República Bolivariana de Venezuela
Superintendencia de Bancos y Otras Instituciones Financieras
RIF: G-20007161-3

BICENTENARIO

RESOLUCIÓN

NÚMERO: 641.10 **FECHA:** 23 DIC 2010

Visto que el artículo 117 de la Constitución de la República Bolivariana de Venezuela consagra, entre otros aspectos, que todas las personas tendrán derecho a disponer de bienes y servicios de calidad; así como, a una información adecuada y no engañosa sobre el contenido y características de los productos y servicios que consumen.

Visto que este Ente Regulador, debe velar por un desarrollo armónico y ordenado de la red de distribución de los servicios bancarios a los fines que éstos cubran racionalmente las expectativas de crecimiento de la demanda de tales servicios.

Visto la necesidad de fomentar el uso de los servicios ofrecidos a través de la Banca Electrónica por parte de los clientes y/o usuarios de las Instituciones Financieras, de una forma segura, económica y rápida.

Visto que esta Superintendencia tiene la obligación de instruir a los Bancos y demás Instituciones Financieras, mecanismos y controles de seguridad asociados a la plataforma tecnológica para proteger a sus clientes y/o usuarios contra los fraudes electrónicos.

Visto que la Banca Electrónica constituye un canal efectivo para lograr un mayor nivel de bancarización y brindar servicios bancarios a todas las localidades del país.

Visto que el artículo 43 de la Ley General de Bancos y Otras Instituciones Financieras establece que los Bancos, Entidades de Ahorro y Préstamo y demás Instituciones deben mantener sistemas de seguridad adecuados a fin de evitar la comisión de delitos que afecten los depósitos del público; así como brindar atención y oportuna respuesta, tanto a los clientes como a los depositantes que denuncien cargos no reconocidos u omisiones presentadas en sus cuentas.

Visto que en el numeral 9 del artículo 235 de la Ley General de Bancos y Otras Instituciones Financieras, confiere a este Organismo la atribución de promulgar todas aquellas normativas prudenciales y preventivas necesarias para la seguridad del Sistema Bancario Nacional y la protección de los usuarios de los servicios bancarios.

Visto lo anterior, esta Superintendencia de Bancos y Otras Instituciones Financieras, resuelve dictar las siguientes:

"NORMAS QUE REGULAN EL USO DE LOS SERVICIOS DE LA BANCA ELECTRÓNICA"

Artículo 1: Las presentes Normas están dirigidas a los Bancos y demás Instituciones Financieras que ofrecen a sus clientes productos y servicios bancarios autorizados por la Superintendencia de Bancos y Otras Instituciones Financieras, a través de la Banca Electrónica.

Artículo 2: A los efectos de interpretar la presente Normativa, se definen los términos que se mencionan a continuación, los cuales tendrán el significado que indica el presente artículo, pudiendo ser utilizados tanto en plural como singular, masculino, femenino o cualquier forma verbal según el contexto en que se presente:

- **Afiliación:** Incorporación de productos y servicios a la Banca Electrónica, por parte de los clientes naturales y jurídicos, para efectos de realizar operaciones o transacciones.

- **Autenticación:** Conjunto de técnicas y procedimientos tecnológicos utilizados para verificar la identidad de un usuario persona natural o jurídica.

- **Banca Electrónica:** Productos y servicios ofrecidos por los Bancos y demás Instituciones Financieras a través de canales electrónicos.

- **Banca por Internet:** Canal electrónico utilizado por los Bancos y demás Instituciones Financieras para ofrecer a sus clientes los productos y servicios, a través de sus portales transaccionales.

- **Banca Móvil:** Canal electrónico utilizado por los Bancos y demás Instituciones Financieras para ofrecer a sus clientes los productos y servicios, basados en una aplicación instalada en un dispositivo móvil.

- **Banca Telefónica:** Canal electrónico utilizado por los Bancos y demás Instituciones Financieras para ofrecer a sus clientes los productos y servicios, a través de los centros de atención telefónica.

- **Biometría:** Métodos automáticos para el reconocimiento único de humanos, basados en uno o más rasgos conductuales o físicos intrínsecos.

- **Canal Electrónico:** Medio que permite el intercambio de información a través de la utilización de cajeros automáticos, puntos de ventas, puntos de ventas virtuales, Robot de Voz Interactivo (IVR), Banca por Internet, televisión interactiva, entre otros.

- **Claves Dinámicas:** Son claves criptográficas simétricas de un sólo uso, formadas a través de una secuencia aleatoria.

- **Certificado Digital:** Credencial digital basada en el estándar X.509 recomendada por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T).

- **Cifrado o Encriptación:** Proceso de convertir en ilegible un mensaje que se encuentra en texto claro, usualmente mediante la utilización de algoritmos matemáticos y una clave.

- **Dato Sensible:** Datos con carácter confidencial del cliente y/o usuario de la Banca Electrónica, tales como: número de cuenta; número de identificación personal; claves del cliente; número de la tarjeta; código de seguridad de la tarjeta.

- **Desafiliación:** Es el proceso mediante el cual los clientes solicitan a los Bancos y demás Instituciones Financieras desincorporar los productos y servicios ofrecidos por éstas, a través de los canales electrónicos.

- **Dispositivos de Autoservicio:** Equipos electrónicos ofrecidos a los clientes para realizar operaciones bancarias no monetarias, que habitualmente son efectuadas a través de las agencias de los Bancos y demás Instituciones Financieras.

- **Factor de Autenticación:** Técnica de verificación de identidad basada en dispositivos o información que sólo el cliente posea, sea, haga o conozca.

- **Firma Electrónica:** Información creada o utilizada por el Signatario (es la persona titular de una Firma Electrónica o Certificado Electrónico) asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado, conforme lo consagra el Decreto con Fuerza de Ley N° 1.204 de fecha 10 de febrero de 2001, de Mensaje de Datos y Firmas Electrónicas, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001.

- **Identificación:** Validación de la identidad del cliente para el uso del servicio de Banca Electrónica, mediante la utilización de datos e información que conozca tanto la Institución como el cliente.

- **IVR:** Son las siglas en inglés de Robot de Voz Interactivo, la cual consiste en un sistema telefónico que es capaz de recibir una llamada e interactuar con el humano a través de grabaciones de voz y el reconocimiento de respuestas simples.

- **No Repudio:** Es un método de seguridad que permite probar la participación de las partes en una comunicación. Existirán por tanto dos (2) posibilidades:
    - No repudio en origen: el emisor no puede negar que lo envió porque el destinatario tiene pruebas del envío.

    - No repudio en destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

El origen o recepción de un mensaje específico debe ser verificable por parte de un tercero de confianza.

- **Mantenimiento de Servicios:** Son todos los cambios a los parámetros y/o condiciones asociadas a los productos y servicios afiliados.

- **Mantenimiento de Contraseñas:** Son todos los cambios que realizan los clientes a sus claves de acceso.

- **Medio de Comunicación Electrónica:** Medio electrónico utilizado para la transmisión de mensajes desde el Banco y hacia el cliente.

- **Operaciones Bancarias no Monetarias:** Son operaciones financieras que no requiere de la dispensación de dinero tales como: dispensación de chequeras, estados de cuentas y referencias bancarias.

- **Pago Móvil:** Es un servicio ofrecido por los Bancos y demás Instituciones Financieras con la finalidad que los clientes realicen pagos o transferencias desde un dispositivo móvil a través de su línea telefónica.

- **Perfil Transaccional:** Es el conjunto de características asociadas al comportamiento transaccional de un cliente, de acuerdo a los análisis sistematizados realizados por la Institución, para protejer a éstos.

- **Programaciones de Pago:** Es la autorización por parte del cliente para el cobro automático en sus cuentas bancarias.

- **Token:** Dispositivo electrónico utilizado para facilitar el proceso de autenticación. Puede ser utilizado para la generación de contraseñas de un solo uso; así como, para almacenar contraseñas, firmas electrónicas o datos biométricos de la persona.

CAPÍTULO I
DE LA AFILIACIÓN, IDENTIFICACIÓN Y LA AUTENTICACIÓN DEL CLIENTE EN LOS SERVICIOS DE BANCA ELECTRÓNICA

Artículo 3: Los Bancos y demás Instituciones Financieras que ofrecen los servicios de Banca Electrónica, deben informar a sus clientes de forma escrita, impresa o a través de medios electrónicos, lo siguiente:

- Servicios ofrecidos y las responsabilidades de su uso.
- Procedimientos para la afiliación, cancelación, suspensión y reactivación del servicio.
- Límites diarios de montos y transacciones electrónicas.
- Comisiones y tarifas por el uso de servicio de Banca Electrónica.
- Riesgos inherentes a la utilización del servicio de Banca Electrónica.
- Procedimiento para informar cualquier irregularidad detectada.

Artículo 4: Los Bancos y demás Instituciones Financieras deben obtener la firma autógrafa de los clientes titulares, previa identificación de éstos, para contratar los productos de tarjetas de crédito y débito. En cuanto a la afiliación del servicio de Banca por Internet y Banca Móvil, las Instituciones Financieras podrán implementar la aceptación de contratos electrónicos, utilizando Factor de autenticación categoría 1 a que hace referencia el artículo 5 de las presentes normas. Lo anterior, se considerará como la confirmación y autorización de uso de los servicios de Banca Electrónica.

Artículo 5: Los Bancos y demás Instituciones Financieras deberán utilizar factores de autenticación para verificar la identidad de sus clientes y la cualidad de éstos para realizar operaciones mediante la Banca Electrónica. Dichos factores de autenticación serán los siguientes:

- Factor de autenticación categoría 1: Se compone de la información obtenida de la ficha del cliente y del uso de productos, servicios u

operaciones efectuadas por éstos mediante los diversos canales. Esta información será utilizada mediante la aplicación de cuestionarios al cliente a través del servicio de IVR, Banca por Internet y la asistencia de operadores telefónicos. Para este tipo de factor los Bancos y demás Instituciones Financieras deberán:

- Definir previamente los cuestionarios que serán aplicados para la identificación positiva de los clientes y modificar su contenido al menos una (1) vez al año.

- Establecer generadores aleatorios de las preguntas de los cuestionarios.

- Cuando intervenga el operador, éste no podrá consultar o conocer anticipadamente las respuestas para la identificación positiva del cliente, las cuales deben ser validadas con el uso de sistemas informáticos.

- Factor de Autenticación Categoría 2: Se compone de contraseñas que sólo el cliente conoce e ingresa mediante un mecanismo o dispositivo de acceso, el cual debe cumplir con las siguientes características:

  - Su longitud mínima debe ser de:

    - Cuatro (4) caracteres para los servicios ofrecidos a través de cajeros automáticos, puntos de ventas, Banca Telefónica, servicio de IVR y Pago Móvil.

    - Ocho (8) caracteres para Banca por Internet y Banca Móvil.

    - Cuando el dispositivo de acceso lo permita, la composición de este factor de autenticación deberá incluir caracteres alfabéticos, numéricos y especiales.

    - Se debe validar el uso de las últimas cinco (5) contraseñas.

  - Su vencimiento no será superior a ciento ochenta (180) días para

todos los canales electrónicos; no obstante, los Bancos y demás Instituciones Financieras están en la obligación de ofrecer a sus clientes la posibilidad de realizar el cambio de las contraseñas cuando éstos lo requieran.

- En el caso de las contraseñas asignadas por los Bancos y demás Instituciones Financieras, para el acceso a la Banca Electrónica, se debe requerir en forma automática que el cliente la modifique inmediatamente después de iniciar la primera sesión.

- Garantizar que la primera sesión se efectúe como máximo al siguiente día hábil bancario de la generación de la contraseña por parte de la Institución; en caso contrario, ésta debe ser inhabilitada automáticamente.

- En ningún caso se podrá utilizar como contraseña, la siguiente información:

    - El identificador del cliente.
    - El nombre de la Institución.
    - Más de tres (3) caracteres iguales consecutivos numéricos o alfabéticos.
    - Fecha de nacimiento, nombres, apellidos y número telefónico, registrado por el cliente en la Institución.

- Factor de Autenticación Categoría 3: Se compone de claves dinámicas de un único uso, generadas por dispositivos electrónicos o cualquier otro medio, las cuales deben cumplir con las siguientes características:

    - Contar con mecanismos que impidan su duplicación o alteración.
    - Una vez generada la clave dinámica, ésta tendrá vigencia:
        - Hasta dos (2) minutos, en el caso de que sean generados por

Tokens.

- Hasta el cierre de sesión, para los canales de Banca por Internet y Banca Móvil.

- Hasta seis (6) horas, para los servicios de cajeros automáticos y Pago Móvil.

- No ser conocida antes de su generación ni durante su uso, por los funcionarios, empleados, representantes o por terceros de la Institución.

- Se podrán utilizar tablas aleatorias de contraseñas como factor de autenticación de esta categoría, siempre y cuando cumplan con las características listadas en este factor de autenticación.

Los Bancos y demás Instituciones Financieras deben facilitar a los Clientes los mecanismos, dispositivos o medios generadores de las claves dinámicas. Asimismo, podrán considerar dentro de esta categoría la información contenida en el circuito integrado (chip) de las tarjetas bancarias, siempre y cuando dichas tarjetas se utilicen únicamente para operaciones que se realicen a través de cajeros automáticos y terminales de puntos de ventas y obtengan la información de la tarjeta a través de dicho circuito o chip. Las Instituciones, deberán considerar lo siguiente:

- Si la autenticación es estática, la validación de los datos deberá realizarse en tiempo real en los computadores centrales de la Institución Financiera.

- Si la autenticación es dinámica, la validación de los datos podrá realizarse fuera de línea.

Los Bancos y demás Instituciones Financieras que ejecuten y autoricen transacciones mediante el uso de tarjetas bancarias sin circuito integrado, en cajeros automáticos y terminales de puntos de ventas o sin el uso de un factor de autenticación de la categoría tipo 3, como mínimo, asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por los Clientes.

Los reclamos derivados de estas operaciones deberán ser atendidos en el plazo establecido por la Ley General de Bancos y Otras Instituciones Financieras y las normas vigentes.

- Factor de Autenticación Categoría 4: Se refiere a la utilización de firmas electrónicas certificadas debidamente emitidas a nombre del Cliente por un Proveedor de Servicios de Certificación (PSC).

  Los Bancos y demás Instituciones Financieras que aprueben operaciones mediante el uso de tarjetas bancarias con circuito integrado (chip), en cajeros automáticos y terminales de punto de venta, podrán implementar este factor en dichas tarjetas para operaciones donde sea requerido la autenticación del Cliente; así como, el no repudio.

- Factor de Autenticación Categoría 5: Se compone de información del Cliente derivada de sus características Biométricas.

Artículo 6: Los sistemas de Banca Electrónica de los Bancos y demás Instituciones Financieras deberán requerir a sus Clientes un factor para inicio de sesión más un segundo factor de autenticación de categorías 3, 4 ó 5 a que hace referencia el artículo 5 de las presentes normas. Estos factores serán aplicados de acuerdo con el siguiente esquema:

Operaciones	Factores Requeridos*	
	Factor Base	Factor Adicional
Afiliación y desafiliación de productos y servicios.	2	3,4 ó 5
Mantenimiento de productos, servicios y programaciones de pago.	2	3,4 ó 5
Pagos o transferencias electrónicas a terceros.	2	3,4 ó 5
Retiros o adelantos de efectivo.	2	3,4 ó 5
Apertura de segundas cuentas o productos financieros.	2	4
Actualización de datos de la ficha del Cliente a través de Banca por Internet.	2	4
Mantenimiento de contraseñas, activación o desactivación de Tarjetas de Crédito y desactivación de Tarjetas de Débito.	1, 2	N/A
Consultas.	2	N/A
Transacciones ofrecidas a través de dispositivos de autoservicio.	2	N/A
Pagos o transferencia electrónica mismo titular y mismo banco.	2	N/A

* **Factor base:** Es el factor mínimo requerido para realizar la autenticación inicial del Cliente.
Factor Adicional: Es el segundo factor o grupo de factores de autenticación que se debe requerir al Cliente.

Artículo 7: Para las operaciones de pagos o transferencias electrónicas a terceros que no requieran la afiliación o registro de cuentas, se deberá utilizar el factor adicional, a que hace referencia el artículo anterior.

Artículo 8: En cuanto al servicio de Pago Móvil, los Bancos y demás Instituciones Financieras podrán ofrecer las operaciones de transferencias y pagos a terceros sobre cuentas y tarjetas de crédito previamente afiliadas por los Clientes, validando un factor de autenticación de categoría 2, a que hace referencia el artículo 5 de las presentes normas.

Artículo 9: Para el uso del servicio de Banca Telefónica los Clientes deberán autenticarse a través del Robot de Voz Interactivo (IVR) con un factor de autenticación de categoría 2, a que hace referencia el artículo 5 de las presentes normas.

Artículo 10: Para permitir el inicio de sesión a los Clientes a través de los servicios ofrecidos por la Banca por Internet, Banca Móvil u otro canal electrónico que así lo requiera, los Bancos y demás Instituciones Financieras deberán solicitar y validar al menos:

- Un identificador de Cliente de por lo menos seis (6) caracteres.
- Un factor de autenticación de las categorías 2, 3 ó 4.

El identificador del Cliente deberá ser único y permitirá a los Bancos y demás Instituciones Financieras, determinar todas las operaciones realizadas por el propio Cliente mediante estos canales.

Tratándose de Pago Móvil, el identificador de Cliente deberá ser el número de la línea del teléfono móvil asociado al uso de dicho servicio, debiendo las Instituciones; en todo caso, obtenerlo de manera automática e inequívoca del teléfono móvil correspondiente.

Artículo 11: Los Bancos y demás Instituciones Financieras deben inhabilitar inmediatamente el acceso a los servicios ofrecidos por la Banca Electrónica cuando el Cliente lo solicite de forma escrita o cese su relación con la

Institución. En caso de ser realizada la solicitud por medio de la Banca Telefónica, se efectuará un bloqueo preventivo hasta su formalización.

Artículo 12: En la Banca por Internet, los Bancos y demás Instituciones Financieras deben proveer información al Cliente, de acuerdo con lo siguiente:

- Elementos que identifiquen a la Institución, antes de ingresar todos los elementos de autenticación. Para ello, deberán usar certificados digitales (SSL) u otros mecanismos que permitan autenticar el sitio transaccional. Adicionalmente, podrán utilizar la siguiente información:

  - Aquella que el Cliente conozca y haya proporcionado a la Institución, o bien, que haya señalado para este fin, tales como nombres y apellidos, imágenes, entre otros.

  - La provista por el factor de autenticación de categoría 4.

- Una vez que el Cliente verifique que se trata de la Institución e inicie una sesión segura, se deberá proporcionar de forma notoria y visible, al menos la siguiente información:

  - Fecha y hora del ingreso a su última sesión; y,

  - Nombre y apellido del Cliente.

Artículo 13: Para el uso de los factores de autenticación, los Bancos y demás Instituciones Financieras se sujetarán a lo siguiente:

- Deberán mantener procedimientos que proporcionen seguridad a la información de sus Clientes durante la generación, custodia, distribución, asignación y reposición de dichos factores.

- Tratándose de los servicios prestados a las personas jurídicas, a través de la Banca por Internet, los Bancos y demás Instituciones Financieras podrán implementar mecanismos mediante los cuales una persona autorizada por el Cliente, realice la solicitud para efectuar las operaciones, y otra persona distinta que sea designada por el propio

Cliente, autorice su ejecución. En estos casos, se podrá exceptuar a las Instituciones Financieras de la obligación de fijar límites de sesiones simultáneas, siempre y cuando el Cliente cuente con factores de autenticación indicados en las categorías 4 y 5 a que se refiere el artículo 5.

- Tendrán prohibido divulgar la información protegida por los factores de autenticación.

- Tendrán prohibido solicitar a sus Clientes, a través de sus funcionarios, empleados, representantes o terceros, la información parcial o completa, establecida en los factores de autenticación de las categorías 2 ó 3 a que se refiere el artículo 5 de las presentes normas.

Artículo 14: Los Bancos y demás Instituciones Financieras podrán establecer métodos adicionales de autenticación a los previstos en esta norma para las transacciones realizadas en la Banca Electrónica.

CAPÍTULO II
DE LA OPERACIÓN DE LOS SERVICIOS DE BANCA ELECTRÓNICA

Artículo 15: Los Bancos y demás Instituciones Financieras deben establecer montos máximos diarios para cada canal electrónico, con base a estudios realizados por su Unidad de Administración Integral de Riesgo (UAIR), sin perjuicio de lo establecido en la legislación y las normas vigentes. Para el servicio de pago móvil, los montos máximos diarios no deberán ser mayores a los establecidos para los retiros en los cajeros automáticos.

Artículo 16: Los Bancos y demás Instituciones Financieras deberán generar comprobantes electrónicos para todas las operaciones realizadas en el servicio de Banca Electrónica.

Artículo 17: Con respecto a la sesión del Cliente, los Bancos y demás Instituciones Financieras deben garantizar lo siguiente:

- Finalizar la sesión en forma automática en los casos siguientes:

- Cuando la inactividad alcance a tres (3) minutos en la Banca por Internet y Banca Móvil.

- Cuando el período de inactividad alcance los diez (10) segundos en las operaciones realizadas mediante cajeros automáticos y puntos de ventas.

- Cuando se detecten sesiones simultáneas.

- Los Bancos y demás Instituciones Financieras que ofrezcan enlaces a empresas mediante su página web, deberán comunicar a sus Clientes que al momento de ingresar a éstos, su seguridad no depende ni es responsabilidad de dicha Institución.

Artículo 18: Los Bancos y demás Instituciones Financieras deberán informar a sus Clientes, mediante campañas educacionales, sobre el funcionamiento de los canales electrónicos que pongan al alcance de éstos, a fin de prevenir actos que pudieran derivar en operaciones irregulares o ilegales que afecten a los Clientes o a las propias Instituciones.

Artículo 19: Los Bancos y demás Instituciones Financieras podrán enviar a solicitud de sus Clientes, estados de cuenta a través de medios de comunicación electrónica, siempre y cuando la información se transmita de forma cifrada y garanticen la autenticación empleando como mínimo un factor de autenticación de categoría 2 a que se refiere el artículo 5 de las presentes normas.

Artículo 20: Los Bancos y demás Instituciones Financieras que ofrezcan el servicio de puntos de ventas virtuales, deben garantizar lo siguiente:

- Elementos que identifiquen a la Institución, antes de ingresar todos los datos de autenticación.

- Proteger el canal de comunicación utilizando cifrado robusto.

- Mantener los límites diarios establecidos en la red para el monto de los pagos.

- Utilizar un Factor de autenticación de categoría 2 a que se refiere el artículo 5 de las presentes normas, aunado a los datos de la tarjeta con la cual se va a realizar la operación.

- Los puntos de ventas virtuales siempre deben ser dispuestos por las Instituciones Financieras. En este sentido, no afiliaran comercios que pretendan instalar sus propios puntos de ventas virtuales.

CAPÍTULO III
DE LA INFORMACIÓN TRANSMITIDA, ALMACENADA O PROCESADA A TRAVÉS DE LOS CANALES ELECTRÓNICOS

Artículo 21: Para las operaciones que se realicen a través de la Banca Electrónica, los Bancos y demás Instituciones Financieras deben implementar mecanismos de cifrado en la transmisión y almacenamiento de la información, a fin de evitar que los datos sensibles sean conocidos por terceros no autorizados.

Artículo 22: En ningún caso, los Bancos y demás Instituciones Financieras podrán transmitir las contraseñas de categoría 2 a que se refiere el artículo 5 de las presentes normas o números de identificación personal y de productos, a través de algún medio de comunicación electrónica.

Artículo 23: Los datos sensibles de las tarjetas de débito y crédito sólo podrán ser almacenados por las Operadoras de Tarjetas durante el tiempo que tome los procesos de validación, grabación y autorización de las transacciones.

Artículo 24: Las operaciones de compras nacionales, a través de los terminales de puntos de venta con tarjetas de débito, deberán hacer uso de sistemas de transportes de datos dentro del territorio de la República Bolivariana de Venezuela.

CAPÍTULO IV
DEL MONITOREO Y CONTROL DE LAS OPERACIONES Y SERVICIOS DE BANCA ELECTRÓNICA

Artículo 25: Los Bancos y demás Instituciones Financieras deben notificar en forma inmediata a los Clientes, las alertas asociadas a las operaciones realizadas a través de los canales electrónicos de acuerdo al perfil transaccional del cliente, determinado oportuna y automáticamente por la Institución, a través de mensajes de texto (SMS) al teléfono móvil registrado. En caso que el Cliente no posea el mencionado dispositivo o manifieste no desear el servicio, la Institución podrá realizar la notificación por cualquier otro medio de comunicación electrónica.

El mensaje enviado deberá incluir al menos la siguiente información: fecha y hora de la transacción, monto de la operación, serial o número de referencia de la transacción, nombre y número de teléfono de la Institución, canal utilizado y tipo de operación. Para ello, los Bancos y demás Instituciones Financieras deberán asegurar que los Robot de Voz Interactivo (IVR) permitan al Cliente acceder a opciones para reportar, de forma expedita, los presuntos fraudes y obtener asistencia debida a su reclamo.

Artículo 26: Los Bancos y demás Instituciones Financieras deberán establecer procesos y mecanismos automáticos para bloquear preventivamente el acceso a la Banca Electrónica, en los siguientes casos:

- Cuando se intente ingresar al servicio utilizando información de autenticación incorrecta. En ningún caso, los intentos de acceso fallidos podrán exceder tres (3) intentos consecutivos.
- Cuando los sistemas de monitoreo detecten comportamiento transaccional irregular o los sistemas de seguridad detecten un ataque informático que comprometa los datos sensibles.
- Cuando existan situaciones que comprometan la seguridad de los sistemas de información y del Cliente.

Artículo 27: Cuando los sistemas de Banca Electrónica determinen fallas de dispensación de efectivo en los cajeros automáticos, los Bancos y demás Instituciones Financieras deberán reintegrar los montos comprometidos de manera inmediata sin la necesidad de reclamo del Cliente, sin que esto incluya

el cobro de comisiones. Adicionalmente, deberán mantener a disposición de este Organismo los reportes o estadísticas producto de estos eventos.

Artículo 28: Los Bancos y demás Instituciones Financieras deben definir mecanismos de monitoreo y control para asegurar el adecuado funcionamiento de los canales electrónicos.

CAPÍTULO V
REGIMEN SANCIONATORIO

Artículo 29: La infracción a las presentes normas podrá ser sancionada de conformidad con lo previsto en el numeral 5 del artículo 363 de la Ley General de Bancos y Otras Instituciones Financieras, sin perjuicio de otras medidas administrativas e instrucciones que este Organismo pueda imponer en atención a sus competencias.

CAPÍTULO VI
DISPOSICIONES FINALES

Artículo 30: La gestión de la seguridad, contingencias y comunicaciones deben estar en concordancia con lo establecido en:

- La Circular N° SBIF-DSB-IO-GGT-GRT-01907 de fecha 30 de enero de 2008, contentiva de la Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica Virtual y en Línea para los Entes sometidos al Control, Regulación, Vigilancia y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras.

De igual forma podrán tener como referencia:

- El Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS por sus siglas en inglés).

Artículo 31: La presente Resolución entrará, en vigencia a partir de la fecha de

su publicación en la Gaceta Oficial de la Republica Bolivariana de Venezuela.

Artículo 32: Los Bancos y demás Instituciones Financieras tendrán un plazo de cuatro (4) meses a partir de la entrada en vigencia de esta normativa para consignar a esta Superintendencia de Bancos y Otras Instituciones Financieras, un plan de trabajo con su respectivo análisis de brechas en los sistemas de información y dieciocho (18) meses adicionales, contados a partir de la entrega de la citada información, para efectuar las adecuaciones que aseguren el cumplimiento de las disposiciones establecidas.

Comuníquese y Publíquese

Edgar Hernández Behrens
Superintendente

SUDEBAN
SUPERINTENDENCIA DE BANCOS Y OTRAS INSTITUCIONES FINANCIERAS

Asunto: Norma prudencial