ACUERDO No. 006-2011[1]
(de 6 de diciembre de 2011)

"Por medio del cual se establecen lineamientos sobre banca electrónica y la gestión de riesgos relacionados"

LA JUNTA DIRECTIVA
En uso de sus facultades legales, y

CONSIDERANDO

Que a raíz de la emisión del Decreto Ley 2 de 22 de febrero de 2008, el Órgano Ejecutivo elaboró una ordenación sistemática en forma de texto único del Decreto Ley 9 de 1998 y todas sus modificaciones, la cual fue aprobada mediante el Decreto Ejecutivo No. 52 de 30 de abril de 2008, en adelante la Ley Bancaria;

Que son objetivos de la Superintendencia de Bancos velar porque se mantenga la solidez y eficiencia del sistema bancario y fomentar las condiciones propicias para el desarrollo de Panamá como centro financiero internacional, según dispone el artículo 5 de la Ley Bancaria;

Que de conformidad a lo establecido en el numeral 3 del Artículo 5 de la Ley Bancaria, son objetivos de la Superintendencia promover la confianza pública en el sistema bancario;

Que de conformidad a lo establecido en el Artículo 54 de la Ley Bancaria, los bancos contarán con políticas, normas y procedimientos para asegurar que sus operaciones puntuales se puedan mantener o recuperar de forma oportuna en el evento de cualquier interrupción significativa que afecte su operatividad, con el propósito de minimizar las consecuencias que puedan surgir de dicha interrupción;

Que la constante aparición de nuevas tecnologías y la transformación de las ya existentes conllevan numerosos riesgos que requieren la actualización del marco normativo vigente para la prestación de servicios por medio de la banca electrónica, a fin de que sus operaciones se lleven a cabo de una forma más segura, transparente confiable y eficiente.

Que de conformidad a lo establecido en el Artículo 11 de la Ley Bancaria, son atribuciones de carácter técnico de la Junta Directiva, fijar en el ámbito administrativo, la interpretación y el alcance de las disposiciones legales o reglamentarias en materia bancaria;

Que en sesiones de trabajo de esta Junta Directiva, se ha puesto de manifiesto la necesidad y conveniencia de actualizar los parámetros y lineamientos para la prestación del servicio de banca electrónica a fin de fortalecer la gestión de los riesgos a los que se encuentran expuestas las operaciones llevadas a cabo por medios o canales electrónicos:

ACUERDA:

ARTÍCULO 1: **ÁMBITO DE APLICACIÓN.** Las disposiciones del presente Acuerdo se aplicarán a los bancos oficiales, a los bancos de licencia general y a los bancos de licencia internacional que presten servicios o faciliten productos a sus clientes a través de banca electrónica.

ARTÍCULO 2: **DEFINICIONES.** Para los efectos del presente Acuerdo, los siguientes conceptos se entenderán así:

1. **Banca electrónica**: Es la prestación de servicios bancarios a través de medios o canales electrónicos. La banca electrónica involucra los servicios ofrecidos por: banca por internet, banca móvil, banca por teléfono, terminales de puntos de venta(POS), mensajería instantánea (chat), redes sociales, correo electrónico, firma electrónica, dinero electrónico, red ACH, redes especializadas, cajeros automáticos, monedero o

[1] Deroga el Acuerdo No. 5-2003 de 12 de junio de 2003. Modificado por el Acuerdo No. 9-2014 de 23 de septiembre de 2014, por el Acuerdo No. 5-2021 de 23 de noviembre de 2021 y por el Acuerdo No. 2-2022 de 22 de marzo de 2022.

pago móvil, tarjeta bancaria con circuito integrado, medios de pago electrónico o cualquier otro medio o canal electrónico.

2. **Dispositivo tecnológico de acceso**: Elemento o componente, ya sea de hardware y/o software, que permita a un cliente bancario acceder a los servicios de banca electrónica.

3. **Medios o canales electrónicos**: Dispositivo tecnológico de acceso, medios de transporte de datos, sistemas de almacenamiento o cualquier otra tecnología actual y futura, que sea empleada para consultar, ingresar, transportar, proteger, procesar y/o almacenar datos de clientes y sus transacciones bancarias.

4. **Banca por Internet**: Servicios de banca electrónica suministrados a clientes a través de internet, en el sitio que corresponda a uno o más dominios del banco, mediante protocolos HTTP (Hypertext Transfer Protocol), HTTPS (HypertextTransfer Protocol Secure), o protocolos con propósitos equivalentes, indistinto del dispositivo tecnológico de acceso**.**

5. **Banca móvil:** Servicios de banca electrónica provistos a clientes a través de un teléfono móvil, cuyo número de línea se encuentre afiliado al servicio, mediante protocolos SMS (Short Message Service), WAP (Wireless Access Protocol) o protocolos con propósitos equivalentes.

6. **Banca por teléfono**: Servicio de banca electrónica mediante el cual, el cliente envía instrucciones al banco a través de un sistema telefónico, fijo o móvil, por medio de tonos, pulsos o mecanismos de reconocimiento de voz, y recibe respuesta grabada o interactiva de voz.

7. **Banca telefónica voz a voz**: Servicio de banca electrónica mediante el cual el cliente provee instrucciones a través de un sistema telefónico, fijo o móvil, al banco por intermedio de un representante autorizado por la institución, ubicado en un centro de llamadas.

8. **Terminal de puntos de venta**: Dispositivos tecnológicos de acceso, que permiten proveer servicios de banca electrónica, tales como datáfonos, terminales electrónicas micro-computarizadas, teléfonos móviles y programas de cómputo, que pueden ser operados por individuos o comercios para debitar o acreditar cuentas bancarias, o bien para hacer cargos a tarjetas.

9. **Mensajería instantánea:** Medio o canal tecnológico de acceso, mediante el cual el cliente contacta por internet o similar y en tiempo real a un banco y consulta o provee información por intermedio de un representante autorizado de la institución.

10. **Redes Sociales:** Medio o canal tecnológico de acceso, mediante el cual el cliente interactúa con un banco por internet o similar, y consulta o provee información por intermedio de un representante autorizado de la institución, sea o no en tiempo real.

11. **Correo electrónico:** Medio o canal tecnológico de acceso, mediante el cual el cliente intercambia información con un banco por internet, y consulta o provee información por intermedio de un representante autorizado de la institución.

12. **Dinero electrónico**: Valor monetario en una cuenta bancaria u otro producto bancario accedido por medio de dispositivos electrónicos, para la ejecución de pagos por medio de terminales en los puntos de venta, transferencia directa entre dos dispositivos o mediante redes abiertas de computación.

13. **Cajero automático**: Dispositivo tecnológico de acceso que provee servicios de banca electrónica, al cual se accede mediante el uso de una tarjeta y/o procedimientos de autenticación.

14. **Pago o monedero móvil**: Servicio de banca electrónica en el cual el dispositivo tecnológico de acceso consiste en un dispositivo electrónico o un teléfono móvil del cliente, cuya línea telefónica se encuentra asociada al servicio.

15. **Tarjeta bancaria**: Dispositivo tecnológico de acceso utilizado como medio de pago (tarjetas de crédito, débito, prepagadas y otras).

16. **Tarjeta bancaria con circuito integrado**: Tarjeta bancaria que cuenta con un circuito integrado o chip, y que puede almacenar información del tarjeta habiente con el fin de verificar, mediante procedimientos criptográficos, que la tarjeta y el punto de venta donde se utilizan son válidos, antes de ejecutar servicios de banca electrónica.

17. **Redes especializadas:** Sistemas de transferencias de información y/o fondos, local o internacional, entre instituciones financieras y cualquier otra entidad que contenga información de clientes. Esta definición incluye entre otras el sistema conocido como SWIFT.

18. **Factores de autenticación**: Mecanismo de autenticación basado en información o dispositivos que sólo el cliente conozca y posea o basados en sus atributos físicos, los cuales contienen las siguientes categorías**:**

    a. **Factor de categoría 1**: Información que sólo el cliente conoce, tales como número de identificación personal, contraseña o datos personales proporcionados voluntariamente por el cliente, a través de canales de información y/o electrónicos seguros.
    b. **Factor de categoría 2**: Información que sólo el cliente tiene, tales como generadores de contraseñas de un solo uso (tokens), teléfono móvil o tarjetas bancarias con circuito integrado u otras tecnologías de seguridad que vayan surgiendo.
    c. **Factor de categoría 3**: Información biométrica, tales como huellas digitales, geometría de la mano, características del iris del ojo, etc.

ARTÍCULO 3: **AUTORIZACION PREVIA Y CONTROL DE LA SUPERINTENDENCIA.** Todo banco podrá llevar a cabo cualquier servicio de banca electrónica en o desde la República de Panamá, siempre que haya obtenido previamente la debida autorización de la Superintendencia de Bancos para cada canal electrónico que desee implementar. Para tal efecto, el banco deberá suministrar a la Superintendencia de Bancos información completa donde conste la implementación y mantenimiento de las estructuras y medidas mencionadas en el presente Acuerdo.

Adicionalmente, el banco deberá solicitar autorización a esta Superintendencia de Bancos para incorporar nuevos servicios al canal electrónico previamente autorizado, según lo dispuesto en el párrafo anterior. Cuando el banco incorpore servicios de la misma naturaleza y estructura de los previamente aprobados, se requerirá una notificación a esta Superintendencia.
Previo a la autorización del servicio, la Superintendencia realizará las inspecciones que estime conveniente para la verificación, evaluación y revisión de la información suministrada y el respectivo cumplimiento de las disposiciones de este Acuerdo.

Los cajeros automáticos, los puntos de venta (POS) y en general, los dispositivos tecnológicos de acceso que se vayan adicionando a la red del banco, siempre que estos suministren los mismos servicios previamente autorizados desde los mismos canales electrónicos autorizados por esta Superintendencia, no requerirán de la autorización a que se refiere este artículo. Sin perjuicio de lo anterior, el banco deberá notificar a esta Superintendencia, previo a la instalación de dichos equipos, informando sobre las medidas de seguridad que se implementarán en estos canales.

ARTÍCULO 4: **RESPONSABILIDADES DE LA JUNTA DIRECTIVA Y DE LA ALTA GERENCIA DEL BANCO.** La junta directiva y la alta gerencia del banco serán responsables de establecer e implementar un sistema efectivo de gestión de riesgos asociados específicamente a las actividades de banca electrónica, el cual deberá incluir como mínimo:

1. El establecimiento de responsabilidades específicas, políticas y controles para el análisis y la gestión permanente de dichos riesgos, incluyendo la conformación de la Unidad Responsable y la gestión por medio del Comité de Riesgos.

2. La revisión y aprobación de los aspectos esenciales del proceso de control de riesgos y de seguridad de los canales electrónicos del banco;

3. El establecimiento de un proceso íntegro y continuo de debida diligencia y supervisión para el manejo de sus relaciones con proveedores de servicios externos y sujeciones a terceros en general que asistan o complementen la banca electrónica.

ARTÍCULO 5: **ESTRUCTURA ADECUADA DE LA BANCA ELECTRÓNICA.** La junta directiva o gerencia superior de cada banco debe asegurarse de integrar al manual de operaciones de la institución, los procedimientos, políticas y controles internos necesarios a fin de mantener una estructura administrativa y operativa para ofrecer el servicio de banca electrónica, que incluya especialmente lo siguiente:

1. Naturaleza de las transacciones y operaciones bancarias ofrecidas.
2. Sistema de registro de las transacciones y operaciones.
3. Mecanismos efectivos para la supervisión de los riesgos asociados con las actividades de banca electrónica (como por ejemplo, riesgo operacional, tecnológico, de seguridad, etc.) que incluyan, por lo menos, el establecimiento de políticas y controles para administrar tales riesgos.
4. Mecanismos efectivos para la evaluación de las amenazas, vulnerabilidades e impactos derivados de los archivos de información que conforman los procesos asociados a la banca electrónica.
5. Mecanismos efectivos para la gestión de los incidentes que atenten contra la seguridad de la banca electrónica y su retroalimentación a la gestión de riesgos.
6. Políticas y procedimientos que sean aplicables en caso de amenazas potenciales de seguridad interna y externa a la banca electrónica, tanto para prevención como para respuesta.
7. Políticas y procedimientos que sean aplicables en caso de violaciones a la seguridad interna y externa a la banca electrónica, incluyendo las acciones a tomar.
8. Políticas y procedimientos que incluyan mecanismos de seguridad que incluyan planes de continuidad del servicio y de recuperación ante desastres.
9. Mecanismos de diligencia debida y vigilancia de las relaciones de tercerización que guarden relación con el servicio de banca electrónica.

ARTÍCULO 6: **PLANIFICACIÓN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES.** La unidad de riesgo o instancia responsable existente en cada banco, deberá tener entre sus funciones el desarrollo de un plan integral tanto de continuidad del negocio así como de recuperación ante desastres.

Se entiende como plan de continuidad del negocio aquella metodología operativa interdisciplinaria, compuesta por diversos planes de respuesta ante contingencias o incidentes de seguridad, que le permita al banco restaurar inmediatamente las funciones críticas del negocio que hayan sido, parcial o totalmente, afectadas como resultado de un ataque, sabotaje o desastre natural.

Se entiende como el plan de recuperación ante desastres el proceso de recuperación respecto de los datos, enlaces de comunicación, el hardware y el software críticos, que eventualmente hayan sufrido un incidente de seguridad o disponibilidad, para reanudar el normal funcionamiento del banco y la prestación de sus servicios.

ARTÍCULO 7: **UNIDADES RESPONSABLES.** La unidad de riesgo o instancia responsable existente en cada banco, deberá tener entre sus funciones la identificación, evaluación y control de los riesgos tecnológicos, incluyendo los riesgos asociados al servicio de banca electrónica.

Para la gestión diaria de la seguridad de la información, todo banco deberá tener dentro de su estructura organizacional una unidad de seguridad de la información, que reporte a un funcionario de jerarquía e independencia.

Por razones de su estructura organizativa, un banco podrá solicitar al Superintendente dispensas para el cumplimiento de lo establecido en el párrafo anterior, siempre que éste evidencie a satisfacción de la Superintendencia que la gestión de la seguridad de la información es llevada a cabo eficientemente ya sea por su casa matriz o un tercero proveedor de seguridad.

ARTÍCULO 8: **AUDITORIA INTERNA.** En materia de auditoría interna, serán responsabilidades del banco:

1. Velar porque se realicen auditorias periódicas de acuerdo al volumen y complejidad de las operaciones que realicen, asegurándose de incorporar dichas auditorías en suplan anual de auditoría, y
2. Contar con los programas necesarios y personal especializado en el área respectiva.

ARTÍCULO 9: REVISIONES EXTERNAS. El banco deberá asegurarse de realizar revisiones externas de riesgo, con personal o empresas debidamente calificadas, para los canales de banca electrónica y de los medios de pago electrónicos.

ARTÍCULO 10. PRUEBAS DE INTRUSIÓN Y VULNERABILIDAD. Con la finalidad de minimizar el acceso no autorizado a sus sistemas todo banco deberá ejecutar al menos las siguientes pruebas de intrusión y vulnerabilidad realizadas por profesionales idóneos externos al banco:

1. **Prueba de Intrusión Externa (**En inglés conocidas como **"External Security Penetration Test")**: Esta prueba deberá realizarse como mínimo una vez al año y deberá tener el siguiente alcance:

    a. Dispositivos de seguridad y su funcionamiento ante ataques.
    b. Vulnerabilidades en las aplicaciones web y banca por internet.
    c. Evaluación de los sistemas de detección de intrusos.
    d. Servicios expuestos hacia las redes públicas.
    e. Estructura de red.
    f. Fallas en los sistemas de autenticación y políticas de contraseñas.
    g. Ingeniería social interna.

2. **Prueba de Intrusión Interna (**En inglés conocido como **"Internal Security Penetration Test"):** Esta prueba deberá realizarse por lo menos cada dos (2) años y deberá tener los siguientes alcances:

    a. Análisis de la arquitectura de red y su topología.
    b. Identificación de los componentes críticos de tecnología de la información.
    c. Identificación de vulnerabilidades y áreas a proteger.
    d. Gestión de riesgos, incidentes, redes y sistemas.
    e. Seguridad física y lógica.
    f. Gestión ante incidencias.

PARÁGRAFO. Sin perjuicio de lo dispuesto en el presente artículo, el banco deberá realizar, con personal propio e idóneo, pruebas regulares de intrusión y vulnerabilidad.

ARTÍCULO 11: **GESTIÓN INTEGRAL DE LOS RIESGOS ASOCIADOS A LA BANCA ELECTRÓNICA.** Todo banco, dentro de su proceso de gestión integral de riesgos, deberá contemplar los riesgos asociados a la prestación de servicios y productos a través de banca electrónica, prestando especial atención al manejo de los riesgos operativo, legal y de reputación, en los siguientes aspectos:

1. Asegurarse que la información suministrada o publicada en sus sitios en internet o por medio de cualquier canal electrónico sea adecuada y permita a sus clientes realizar una identificación correcta y adecuada del banco.
2. Asegurarse que la información suministrada o publicada sobre las características delos servicios de la banca electrónica y de las medidas preventivas mínimas que debe llevar a cabo el cliente, sea correcta y actualizada.

3. Establecer medidas técnicas y procedimientos que aseguren la observancia de las condiciones de privacidad aplicables a los clientes y la seguridad de sus operaciones.
4. Adoptar medidas de privacidad aplicables de acuerdo a las jurisdicciones donde el banco suministra los productos y servicios por cualquier canal de banca electrónica.
5. Establecer programas que garanticen la capacidad efectiva y continuidad de negocios, que contribuyan a asegurar la disponibilidad de los sistemas y servicios de banca electrónica.
6. Desarrollar planes de respuesta y comunicación de incidentes, para gestionar, detener y mitigar problemas que surjan de eventos imprevistos, incluyendo ataques internos y/o externos, que puedan dificultar el suministro de sistemas y servicios de banca electrónica.
7. Establecer sistemas para la administración de los casos de fraude relacionados con los servicios de banca electrónica, incluyendo una solución integral de monitoreo de comportamiento transaccional del cliente que contenga los mecanismos de identificación, alertas tempranas, acciones de mitigación y seguimiento investigativo de cada caso.

ARTÍCULO 12: **REGISTRO DE ACCESOS A LA BANCA ELECTRÓNICA.** El banco que ofrezca servicios de banca electrónica, establecerá y mantendrá las bitácoras necesarias, protegidas de manipulación o alteración arbitraria, que permitan llevar una clara pista de auditoría, con la fecha y hora sincronizada con el tiempo universal coordinado.

Las bitácoras incluirán un registro de acceso y de uso del sistema, registrando las transacciones y operaciones realizadas por los clientes, las que el banco mantendrá a disposición de la Superintendencia y conservará por cualquier medio autorizado por Ley, por un periodo de tiempo no inferior a un (1) año, contado a partir de la fecha de la transacción. Las bitácoras deberán contener, como mínimo, la siguiente información:

1. El registro de acceso a los canales electrónicos, incluyendo el identificador del cliente, fecha y hora.
2. Detalle de las operaciones monetarias realizadas, tales como fecha, hora, canal tecnológico de acceso, monto, cuenta origen y cuenta destino y el tipo de transacción (débito / crédito).
3. Datos que permitan realizar investigaciones, a los efectos de facilitar la identificación del origen de cualquier fraude o bien su intento, sobre medios y/o canales electrónicos.
4. En el caso de banca por internet, se requiere almacenamiento de las bitácoras generadas en el servidor web (webserver), los cuales deberán contener, como mínimo, el método de registro (GET/POST/HEAD), el Identificador Uniforme de Recurso y sus parámetros (Uniform Resource Indentifer–URI), la hora y fecha (timestamp).

El banco deberá asegurarse que los servicios de banca electrónica suministrados por terceros cumplen con los requerimientos de bitácoras establecidos en los numerales anteriores y que tanto el banco como la Superintendencia tendrán acceso a los mismos encaso de ser necesario.

ARTICULO 13: REGISTRO DE TRANSACCIONES DE BANCA ELECTRONICA. El banco deberá llevar un registro de transacciones de sus clientes tal y como lo dispone el Código de Comercio.

ARTÍCULO 14: **INFORMACIÓN Y CONTRATO DE BANCA ELECTRONICA.** El banco está obligado a informar al cliente de banca electrónica sobre las características, condiciones, posibles costos y cualquier otra estipulación determinante que conlleve el uso del servicio de banca electrónica. Esta descripción deberá ser específica e individual para cada medio o canal electrónico.

Para tal propósito, el banco debe informar para cada medio o canal electrónico e incluir en su contrato de banca electrónica, en lo que aplique, las disposiciones contenidas en el Artículo 196 de la Ley Bancaria; asegurándose que el cliente conozca el costo por la prestación del servicio a través del canal electrónico.

Igualmente será necesaria la constancia de la aceptación del cliente de los términos y condiciones contractuales aplicables a cada servicio de banca electrónica.

ARTÍCULO 15: **CONTROLES DE SEGURIDAD.** El banco debe asegurar al brindar los servicios de banca electrónica, la autenticidad, integridad, confidencialidad y el no rechazo de una transacción válida una vez aceptada, al igual que la segregación de responsabilidades y controles de autorización. Para tal propósito se debe contar con, al menos, lo siguiente:

1. **Infraestructura Tecnológica**
   A nivel de infraestructura tecnológica, todo banco deberá contar al menos con las siguientes soluciones de seguridad:

Medida	Descripción
Implementación de ZONAS seguras mediante Firewall.	Toda entidad deberá contar con una Zona Desmilitarizada (DMZ) que aísle los servicios públicos de la red interna de la organización.
Servidor de Logs.	Deberá existir un servidor que se ocupe de almacenar los LOGS que genere el firewall (dirección IP, timestamp, evento).
Se requiere la implementación de un sistema de detección de intrusos con capacidad de trabajar en forma activa (IPS) o pasiva (IDS).	Debe existir un Sistema de Detección de Intrusos que se encuentre analizando el tráfico de las redes públicas de la entidad, delante de la Zona Desmilitarizada (DMZ) sobre los servicios publicados hacia Internet. Los logs generados por el sistema deberán ser almacenados por un (1) año. La solución deberá ser capaz de generar, estadísticas y resúmenes que podrán ser solicitados por la Superintendencia de Bancos de Panamá.

2. **Banca por Internet y Banca Móvil** [2]
   A nivel de banca por internet y banca móvil, todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

   a. Autenticación del banco. Para que el cliente reconozca al banco será necesario contar con al menos las siguientes medidas:
      a.1. Método digital que le permita al cliente identificar que es el banco al cual corresponde; como certificados digitales, imágenes preseleccionadas por el cliente o equivalentes, antes de que el mismo ingrese su contraseña.
      a.2. Inmediatamente luego del ingreso debe presentarse el nombre completo del cliente y su última fecha de ingreso al servicio, para la verificación por el mismo.
   b. Autenticación del cliente. Para el acceso a este servicio será necesario contar con las medidas de autenticación siguientes:
      b.1. Factor de autenticación de categoría 1, el cual deberá cumplir con los siguientes parámetros: debe ser en primera instancia por el banco y luego de posible modificación por el mismo cliente y que contenga como mínimo ocho (8) caracteres alfanuméricos.
      b.2. Factor de autenticación de categoría 2, el cual deberá cumplir con los siguientes parámetros: implementación de una capa de "validación dinámica" o tecnología y procesos similares que ofrezcan al menos el mismo nivel de seguridad. Este factor será aplicable cuando se trate de transacciones realizadas por el cliente a un tercero ya sea dentro de la misma entidad bancaria o en otra entidad bancaria.

[2] Modificado por el artículo 1 del Acuerdo No. 5-2021 de 23 de noviembre de 2021 y por el artículo 1 del Acuerdo No. 2-2022 de 22 de marzo de 2022.

En caso de tratarse de la validación dinámica, el banco deberá contar con un sistema de generación de PIN automatizado con un mínimo de seis (6) dígitos en la generación de los mismos.

El factor de autenticación de categoría 2 podrá ser realizado tanto por dispositivos de hardware como por soluciones de software portables en dispositivos móviles. Este factor será de cumplimiento obligatorio para la realización de transacciones bancarias, y opcional para las consultas que realice un cliente a través de estos canales.

PARÁGRAFO 1. Para los efectos de lo establecido en el literal b.2., inciso b., numeral 2 del artículo 15 del presente Acuerdo, las entidades bancarias deberán asegurarse que para el proceso de activación del componente de seguridad (soft token) se realice un proceso seguro de autenticación del cliente, para lo cual el banco deberá asegurarse de utilizar los mecanismos de autenticación más seguros, como por ejemplo, el hard token (factor de categoría 2), o el factor de categoría 3 y sus derivados con el nivel de certeza más alto, o pruebas de vida u otros que vayan surgiendo.

Igualmente, para los clientes activos de banca por internet y banca móvil, el banco deberá asegurarse que cualquier cambio vinculado con la información del cliente, como por ejemplo cambios del número del teléfono, correo electrónico, dirección u otros datos sensitivos, contemple en su proceso el factor de autenticación de categoría 2 o categoría 3.

Las entidades bancarias contarán con un plazo hasta el 30 de junio de 2022 para el cumplimiento de las disposiciones establecidas en el presente parágrafo.

PARÁGRAFO 2. El banco que a partir de la entrada en vigor del presente Acuerdo solicite autorización para la implementación de nuevos canales electrónicos o para la adición de nuevos servicios a un canal previamente autorizado, en cumplimiento de lo dispuesto en el artículo 3 del presente Acuerdo, deberá cumplir con los requerimientos establecidos en el parágrafo 1 del presente numeral, como parte de una buena gestión de los riesgos de los canales electrónicos.

No obstante lo anterior, hasta el 30 de junio de 2022 la Superintendencia podrá aprobar la utilización de un canal o la adición de nuevos servicios a un canal previamente autorizado, sin embargo, en estos casos el banco deberá asumir los riesgos y costos por las transacciones no reconocidas por sus clientes, como consecuencia de la activación del doble factor de autenticación sin las medidas de seguridad previstas en el parágrafo 1 del presente numeral.

3. **Pago móvil**:
A nivel de pago móvil, todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

Se debe identificar al cliente por el número de línea del teléfono móvil, el cual debe ser obtenido automática e inequívocamente por el banco.

a. El factor de autenticación categoría 1, deberá contener como mínimo cuatro (4) caracteres.
b. Proveer lo necesario para impedir la lectura en pantalla del dispositivo de acceso de la información de identificación y autenticación proporcionada por el cliente.
c. Implementar controles compensatorios para proteger la transmisión de la información sensible del cliente.

4. Cajeros automáticos y tarjetas de circuito integrado: [3]
A nivel de cajeros automáticos, todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

a. Identificar al cliente a través del número de la tarjeta bancaria.
b. Factor de autenticación categoría uno (1) cuya contraseña o número de identificación personal contenga como mínimo cuatro (4) dígitos y adicionalmente la tarjeta bancaria con circuito integrado.

[3] Modificado por el artículo 1 del Acuerdo No. 9-2014 de 23 de septiembre de 2014.

c. Si el servicio de cajero automático se ofrece mediante tarjetas sin circuito integrado, los bancos deberán asumir los riesgos y costos de las operaciones no reconocidas por los clientes, mientras que el saldo de dichas operaciones deberá ser abonado al cliente en un plazo de setenta y dos (72) horas posteriores a la reclamación, siempre que se trate de operaciones realizadas por clientes de una entidad bancaria en cajeros automáticos de esa misma entidad bancaria.

   Igualmente, cuando se trate de operaciones realizadas por un cliente, en cajeros automáticos de otra entidad bancaria de la plaza, el banco que recibe el reclamo deberá abonar al cliente el saldo de dichas operaciones en un plazo de diez (10) días posteriores a la reclamación.

   Todo banco establecido en la plaza panameña, deberá contar con tarjetas de circuito integrado en un plazo de treinta y seis (36) meses, contados a partir de la promulgación del presente Acuerdo. No obstante el banco deberá contar con un plan de trabajo e implementación en veinticuatro (24) meses a partir de la promulgación de la norma.

d. Proveer lo necesario para impedir la lectura en pantalla del dispositivo de acceso, de la información de identificación y autenticación proporcionada por el cliente.
e. Transmisión cifrada de las contraseñas, números de identificación personal u otra información sensible del cliente.
f. Cámaras de circuito cerrado de televisión (CCTV) y grabación de imágenes, cuyas grabaciones deberán ser conservadas por el banco por un período mínimo de doce (12) meses. No obstante, ante notificación de autoridad competente, el banco deberá mantener la grabación a disposición de la autoridad por el periodo que esta lo requiera.

PARÁGRAFO. Una vez transcurridos los treinta y seis (36) meses a los que se refiere el literal c del presente artículo, los bancos que aún no hayan completado el proceso de distribución de las tarjetas de circuito integrado contarán con tres (3) meses adicionales para realizar dicho proceso.

Una vez transcurridos los tres (3) meses señalados en el párrafo anterior sin haber completado el proceso de distribución de las tarjetas de circuito integrado a todos sus clientes, el banco podrá solicitar al Superintendente una dispensa para prorrogar dicho plazo, explicando detalladamente los motivos que le impiden cumplir con los plazos establecidos en el presente artículo. El Superintendente evaluará en atención al volumen de tarjetas de cada banco y a la complejidad de cada caso en particular, otorgar un plazo superior al establecido, en cuyo caso estimará el plazo que se concederá, tomando en consideración los planteamientos realizados por el banco.

No obstante, a partir del 20 de diciembre de 2014 el banco deberá asumir los riesgos y costos de las operaciones no reconocidas por los clientes que aún no tengan acceso a la tecnología de circuito integrado, siempre que no haya existido negligencia de parte del cliente.

5. <u>Terminal de punto de venta (POS)</u>:
A nivel de terminal de puntos de venta (POS), todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

a. Identificar al cliente a través del número de la tarjeta bancaria.
b. El factor de autenticación categoría 1 deberá contener como mínimo cuatro (4) dígitos cuando aplique en base al tipo de tarjeta, o la tarjeta bancaria con circuito integrado.
   En el supuesto que el servicio de terminal de punto de venta se ofrezca mediante tarjetas sin circuito integrado, los bancos deberán asumir los riesgos y costos delas operaciones no reconocidas por los clientes y el saldo de dichas operaciones deberá ser abonado al cliente en un plazo de setenta y dos (72) horas posteriores a la reclamación. El banco deberá asegurarse que las terminales de puntos de venta que son propiedad de un tercero ajeno a la entidad bancaria, cuenten con los mecanismos de seguridad requeridos en el presente acuerdo.

c. Proveer lo necesario para impedir la lectura en pantalla del dispositivo de acceso, de la información de identificación y autenticación proporcionada por el cliente.
d. Transmisión cifrada de las contraseñas, números de identificación personal u otra información sensible del cliente.
e. El dispositivo electrónico utilizado como terminal de punto de venta deberá cumplir con las medidas de seguridad establecidas para los medios de pago electrónico.

6. <u>Banca telefónica audio-respuesta</u>:
A nivel de banca telefónica audio-respuesta, todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

a. Asignar un identificador único de cliente, definido por la institución o por el propio cliente que cuente como mínimo con seis (6) caracteres.
b. Factor de autenticación categoría dos (2) cuya contraseña o número de identificación personal contenga como mínimo seis (6) dígitos. Este factor será aplicable cuando se trate de transacciones realizadas por el cliente a un tercero ya sea dentro de la misma entidad bancaria o en otra entidad bancaria.

7. <u>Banca telefónica voz a voz</u>:
A nivel de banca telefónica voz a voz, todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

a. Asignar un identificador único de cliente, definido por el banco o por el propio cliente que cuente como mínimo con seis (6) caracteres.
b. Factor de autenticación categoría uno (1) que contenga información proporcionada a través de cuestionarios en centros de atención telefónica que permita proteger la información sensible del cliente.

8. <u>Redes especializadas</u>:
A nivel de redes especializadas, todo banco deberá asegurarse de implementar, como mínimo, las siguientes medidas de seguridad:

1. Interacción de las partes:

Para servicios de banca electrónica que se brinden por redes especializadas de servicios, será necesario contar con las siguientes medidas de seguridad:

a. Ambas partes deberán emplear certificados digitales, y/o medidas similares que los identifique y valide el origen legítimo y contenido de la transacción.
b. Se deberán establecer enlaces cifrados con el más alto nivel de seguridad comercialmente disponible.
c. Se deberá contar con servidores de bastión que aíslen y protejan a los repositorios centrales de información del banco.
d. Se deberá contar con las medidas necesarias que garanticen la integridad, confiablidad y no rechazo o repudio de las transacciones.

9. <u>Mensajería instantánea, redes sociales y correos electrónicos</u>:
A nivel de mensajería instantánea, redes sociales y correos electrónicos, todo banco deberá asegurarse de suministrar información en general y cualquier otra que ha sido autorizada por un cliente del banco a través de contrato y cualquier otro medio.

ARTÍCULO 16: **OTROS CONTROLES PARA BANCA ELECTRÓNICA** .Adicionalmente a los controles establecidos en el artículo anterior, el banco deberá asegurarse de implementar los siguientes controles para la banca electrónica en general:

a. Métodos para la verificación de la identidad y autorización de nuevos clientes, así como también la autenticación de la identidad y autorización de clientes existentes que deseen iniciar transacciones a través del servicio de banca electrónica.
b. Medidas establecidas para preservar la confidencialidad e integridad de la información relevante del banco, las cuales deben estar acorde con la sensibilidad de la información transmitida y/o guardada en bases de datos.

c. Técnicas que ayuden a establecer la no renuncia o rechazo de la información recabada y asegurar la confidencialidad e integridad de transacciones de banca electrónica.
d. Proporcionar la confirmación de la ejecución de las transacciones efectuadas por el cliente a través del servicio.
e. Medidas de segregación de responsabilidades en función del control interno, de manera que se pueda reducir el riesgo de fraude en procesos y sistemas operacionales y asegurar que las transacciones estén apropiadamente autorizadas, registradas y salvaguardadas.
f. Debe existir una estructura física adecuada y con los respectivos controles, de manera que todos los sistemas, servidores, bases de datos o información física relacionada al servicio de banca electrónica este protegida y se pueda detectar cualquier acceso sin autorización.
g. Medidas apropiadas que aseguren la correcta efectividad de las transacciones a través de registros de información relacionada a la banca electrónica que puedan ser transmitidos por medio de un canal electrónico o sitio de Internet, ya sea bases de datos internas del banco o guardadas por proveedores externos al servicio del banco.
h. Asegurar la implementación de controles internos adecuados, particularmente en casos y operaciones relevantes de banca electrónica, tales como:
    h.1. La apertura, modificación o cancelación de una cuenta.
    h.2. Transacciones con consecuencias financieras.
    h.3. Autorización aprobada a un cliente para excederse del límite.
    h.4. Aprobación, modificación o revocación de derechos o privilegios para acceder al sistema.
i. Planes apropiados de respuesta a incidentes de seguridad o disponibilidad de la información que incluyan estrategias de comunicación que aseguren la continuidad del servicio y responsabilidad limitada asociada con interrupciones del servicio de banca electrónica incluyendo aquellos originados desde sistemas externos, las cuales permitan una retroalimentación sobre el sistema de gestión de riesgos a fin de trabajar sobre la mejora continua respecto a la efectividad delos controles aplicados, y la consiguiente minimización del riesgo asumido.
j. Políticas adecuadas que aseguren una debida asignación de responsabilidades por motivo de irregularidades en la ejecución del servicio de banca electrónica por terceras dependencias que hayan sido contratadas para la implementación y ejecución de dicho servicio, a través de acuerdos de calidad de servicio donde se indiquen claramente los controles de seguridad que deben ser implementados por las terceras dependencias.
k. Rastros de auditoría claros para todas las transacciones bancarias electrónicas.

ARTÍCULO 17: REPORTE DE INCIDENTES DE SEGURIDAD. El banco deberá reportar a la Superintendencia de Bancos cualquier evento o intento de fraude de los servicios de banca electrónica, mediante formulario provisto para tal fin. Este reporte debe ser enviado dentro del plazo que establezca la Superintendencia, inclusive si aún no ha sido determinado su origen, informando entre otros: fecha y hora del mismo, tipología, medio o canal electrónico afectado, cantidad de clientes afectados, monto estimado y demás aspectos que se señalen en el respectivo formulario.

ARTÍCULO 18: LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN DELCLIENTE. El banco empleará técnicas de control apropiadas, tales como criptografía, protocolos específicos u otros controles para garantizar la privacidad y confidencialidad dela información del cliente.

El banco debe establecer las medidas apropiadas para informar a los clientes del servicio de banca electrónica sobre el manejo de la seguridad y privacidad de la información recabada.
Para tal propósito se deben aplicar, al menos, las medidas siguientes:

a. Informar a los clientes, en forma clara, la política de privacidad del banco para cada servicio de banca electrónica, donde aplique.
b. Instruir y mantener informados a los clientes, sobre la necesidad de proteger su clave secreta, número de identificación personal y cualquier información bancaria y personal.
c. En los casos de banca electrónica por internet, en el momento en que el cliente haya introducido su clave, código o contraseña y se encuentre en el “canal seguro” no se

podrá re-direccionar la sesión del usuario a sitios ajenos a la transacción y/o consulta, sin antes informar al cliente que está saliendo del sitio del banco.

ARTÍCULO 19: RELACIÓN CON TERCEROS Y PROVEEDORES DE SEGURIDAD DEL SERVICIO DE BANCA ELECTRÓNICA. Cuando el banco contrate los servicios de proveedores o terceros para que ejecuten procesos de los servicios de banca electrónica, se requerirá obtener la autorización previa de esta Superintendencia de Bancos, de conformidad con lo establecido en el Acuerdo sobre Tercerización emitido por esta Superintendencia. En caso tal de que se trate de un proveedor de seguridad, el mismo debe contar con personal idóneo para el manejo de los servicios contratados.

Adicionalmente, los proveedores de seguridad de la información, deben dividirse según las siguientes categorías:

a. Análisis, planificación e implementaciones de sistemas de gestión de seguridad dela información y/o soluciones de monitoreo lógico y gestión de la seguridad de la información.
b. Auditoría y certificadoras.

Para los servicios señalados en el literal "a", el proveedor que preste dicho servicio no podrá ser el mismo que ejecute lo establecido en el literal "b" del presente artículo.

ARTÍCULO 20: REMISIÓN DE INFORMACIÓN. Los bancos sujetos a este Acuerdo deberán remitir a la Superintendencia toda la información y reportes relacionados con los servicios de banca electrónica que sean requeridos por la Superintendencia en la forma, periodicidad y contenido que ésta establezca.

ARTÍCULO 21: **PREVENCIÓN DEL USO INDEBIDO DE LA BANCA ELECTRÓNICA.** El banco, para prevenir el uso indebido de los servicios bancarios a través de la banca electrónica, debe asegurar la existencia y funcionamiento de procedimientos y medidas eficaces de seguridad para la identificación y seguimiento de transacciones sospechosas.

En adición a lo anterior, el banco debe aplicar la política de conozca a su cliente, los procedimientos de debida diligencia y aquellas disposiciones legales y reglamentarias referentes a la prevención del uso indebido de los servicios bancarios y fiduciarios.

ARTÍCULO 22: SANCIONES POR INCUMPLIMIENTO DEL ACUERDO. El incumplimiento de las disposiciones contenidas en el presente Acuerdo será sancionado por el Superintendente con arreglo a lo dispuesto en el Título IV de la Ley Bancaria.

ARTÍCULO 23: DEROGATORIA. Con la entrada en vigencia del presente Acuerdo, se deroga en todas sus partes, el Acuerdo No. 5-2003 de 12 de junio de 2003.

ARTÍCULO 24. [4] **VIGENCIA**. El presente Acuerdo comenzará a regir el diez (10) de septiembre de dos mil doce (2012). No obstante lo anterior:

a. El numeral 7 del artículo 11 empezará a regir veinticuatro (24) meses posteriores a la promulgación del presente Acuerdo. Sin embargo, dentro de los nueve (9) meses siguientes a la entrada en vigencia del presente Acuerdo, todo banco deberá presentar un plan de acción para la implementación de este numeral.
b. Las disposiciones establecidas en los numerales 2, 4 y 5 del artículo 15, tendrán un plazo de adecuación de (24) meses contados a partir de la promulgación del presente Acuerdo y bajo las condiciones y excepciones que señalan los citados numerales.
c. Todo banco deberá contar con la tecnología de circuito integrado en un plazo de treinta y seis (36) meses, contados a partir de la promulgación del presente Acuerdo. Una vez transcurrido el plazo antes señalado, el banco podrá acogerse a un plazo adicional de tres (3) meses, es decir hasta el 20 de marzo de 2015.

Dado en la ciudad de Panamá, a los seis (6) días del mes de diciembre de dos mil once (2011).

---

[4] Modificado por el artículo 2 del Acuerdo No. 9-2014 de 23 de septiembre de 2014.