

## **La Superintendencia Financiera de Colombia y la inseguridad informática en el sector financiero**

Por:

*Jeimy J. Cano, Ph.D, CFE*

*Profesor Investigador*

*GECTI - Uniandes*

### **Introducción**

Siguiendo la evolución de las tendencias internacionales sobre la expedición de normas que busquen fortalecer la gestión de la seguridad de la información, la Superintendencia Financiera de Colombia – SFC, ha publicado la Circular 052 del 25 de octubre de 2007, denominada “Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios”, la cual busca establecer un referente básico para la seguridad informática del sector Bancario Colombiano.

Esta circular, consecuente con los esfuerzos adelantado por países como Argentina y Chile donde normas similares hace algún tiempo funcionan, es la enzima catalizante que impulse a los Bancos a considerar de manera formal y efectiva las directrices de seguridad de la información que beneficien tanto a sus clientes como a sus estrategias de negocio. Un sistema financiero fortalecido en la gestión de seguridad de la información establece una base de confianza para generación de nuevos y mejores servicios que promuevan el uso de las tecnologías de información.

Bien anota la reunión de las Naciones Unidas sobre la Sociedad de la Información realizada en Túnez en 2005, que la seguridad de la información es un factor fundamental para el desarrollo de las economías mundiales y como un elemento fundamental para el fortalecimiento de la confianza en el uso de las TIC (Tecnologías de Información y Comunicaciones) que permitan un sociedad digital vinculante e incluyente, que sólo es posible con a través de métodos y sistemas más confiables y de fácil utilización.

La SFC al promulgar esta circular, establece un referente nacional importante que le dice a los otros sectores de la economía colombiana que la seguridad de la información es una variable definitiva que afecta el buen desempeño de los mercados y la confianza de los inversionistas. Así mismo, el proyecto de ley de Habeas Data, actualmente en revisión por parte de la Corte Constitucional<sup>1</sup>, es un complemento clave para fortalecer los derechos de los usuarios frente a su información, lo cual permite ir forjando una cultura de seguridad y custodia de los datos, que profundice aún más la cultura de todos los ciudadanos sobre la protección de nuestra propia información.

---

<sup>1</sup> El literal f) del artículo 5 consagra el principio de seguridad según el cual "La información que conforma los registros individuales constitutivos de los bancos de datos (.), así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado"; así mismo el artículo 7, por su parte, ordena a los operadores (.) "Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento".

## **La Circular**

La norma de la SFC cuenta siete secciones que detallan el ámbito de aplicación, las definiciones y criterios de seguridad y calidad de la información, las obligaciones generales, las obligaciones adicionales por tipo de canal, reglas sobre la actualización de software, obligaciones específicas por tipo de medio y análisis de vulnerabilidades.

Una revisión básica de la norma nos ilustra el espíritu del órgano de supervisión y control para que los servicios bancarios desarrollen un nivel de seguridad mínimo para bien de los usuarios y del sector en general; que se promueva una cultura de riesgos y transparencia en el manejo de las vulnerabilidades, y sobremanera una actitud responsable de los bancos y los usuarios sobre el buen uso de los recursos de informáticos que agilizan las transacciones.

Si bien la idea de este documento no es enumerar completamente la norma de la SFC, la cual se encuentra disponible en el sitio web del ente de supervisión, <http://www.superfinanciera.gov.co/NormativaFinanciera/Paginas/circularesexternas07.htm>, sí es detallar, algunos elementos particulares de la misma que generan reflexiones interesantes para las organizaciones financieras y para todos aquellos que quieran avanzar en una revisión de seguridad de la información en términos prácticos y operativos en sus organizaciones.

## **Comentarios sobre algunos numerales de la norma**

En la sección definiciones y criterios de seguridad y calidad resaltamos el concepto de disponibilidad: “La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso”. Esta definición de disponibilidad de la información va más allá de la noción generalmente aceptada del concepto en seguridad de la información. Esta noción exige de la entidad contar con procedimientos y estrategias que le permitan tener acceso a la información ahora y en el futuro, para lo cual los formatos en que los guarde o transforme deberá considerarlos en su proceso de gestión de seguridad informática y de documentación electrónica. Es decir, es responsabilidad de la organización proveer acceso a la información en el tiempo especificado, en el formato establecido y en el momento requerido, con las condiciones de integridad, control y acceso que sean necesarias para validar y certificar la condición de originalidad del documento cuando éste se generó.

Esta connotación de disponibilidad exige de las organizaciones repensar el tema de documentación electrónica y archivo electrónico organizacional, lo cual establece revisar referentes internacionales como el Sedona Guidelines, donde se detallan las mejores prácticas internacionales para el uso de conceptos como el *Record Management*.

En la sección de seguridad y calidad, por cierto, una de las más detalladas y que son de obligatorio cumplimiento, llaman la atención entre otros, los numerales:

3.1.7 Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones

3.1.13 Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para confirmación de las operaciones que no correspondan a sus hábitos.

3.1.16 Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

El numeral 3.1.7 hace énfasis en los temas de keyloggers, spyware y demás plagas informáticas que busquen afectar la información y operaciones de los usuarios en los sistemas de información de los Bancos. Sin embargo, es importante anotar que, si bien los bancos estarán obligados a proteger mejor las estaciones clientes de sus usuarios, los usuarios deben reconocer su responsabilidad como primeros custodios de su información, pues en la lucha contra la inseguridad tanto la organización con el usuario suman a la hora de descubrirla y confrontarla.

En el numeral 3.1.13 se habla de la elaboración de un perfil de transacciones que busca una estrategia de protección adicional para el usuario que permita detectar operaciones anormales o no usuales y así advertir posibles usos no autorizados de sus cuentas. Sin embargo, esta posibilidad debe ser sometida y analizada frente a las implicaciones del proyecto de ley de Habeas Data, donde los usuarios tienen derecho a la privacidad de sus información y habría que balancear hasta dónde y cómo sería el mecanismo previsto para el diseño del perfil, sin que se afecten los derechos de los ciudadanos.

Lo detallado en el numeral 3.1.16 es la formalización de una práctica general de seguridad informática que busca asegurar la confiabilidad e integridad de los registros de las operaciones de los Bancos. El referente de la fecha y hora de la transacción con los datos adicionales que permitan su identificación plena, es factor clave para mantener un debido registro de las acciones de los usuarios y de los sistemas. Sin una sincronización adecuada de la plataforma computacional que soporte los sistemas de información de los bancos, habrá complicaciones y dificultades para identificar situaciones de excepción que generen disputas entre las partes.

En la sección 3.3 denominada Documentación llama la atención el numeral 3.3.2, el cual reza: “Velar por que los órganos de control, incluyan en sus informes la evaluación acerca del cumplimiento de los procedimientos, controles y seguridades, establecidos por la entidad y las norma vigentes, para la prestación de los servicios a los clientes y usuarios, a través de los canales de distribución”. Este aparte, establece una responsabilidad formal de las oficina de auditoría de sistemas, control interno, contraloría interna o su función equivalente, bien sea con personal interno o delegado en un tercero, para adelantar ejercicios de verificación y control de las medidas implementadas por las organizaciones financieras en atención de los riesgos derivados de la creación, transmisión, almacenamiento, recuperación y disposición de la información a través de tecnologías de información.

Otro numeral interesante es el 3.3.6 que dice: “Llevar un registro de las consultas realizadas por lo funcionarios de la entidad sobre la información confidencial<sup>2</sup> de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal

---

<sup>2</sup> Lo confidencial se establece siempre que a la información de saldos, movimientos, inversiones, personal identification number-pin, entre otras, se le agregue el nombre, la identificación del usuario, ver numeral 2.14 de la circular.

utilizado, identificación de equipo, fecha y hora. En desarrollo de lo anterior, se deberán establecer mecanismos que restrinjan el acceso a dicha información, para que sólo pueda ser usada por el personal que lo requiera en función de su trabajo”.

Este numeral busca salvaguardar formalmente la privacidad de los datos de los interesados y exigirle a la entidad vigilada un uso adecuado de la información de sus clientes o usuarios. Esto nos indica que el usuario o cliente de la misma tendrá mayores elementos para demandar una protección adecuada de su información, no solamente amparado en el artículo 15 de la Constitución Nacional y las consideraciones del proyecto de Ley de Habeas Data, sino ahora en las disposiciones que establece la SFC para los Bancos en Colombia.

En la sección 3.4 relacionada con Divulgación de Información se resaltan tres (3) numerales que sugieren nuevas responsabilidades para los Bancos y mayores beneficios para los clientes y usuarios:

3.4.4 Informar y capacitar a los clientes acerca de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de productos y servicios ofrecidos.

3.4.6 Diseñar procedimientos para dar a conocer a los clientes, usuarios y funcionarios, los riesgos derivados del uso de los diferentes medios y canales.

3.4.7 Expedir un soporte, en papel o por medios electrónicos, al momento de la realización de cada transacción. (...)

Estos tres numerales nos muestran que las entidades bancarias deben apersonarse de la formación de los usuarios en temas de seguridad, como una manera real y clara de vincular en su modelo de seguridad de la información a sus clientes y usuarios. En ese mismo sentido, promover una cultura de administración de riesgos asociada con el uso de los canales disponibles para hacer sus operaciones. Este en particular, consignado en el numeral 3.4.6 obliga a un banco a mostrarle a sus clientes los resultados formales de los análisis de riesgos que han adelantado por cada uno de sus servicios y canales, lo que le permite al usuario final conocer las implicaciones del uso de una u otra forma de interacción con la entidad financiera.

Finalmente, el tema del soporte en el momento de la transacción es un avance llamativo, pues resulta particularmente útil para el usuario conocer de antemano las condiciones en las cuales una entidad financiera hará la transacción detallando aspectos como la dirección IP para el caso de Internet, el número del dispositivo móvil desde el cual se hizo la transacción, el costo de la operación, el número de la transacción, entre otros, como una medida de notificación y decisión para el usuario del servicio. Esto necesariamente llevará a las organizaciones financieras a pensar como parte del diseño de las aplicaciones, las consideraciones de registro de auditoría o *logging*, requeridos para soportar las funcionalidades exigidas. No se detalla en el numeral 3.4 el tiempo previsto para almacenar y disponer de los mencionados registros.<sup>3</sup>

---

<sup>3</sup> Se hace la claridad de que existe el Artículo 96 del Estatuto Orgánico del Sistema Financiero – EOSF que dice que los soportes contables deben conservarse 5 años.

En la sección 4 Obligaciones adicionales por tipo de canal, se resalta lo establecido en los numerales 4.1.1 “Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deberán ser conservadas por lo menos un (1) año o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto” y 4.1.6 “Establecer procedimientos necesarios para atender de manera segura y eficiente a sus clientes en todo momento, en particular cuando se presenten situaciones especiales tales como: fallas en los sistemas, restricciones en los servicios, fechas y horas de mayor congestión, posible alteración del orden público, entre otras, así como para el retorno a la normalidad. Las medidas adoptadas deberán ser informadas oportunamente a los clientes y usuarios”.

La información de las imágenes es un reto interesante para los Bancos. Si bien no todos los bancos tienen sistemas de grabación digital de imágenes con tiempos de conservación que oscilan entre 4 a 6 meses por el volumen que esto representa y los costos asociados con los medios ópticos para su almacenamiento (generalmente DVD)<sup>4</sup>, existen organizaciones que tienen su información de video en cintas magnéticas que requieren de cuidados y equipos especiales para su consulta. Con esta nueva directriz de la SFC y considerando el nuevo concepto de disponibilidad, las organizaciones deben prepararse para mantener vigentes los videos e imágenes que se registren con los sistemas de grabación (para oficinas y ATM – Cajeros automáticos), ya que hacen parte del acervo probatorio de la institución y deben ser resguardados y asimilados como información sensible dentro de la gestión de seguridad de la organización.

Leyendo detalladamente el numeral 4.1.6 es claro que las entidades financieras estarán obligadas a vincular y entrenar a los usuarios ante situaciones de contingencia. Lo planes de contingencia ahora contarán con una sección de procedimientos y controles para los usuarios y clientes, los cuales serán participantes activos y jueces de primera mano de cómo la institución bancaria adelanta y afina los procesos de continuidad de operaciones y recuperación ante fallas. Ahora estará más expuesta la imagen de las organizaciones bancarias, pero también será un reto interesante para avanzar en una cultura preventiva y de continuidad que aún está por desarrollar en nuestro país.

Más adelante en la sección 4.7 relativa a los centros de atención telefónica (call center, contact center) se hacen exigencias importantes que hablan de la formalidad y controles que deben existir en esas áreas.

Revisando los cinco (5) numerales de esta sección advertimos que el ente supervisor reconoce estas áreas como sitios de Alta Seguridad, al demandar controles como:

- Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.
- Dotar a los equipos que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados

---

<sup>4</sup> Datos obtenidos luego de consultar a varios proveedores de circuitos cerrados de televisión con almacenamiento digital.

por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.

- En los equipos usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. (...)

Se nota claramente la necesidad de protección de la información de los clientes y la formalidad en la seguridad de las áreas donde se maneja tal información. Estas nuevas normas envían un mensaje muy claro a los Bancos: la información de los clientes es un recurso valioso y un tesoro que hay que cuidar con el rigor más extremo.

La sección 4.9 dedicada a Internet es mucho más específica en términos de medidas de seguridad requeridas para salvaguardar la información y operaciones de los clientes y usuarios. Se establecen aspectos como protocolos y algoritmos para comunicaciones seguras, tema que considera el cifrado de la información; las pruebas de vulnerabilidades tanto de dispositivos como medios de comunicación del canal, cuyos resultados deberán estar disponibles para la SFC cuando ésta los solicite; tiempo de inactividad, que cancelen la sesión y obliguen a nuevo proceso de autenticación; informar al cliente al inicio de cada sesión fecha y hora del último ingreso y la implementación de mecanismos para limitar el *phishing*, suplantación de sus páginas web, y envenenamiento del caché de su DNS – Sistema de nombre de dominio.

Esta sección es un gran resumen de un trabajo detallado de análisis de vulnerabilidades en aplicaciones web (como OWASP – *Open Web Application Security Project*, disponible en <http://www.owasp.org>) combinado con un proceso de revisión de potenciales amenazas y fallas orientados por metodologías de pruebas de penetración como OSSTM (*Open Source Security Testing Methodology*, disponible en <http://www.isecom.org/osstmm/>). En este tema de Internet, hubiese sido útil agregar un enlace adicional, un 4.9.7 que indicara algo como: “Considerar la utilización de herramientas, estrategias o metodologías de reconocida aceptación nacional e internacional en temas de riesgos y vulnerabilidades informáticas que permitan evaluar y afinar las medidas de seguridad vigentes para este canal”.

En el numeral 4.10 las organizaciones bancarias deben realizar formalmente un análisis de riesgos y controles antes de habilitar un nuevo canal. Los resultados de este ejercicio deberán ser informados a la junta directiva y los órganos de control de la organización. La SFC deberá conocer este ejercicio 15 días calendario antes de la fecha prevista para el inicio del mismo. Esta regulación deberá generar una cultura de administración del riesgo más formal en las áreas de tecnologías de información, ayudar al desarrollo de los sistemas de gestión de seguridad de las organizaciones y la especialización de las áreas de seguridad de la información, que contarán con mayores responsabilidades en este nuevo escenario normativo.

Ya en la sección 6, denominada obligaciones especiales por tipo de medio, resaltamos un elemento especial y de avanzada que exige la SFC a los Bancos, lo que implica un cambio en la manera como se percibe la seguridad de la información en los diferentes canales que se establezcan para ello. El numeral 6.11 establece:

“Ofrecer a sus clientes tarjetas débito y/o tarjetas crédito que manejen internamente cualquiera de los mecanismos de autenticación fuerte tales como: OTP – *One time passwords*, biometría, etc; dichas tarjetas deberán servir indistintamente para realizar transacciones en cajeros automáticos, en puntos de pago, en Internet y en sistemas de audio respuesta”

Esta norma reconoce que las contraseñas actuales (generalmente estáticas) que ofrecen los bancos para el acceso a sus servicios en los diferentes no son un mecanismo fuerte para proteger al usuario frente a algunas amenazas contra su información y seguridad de sus transacciones. Es decir, que si usted como ciudadano quiere tener acceso a un nivel de seguridad superior, la entidad vigilada le ofrecerá éstos servicios, los cuales tendrán un costo adicional por su uso. Un mejor nivel de seguridad necesariamente nos va a costar. Considere esto como una inversión, así como usted actualiza las guardas de su casa por una de mejor configuración y tecnología, la cual le va a representar una mayor confiabilidad, lo mismo sucede con la seguridad de las transacciones electrónicas.

Finalmente, la sección 7 que lleva por nombre análisis de vulnerabilidades, es una sección diseñada para las áreas encargadas de la seguridad informática de las organizaciones bancarias. Este numeral formaliza un ejercicio que todas las áreas de seguridad de la información deben hacer para establecer el nivel de riesgo real que se tiene en sus plataformas tecnológicas y detallar las fallas identificadas, así como los correctivos requeridos. Las pruebas de vulnerabilidades se pueden efectuar bien con hardware de propósito específico como con personal especializado en este sentido.

### **Conclusiones**

Como podemos ver la norma es un conjunto base de buenas prácticas de seguridad para las entidades financieras en Colombia y establece un referente fundamental para el desarrollo de la cultura de seguridad informática en Colombia. Así mismo, a pesar de que no lo dice explícitamente, adelantar todas las actividades previstas en esta circular requiere de personal especializado y formado para estas tareas, lo que sugiere la formación de un área de seguridad informática al interior de las organizaciones bancarias. Esta sugerencia tácita, es una excelente excusa para iniciar la reflexión interna de las organizaciones que lleve a la valoración de ese activo fundamental de las organizaciones del siglo XXI como lo es la información.

Esperemos pues que esta iniciativa de la SFC genere la dinámica de la seguridad informática representada en el buen combate contra la inseguridad de la información, no como la enemiga de la gestión estratégica del sector bancario, sino como el motivador y catalizador de iniciativas e innovaciones que permita al sector financiero y demás sectores productivos del país reconocer en los programas de protección de la información, la herramienta base para la generación de productos y servicios de alto valor.