que sólo aquél que tenga en su poder la contraseña o clave de acceso podrá activarlos. Adicionalmente, deberán realizarse las acciones necesarias para que los clientes no utilicen como contraseña o clave de acceso:
 - i. El identificador del cliente.
 - ii. Datos personales del cliente como su cédula o su nombre.
 - iii. El nombre del banco o institución financiera.
 - iv. Más de dos caracteres idénticos en forma consecutiva.



CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

- v. Más de dos consecutivos numéricos o alfabéticos.
- c) La longitud de las contraseñas o claves de acceso deberá ser de al menos ocho caracteres, cuando los medios utilizados sean la red electrónica mundial denominada Internet.
 - d) Cuando el medio electrónico utilizado sea la red electrónica mundial denominada Internet, las contraseñas o claves de acceso deberán incluir mayúsculas, minúsculas y números.
 - e) La vigencia máxima de las contraseñas o claves de acceso será de 30 días naturales.
 - f) Proveer lo necesario 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.
 - g) 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, de acuerdo al servicio de que se trate y en función de los riesgos inherentes al mismo, la sesión se dé por terminada en forma automática. En ningún caso el período de inactividad en una sesión debería exceder de un minuto.
 - h) En el evento de que se ofrezcan servicios de afiliados o de terceros mediante enlaces electrónicos, se deberá comunicar al cliente que al momento de ingresar a dichos servicios se cerrará la sesión establecida con el banco o institución financiera y se ingresará a otra cuya seguridad no depende, ni es responsabilidad de ese banco o institución financiera.
 - i) Establecer esquemas de bloqueo automático de contraseñas o claves de acceso, cuando menos para los casos siguientes:
 - i. Cuando se intente ingresar a los instrumentos electrónicos de pago 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.



CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

- ii. Cuando el cliente se abstenga de realizar movimientos por depósitos o retiros o acceder a su cuenta a través de medios electrónicos por un periodo que determine cada banco o institución financiera en sus políticas de operación, de acuerdo con el servicio de que se trate y en función de los riesgos inherentes al mismo. En los casos anteriores, la institución deberá prever procedimientos para el restablecimiento de contraseñas o claves de acceso que aseguren que el cliente correspondiente sea quien las restablezca, de acuerdo a lo que el medio electrónico de que se trate permita. Los bancos e instituciones financieras podrán hacer uso de preguntas secretas, siempre que las respuestas respectivas sean almacenadas en forma encriptada y que cada pregunta pueda ser utilizada en una sola ocasión para el restablecimiento de sus contraseñas.
- j) Evitar el acceso en forma simultánea mediante la utilización de un mismo Identificador del cliente, al sitio de la red electrónica mundial denominada Internet que corresponda al dominio del banco o institución financiera disponible para la realización de consultas, operaciones monetarias y cualquier otro tipo de transacción bancaria.
- k) Realizar campañas de difusión de recomendaciones de seguridad dirigidas a sus clientes, para la realización de operaciones a través de instrumentos electrónicos de pago.

ARTÍCULO 5.-

Es recomendable que los bancos e instituciones financieras no soliciten a los clientes, a través de sus funcionarios, empleados o terceros, sus contraseñas o claves de acceso. Asimismo, tampoco es recomendable que cuenten con procedimientos o mecanismos que les permitan conocer los valores de dichas contraseñas o claves de acceso.

ARTÍCULO 6.-

El acceso técnico a las bases de datos y archivos de los bancos e instituciones financieras, correspondientes a las operaciones bancarias y servicios proporcionados a través de instrumentos electrónicos de pago, únicamente deberá permitirse a las personas expresamente autorizadas por el banco o institución financiera correspondiente, según se establece en el artículo 10 de este Código de Autorregulación. Al otorgarse los accesos de referencia, se dejará constancia de dicha circunstancia en la bitácora que se prevé en el artículo 11 de este Código de Autorregulación y señalarse expresamente las personas autorizadas, los propósitos y el período al que se limitan los accesos.



ARTÍCULO 7.-

Los bancos e instituciones financieras deberán establecer los controles mínimos que a continuación se mencionan para la realización de operaciones monetarias que se pretendan efectuar a través de la red electrónica mundial denominada Internet o por teléfono, o bien, para la actualización de información que el propio banco o institución financiera considere sensible:

- a) Solicitar en forma adicional al uso del identificador del cliente y su respectiva contraseña o clave de acceso, un segundo factor de autenticación. Para tal efecto, podrán utilizarse generadores de claves de acceso de un solo uso, tablas aleatorias de contraseñas, registros de activos financieros, firma digital, u otro que la institución respectiva determine.
- b) Registrar previamente las cuentas destino, mismas que quedarán habilitadas después de un período determinado por el propio banco o institución financiera, de acuerdo con el servicio de que se trate y en función de los riesgos inherentes al mismo. Los bancos e instituciones financieras informarán al cliente el plazo máximo en que quedarán habilitadas dichas cuentas. Para el registro de las cuentas destino, los bancos e instituciones financieras solicitarán al cliente que se autentique nuevamente con el segundo factor de autenticación, en los términos del inciso anterior.
- c) Validar, con base en la información disponible para el banco o institución financiera correspondiente, la estructura del número de la cuenta destino o del contrato, sea que se trate de cuentas para depósito, pago de servicios, clave bancaria estandarizada, tarjetas de crédito u otros medios de pago.
- d) 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.

Se exceptúan de lo previsto en este artículo, las operaciones monetarias y demás transacciones bancarias que se realicen entre cuentas propias del cliente dentro del mismo banco o institución financiera.



ARTÍCULO 8.-

Los bancos e instituciones financieras que pongan al alcance de los clientes, en sus instalaciones o en áreas de acceso al público, equipos electrónicos o de telecomunicaciones, que permitan llevar a cabo consultas, operaciones monetarias y cualquier otro tipo de transacción bancaria, deberán adoptar medidas de seguridad que impidan la instalación en tales equipos, de dispositivos que puedan interferir con el manejo de la información de los clientes, así como que dicha información sea leída, copiada, modificada o extraída por terceros. Lo anterior, atendiendo al servicio de que se trate y en función de los riesgos inherentes al mismo.

ARTÍCULO 9.-

Es recomendable que los bancos e instituciones financieras mantengan mecanismos de control para la detección de eventos que se aparten de los parámetros de uso habitual previamente establecidos por el cliente.

Para tal efecto, en el respectivo contrato o reglamento deberá facultarse a los bancos e instituciones financieras para solicitar a los clientes la información que estimen necesaria para definir sus parámetros de referencia, así como también los medios y procedimientos por los cuales se les solicitará dicha información. Igualmente, deberá facultarse al banco o institución financiera para que, en caso de que detecte eventos que se aparten de los parámetros de uso habitual del cliente, pueda bloquear las operaciones hasta tanto pueda verificarlas con el cliente.

ARTÍCULO 10.-

Los bancos e instituciones financieras deberán acordar con sus clientes, los mecanismos y medios para notificarles, a la brevedad posible, sobre:

- a) El registro de cuentas a que se refiere el artículo 7 inciso b) de este Código de Autorregulación.
- b) Los cambios o modificaciones a los límites de monto para operaciones monetarias con terceros, definidos por el cliente en los términos de lo establecido en el artículo 7 inciso d) de este Código de Autorregulación.
- c) Medios y procedimientos mediante los cuales se les solicitará y actualizará la información pertinente, para determinar los parámetros de uso habitual de cada cliente.



ARTÍCULO 11.-

Los bancos e instituciones financieras deberán contar con bitácoras en las que se registre, cuando menos, la información siguiente:

- a) Los accesos a los instrumentos electrónicos de pago, tanto de los clientes como de las personas expresamente autorizadas por el banco o institución financiera correspondiente.
- b) La fecha, hora exacta, número de cuenta origen y destino y demás información que permita identificar el mayor número de elementos involucrados en los accesos a los instrumentos electrónicos de pago.
- c) Tratándose de servicios y operaciones a través de la red electrónica mundial denominada Internet, adicionalmente, los datos de las consultas y operaciones incluyendo, en su caso, las direcciones de los protocolos de Internet o similares.

La información a que se refiere el presente artículo deberá ser proporcionada a los clientes que así lo requieran expresamente al banco o institución financiera correspondiente, en un plazo que no exceda de diez días hábiles, de acuerdo con los procedimientos que establezca cada banco o institución financiera y de conformidad con el ordenamiento jurídico vigente.

Dichas 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.

Es recomendable que los bancos e instituciones financieras mantengan las bitácoras a que se refiere este artículo hasta por un plazo de diez años.

Los registros de la bitácora podrán ser utilizados como prueba en caso de que se verifique una anomalía en una transacción electrónica.

ARTÍCULO 12.-

Los bancos e instituciones financieras deberán contar con áreas de soporte técnico y operacional integradas por personal capacitado, que se encargará de atender y dar seguimiento a las incidencias que tengan los clientes de los instrumentos electrónicos de pago, así como de procurar la operación continua de la infraestructura informática del banco y la institución financiera correspondiente y de hacer su mejor esfuerzo para dar un solución expedita para restaurar el servicio, en caso de presentarse algún incidente. Lo anterior será implementado por cada banco e institución financiera según sus propias políticas internas.