La Regulación de la Banca Electrónica en Panamá

Por: Loraine Chavarría
Jefa del Departamento de Normas y Desarrollo

Las entidades bancarias como instituciones innovadoras y en constante búsqueda de nuevas oportunidades de negocio para satisfacer las necesidades de sus clientes, desarrollan nuevos productos y servicios, por lo que han visto en el servicio de banca electrónica una posibilidad de hacer negocio a bajo costo.

En este sentido, el Internet es un medio en expansión de uso dinámico, que permite intercambiar información, hacer transacciones y consultas con gran facilidad y economía de escala, tanto para quien ofrece los servicios como para sus usuarios. Así, el fenómeno de la banca electrónica, también conocido como banca digital, banca virtual o banca online, entre otras denominaciones, permite a los clientes operar con sus bancos con gran rapidez, flexibilidad y seguridad, las 24 horas al día y 7 días a la semana.

Sin embargo, las actividades ofrecidas en el servicio de banca electrónica, deben ser reguladas a nivel jurídico, ajustándose a principios de libertad de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional, equivalencia del soporte electrónico al soporte de papel y equivalencia funcional del comercio tradicional con el comercio electrónico.

De acuerdo con el Principio No. 13 para una Supervisión Bancaria Efectiva del Comité de Basilea "Los supervisores deben estar conformes en cuanto a que los bancos cuentan con un proceso de administración integral de riesgos (con inclusión de la fiscalización apropiada del directorio y de la gerencia superior) para identificar, medir, monitorear y controlar todos los otros riesgos sustanciales y, cuando corresponda, retener capital para hacer frente a estos riesgos".

Así pues, atendiendo las necesidades de las entidades bancarias, la Superintendencia de Bancos (SBP), aprobó el Acuerdo 5-2003 de 12 de junio de 2003 sobre Banca Electrónica, basado en el documento "Principios de Gestión de Riesgo para la Banca Electrónica", emitido por el Comité de Basilea en mayo de 2001, el cual identifica 14 principios básicos para la gestión del riesgo de banca electrónica, integrados en tres grandes grupos, a saber: a) Supervisión de la Junta Directiva y la Gerencia Superior; b) Controles de seguridad; y, c) Manejo del riesgo legal y reputacional.

Dicho Acuerdo es aplicable a los Bancos oficiales, a los Bancos de Licencia General y a los Bancos de Licencia Internacional, que presten el servicio de banca electrónica a sus clientes, destacando los siguientes puntos:

- Todo banco podrá llevar a cabo el servicio de banca electrónica en o desde la República de Panamá siempre y cuando haya obtenido previamente la debida autorización de la Superintendencia de Bancos.

- La Junta Directiva o Gerencia Superior de cada banco debe asegurarse de integrar al manual de operaciones de la entidad bancaria los procedimientos, políticas y controles internos necesarios a fin de mantener una estructura administrativa y operativa adecuada para ofrecer el servicio de banca electrónica.

- La unidad de riesgo existente del banco deberá tener entre sus funciones la identificación, evaluación y control de los riesgos asociados al servicio de banca electrónica.

- Será responsabilidad del banco velar porque se realicen las auditorias periódicas para la evaluación, revisión y seguimiento permanente de la función y operación de los servicios de banca electrónica.

- El banco está obligado a informar al cliente de banca electrónica sobre las características, condiciones, costo y cualquier otra estipulación determinante que conlleve el uso del servicio de banca electrónica.

- El banco debe asegurar en toda transacción la autenticidad, la integridad de la información transmitida, la confidencialidad, la no renuncia o rechazo una vez aceptada, segregación de responsabilidades y controles de autorización.

- El banco debe emplear técnicas de control apropiadas, tales como criptografía, protocolos específicos u otros controles de seguridad para asegurar la privacidad y seguridad de la información del cliente, pues el contenido de las transacciones y operaciones realizadas en un entorno electrónico y la identidad de las partes debe mantenerse en todo momento inaccesible por parte de terceros.

- El banco, para prevenir el uso indebido de los servicios bancarios a través de la banca electrónica, debe asegurar la existencia, vigencia y funcionamiento de procedimientos estrictos y medidas eficaces de seguridad para la identificación y seguimiento de transacciones sospechosas, así como la aplicación de la política Conozca a su Cliente y procedimientos de Diligencia Debida.

Es importante que los usuarios de los servicios bancarios estén anuentes que a la sombra de la banca electrónica han surgido también nuevas técnicas que tratan de utilizar fraudulentamente el sistema de banca electrónica. Los sistemas de banca electrónica tienen dos puntos de ataque, por un lado las propias entidades financieras y, por otro, los clientes de estas. Debido que las entidades bancarias han tomado suficientes medidas de seguridad que dificultan enormemente los posibles fraudes al sistema, los atacantes se dirigen al lado más débil: los clientes bancarios. Así han surgido nuevos procedimientos de fraude que utilizan específicamente la banca electrónica y que son, principalmente, el *"phishing"* y el *"pharming"*.

El ***phishing*** consiste en solicitar a los clientes de una entidad de crédito que visiten una página web falsa, haciendo creer al visitante que se encuentra en la página original o copiada. La vía de difusión más habitual de esta técnica es el correo electrónico, aunque últimamente se han detectado vías alternativas como el teléfono o el fax. Una vez en las páginas falsas, se pide al visitante que introduzca datos personales (nombre de usuario, claves de acceso, etc.) que posteriormente son usados por los creadores de la estafa para hacer disposiciones en las cuentas de los clientes. Por esto, si usted recibe un correo de su banco solicitando que entre en la página web para cambiar sus datos, desconfíe, puede estar sufriendo *"phishing"*.

El ***pharming*** es una técnica más compleja que la anterior que consiste en explotar una vulnerabilidad de los sistemas de servidores DNS (siglas en inglés del Sistema de Nombres de Dominio) de modo que el atacante adquiere el nombre de dominio de un sitio web, y redirige el tráfico de esa página a otro sitio distinto del verdadero. Si el sitio al que se redirige el tráfico es una copia de la página web de una entidad bancaria, puede ser usado para obtener ilícitamente la contraseña, el numero de identificación personal o el número de cuenta del cliente.

En este sentido, se puede elaborar una lista de recomendaciones o medidas básicas a tomar en cuenta para disfrutar de las ventajas que ofrece la banca electrónica minimizando los riesgos.

1. Las claves de acceso son personales e intransferibles.
2. Memorizar las claves y no escribirlas en ningún sitio visible.
3. La entidad bancaria nunca solicitará revelar sus claves.
4. No utilizar computadoras desconocidas para acceder a la banca online. Evite operar con el banco desde computadoras de uso público como los del trabajo o cibercafés.
5. No acceder a "links" propuestos por desconocidos.
6. Comprobar que la página de acceso es una página segura. Puede verificar que la parte inferior de la ventana salga el incono de un candado.
7. Estar atentos a las modificaciones en la Web que pueda introducir la entidad bancaria.
8. Actualizar las medidas de seguridad como los antivirus, antispyware y firewalls.
9. Revisar los avisos de seguridad publicados por la entidad bancaria en la página Web.
10. En caso de sospecha, comunicarlo a la entidad bancaria telefónicamente.