LIBRO I.- NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

TITULO X.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS

CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO (incluido con resolución No JB-2005-834 de 20 de octubre del 2005)

SECCIÓN I.- ÁMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente norma son aplicables a las instituciones financieras públicas y privadas, al Banco Central del Ecuador, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros, a las cuales, en el texto de este capítulo se las denominará como instituciones controladas.

Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en el capítulo I "De la gestión integral y control de riesgos", las instituciones controladas observarán las disposiciones del presente capítulo.

ARTÍCULO 2.- Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

2.1 **Alta gerencia.-** La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

2.2 **Evento de riesgo operativo.-** Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

2.3 **Factor de riesgo operativo.-** Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de la información y eventos externos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.4 **Proceso.-** Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

2.5 **Insumo.-** Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

2.6 **Proceso crítico.-** Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

2.7 **Actividad.-** Es el conjunto de tareas;

2.8 **Tarea.-** Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y mesurable;

2.9 Procedimiento.- Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

2.10 Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad;

2.11 Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

2.12 Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio; (reformado con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

2.14 Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

2.15 Tecnología de la información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.16 Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones;

2.17 Instalaciones.- Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de la información; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.18 Responsable de la información.- Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidade**s**; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.19 Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

2.20 Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

2.21 Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

2.22 Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

2.23 Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

2.24 Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

2.25 Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

2.26 Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

2.27 Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

2.28 Encriptación.- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino;

2.29 Plan de continuidad.- Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.30 Administración de la continuidad.- Es un proceso permanente que garantiza la continuidad de las operaciones del negocio de las instituciones del sistema financiero, a través de la efectividad del mantenimiento del plan de continuidad; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.31 Eficacia.- Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

2.32 Eficiencia.- Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores;

2.33 Calidad de la información.- Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.34 Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.35 Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.36 Banca electrónica.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.37 Banca móvil.- Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de equipos celulares mediante los protocolos propios de este tipo de dispositivos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.38 Tarjetas.- Para efectos del presente capítulo, se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.39 Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios pueden efectuar transacciones con las instituciones del sistema financiero, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.40 Tarjeta inteligente.- Tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores y es capaz de proveer seguridad, principalmente en cuanto a la confidencialidad de la información de la memoria; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.41 Riesgo legal.- Es la probabilidad de que una institución del sistema financiero sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

2.42 Transacción.- Se refiere a las acciones realizadas por los clientes a través de canales electrónicos, tales como: consultas, transferencias, depósitos, retiros, pagos, cambios de clave, actualización de datos y otras relacionadas; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.43 Incidente de tecnología de la información.- Evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad significativa de comprometer las operaciones del negocio; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.44 Incidente de seguridad de la información.- Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

De acuerdo con lo dispuesto en el numeral 2 del artículo 18 del Código Civil, los términos utilizados en la definición de riesgo legal se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras, a menos de que tengan definiciones diferentes expresadas en la ley, reglamentos y demás normativa. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de la información y por eventos externos. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.41 del artículo 2. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 4.- Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

4.1 Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

4.1.1 Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

4.1.2 Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

4.1.3 Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a: (i) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (ii) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (iii) determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros; (iv) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (v) actualización y mejora continua a través del seguimiento permanente en su aplicación.

Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

Las instituciones controladas deberán mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

4.2 Personas.- Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

Dichos procesos corresponden a:

4.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;

4.2.2 Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos,

competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,

4.2.3 Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

4.3 Tecnología de la información.- Las instituciones controladas deben contar con la tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir políticas, procesos, procedimientos y metodologías que aseguren una adecuada planificación y administración de la tecnología de la información. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Dichas políticas, procesos, procedimientos y metodologías se referirán a: (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1 Con el objeto de garantizar que la administración de la tecnología de la información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente: (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia, a través de la asignación de recursos

para el cumplimiento de los objetivos tecnológicos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.2 En función del tamaño y complejidad de las operaciones, las entidades deben conformar el comité de tecnología, que es el responsable de planificar, coordinar y supervisar las actividades de tecnología. El directorio asumirá las responsabilidades del comité de tecnología en las entidades que decidieran no conformarlo. La Superintendencia de Bancos y Seguros podrá disponer la conformación de este comité, si las condiciones de tamaño y complejidad de la entidad lo amerita. (numeral incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Dicho comité debe estará integrado como mínimo por: un delegado del directorio, quien lo presidirá, el representante legal de la institución y el funcionario responsable del área de tecnología;

4.3.1.3 Un plan funcional de tecnología de la información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un (1) año), traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos institucionales propuestos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.4 Tecnología de la información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución, con su correspondiente portafolio de proyectos tecnológicos a ejecutarse en el corto, mediano y largo plazo; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.5 Políticas, procesos, procedimientos y metodologías de tecnología de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de la violación de éstas. (numeral sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Los procesos, procedimientos y metodologías de tecnología de la información deben ser revisados por el comité de tecnología y propuestos para la posterior aprobación del directorio o el organismo que haga sus veces;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos, procedimientos y metodologías, de tal forma que se asegure su implementación; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.7 Una metodología de administración de proyectos que considere al menos su planificación, ejecución, control y cierre, enfocada en la optimización de recursos y la gestión de riesgos. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2 Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente: (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.1 Procedimientos que establezcan las actividades y responsables de la operación y el uso de las instalaciones de procesamiento de información; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.2 Procedimientos de gestión de incidentes de tecnología de la información, que considere al menos su registro, priorización, análisis, escalamiento y solución; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.3 Inventario de la infraestructura tecnológica que considere por lo menos, su registro, responsables de uso y mantenimiento; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.4 Procedimientos de respaldo de información periódicos, acorde a los requerimientos de continuidad del negocio que incluyan la frecuencia de verificación, las condiciones de preservación y eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesto a los mismos riesgos del sitio principal. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3 Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

4.3.3.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.2 Un documento que refleje el alcance de los requerimientos funcionales; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.3 Un documento que refleje los requerimientos técnicos y la relación y afectación a la capacidad de la infraestructura tecnológica actual; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.4 Ambientes aislados con la debida segregación de accesos, para desarrollo, pruebas y producción, los cuales deben contar con la capacidad requerida para cumplir sus objetivos. Al menos se debe contar con dos ambientes: desarrollo y producción; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.5 Escaneo de vulnerabilidades en código fuente para identificar el nivel de riesgo del ambiente de la aplicación y en aplicaciones puestas en producción; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.6 Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.7 Procedimientos de control de cambios que considere su registro, manejo de versiones, segregación de funciones y autorizaciones e incluya los cambios emergentes; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.8 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.9 Procedimientos de migración de la información, que incluyan controles para garantizar las características de integridad, disponibilidad y confidencialidad. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las instituciones controladas deben contar al menos con: (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.1 Procedimientos que permitan la administración, monitoreo y registros de configuración de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.2 Un documento de análisis de la capacidad y desempeño de la infraestructura tecnológica que soporta las operaciones del negocio, que debe ser conocido y analizado por el comité de tecnología con una frecuencia mínima semestral. El documento debe incluir límites y alertas de al menos: almacenamiento, memoria, procesador, consumo de ancho de banda; y, para bases de datos: áreas temporales de trabajo, log de transacciones y almacenamiento de datos; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.3 Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio; e, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.4 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado, daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5 **Medidas de seguridad en canales electrónicos.-** Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el

cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas, éstas deberán cumplir como mínimo con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.1. Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.2. Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.3. Canales de comunicación seguros mediante la utilización de técnicas de encriptación acorde con los estándares internacionales vigentes; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.4. El envío de información de sus clientes relacionada con al menos números de cuentas y tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá ser enmascarada; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.5. La información confidencial que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación acordes con los estándares internacionales vigentes y deberá evaluarse con regularidad la efectividad del mecanismo utilizado; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.6. Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.7. Las instituciones del sistema financiero deberán utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información en todo momento debe estar encriptada; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.8. Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.9. Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones que impliquen movimiento de dinero a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberá constar: el registro de las cuentas a las cuales desea realizar transacciones monetarias, números de suministros de servicios básicos, números de telefonía fija y móvil, montos máximos por transacción diaria, semanal y mensual, entre otros. (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.10. Requerir a los clientes que el registro y modificación de la información referente a su número de telefonía móvil y correo electrónico, se realicen por canales presenciales, además no se debe mostrar esta información por ningún canal electrónico; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.11. Las instituciones del sistema financiero deben registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones. Para permitir transacciones desde direcciones IP y telefonía móvil de otros países se debe tener la autorización expresa del cliente; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.12. Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a los canales electrónicos, la clave de banca electrónica debe ser diferente de aquella por la cual se accede a otros canales electrónicos; (incluido con resolución No.

JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.13. Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus comportamientos transacciones que impliquen movimiento de dinero en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que impliquen movimiento de dinero que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.14. Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.15. Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.16. Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.17. Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.18. Mantener como mínimo durante doce (12) meses el registro histórico de todas las transacciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para transacciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión.

En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso del artículo 80 de la Ley General de Instituciones del Sistema Financiero; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.19. Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos.

Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.20. Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.21. Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.22. Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante sistemas de audio respuesta IVR), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.23. Las instituciones del sistema financiero deberán enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo, notificando el acceso y la ejecución de transacciones realizadas mediante cualquiera de

los canales electrónicos disponibles, o por medio de tarjetas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y sustituido con resolución No. JB-2014-3021 de 30 de julio del 2014)

4.3.5.24. Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.25. Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.26. Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los canales electrónicos ofrecidos por la entidad; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.5.27. Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.28. Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.5.29. En todo momento en donde se solicite el ingreso de una clave, ésta debe aparecer enmascarada; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.6. Cajeros automáticos.- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir con las disposiciones del artículo 40, del capítulo I “Apertura y cierre de oficinas en el país y en el exterior, de las instituciones financieras privadas y públicas sometidas al control de la Superintendencia de Bancos y Seguros”, del título II “De la organización de las instituciones del sistema financiero privado”**,** de este libro y con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013)

4.3.6.1. Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.6.2. La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.6.3. Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 l)

4.3.6.4. Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.6.5. Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013)

4.3.6.6. Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que se es”; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2013-2642 de 26 de septiembre del 2013)

4.3.6.7. Llevar a cabo campañas educativas para los usuarios acerca del uso, ubicación y medidas de seguridad pertinentes durante el uso del cajero, incluyendo la colocación de letreros alusivos a éstas en los recintos de los cajeros. (incluido con resolución No. JB-2013-2642 de 26 de septiembre del 2013 l)

4.3.7. Puntos de venta (POS y PIN Pad).- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.7.1 Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta

con la debida autorización; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.7.2 A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura; y, (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.7.3 Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8. Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente: (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.1 Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.3 Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.4 Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.6 Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.7 Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.8 La institución del sistema financiero deberá implementar mecanismos para detectar la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS); (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.8.9 La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.3.8.10 Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que se es”, considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una transacción, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.8.11 Para establecer las condiciones personales bajo las cuales los clientes realizarán sus transacciones por internet, tales como: matriculación de cuentas, definición de montos máximos, registro de números de teléfono celular, entre otros, que han sido definidos por la institución del sistema financiero, se debe validar o verificar la autenticidad del cliente a través de un canal diferente al de internet; (incluido con resolución No. JB-2014-3021 de 30 de julio del 2014 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.9. Banca móvil.- Las instituciones del sistema financiero que presten servicios a través de banca móvil deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.5 y 4.3.8; (incluido

con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.10. Sistemas de audio respuestas (IVR).- Las instituciones del sistema financiero que presten servicios a través de IVR deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.5 y 4.3.8; y, (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.11. Corresponsales no bancarios.- Las instituciones financieras controladas que presten servicios a través de corresponsales no bancarios deberán sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los subnumerales 4.3.5, 4.3.7 y 4.3.8. (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

4.4 Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 5.- En el marco de la administración integral de riesgos, establecido en la sección II "Administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", las instituciones controladas incluirán el proceso para administrar el riesgo operativo como un riesgo específico, el cual, si no es administrado adecuadamente puede afectar el logro de los objetivos de estabilidad a largo plazo y la continuidad del negocio.

El diseño del proceso de administración de riesgo operativo deberá permitir a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias.

El directorio u organismo que haga sus veces de las instituciones del sistema financiero aprobará las políticas, normas, principios y procesos básicos de seguridad y protección para sus empleados, usuarios, clientes, establecimientos, bienes y patrimonio, así como para el resguardo en el transporte de efectivo y valores. (incluido con resolución No. JB-2011-1851 de 11 de enero del 2011)

ARTÍCULO 6.- Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 4 del presente capítulo y adicionalmente, deberán contar con códigos de ética y de conducta formalmente establecidos; con la supervisión del directorio u organismo que haga sus veces y de la alta gerencia; con una sólida cultura de control interno; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de la información adecuada. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

ARTÍCULO 7.- Con la finalidad de que las instituciones controladas administren adecuadamente el riesgo operativo es necesario que agrupen sus procesos por líneas de negocio, de acuerdo con una metodología establecida de manera formal y por escrito, para lo cual deberán observar los siguientes lineamientos:

7.1 Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos le corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar; y,

7.2 Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo.

ARTÍCULO 8.- Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de la información y los eventos externos. (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Los tipos de eventos son los siguientes:

8.1 Fraude interno;

8.2 Fraude externo;

8.3 Prácticas laborales y seguridad del ambiente de trabajo;

8.4 Prácticas relacionadas con los clientes, los productos y el negocio;

8.5 Daños a los activos físicos;

8.6 Interrupción del negocio por fallas en la tecnología de la información; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

8.7 Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

En el anexo No. 1 se incluyen algunos casos de eventos de riesgo operativo, agrupados por tipo de evento, fallas o insuficiencias que podrían presentarse en las instituciones controladas y su relación con los factores de riesgo operativo.

Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

ARTICULO 9.- Dentro del proceso de identificación al que se refiere el artículo anterior, las instituciones deben adicionalmente determinar de manera puntual las fallas o insuficiencias de orden legal, de tal manera que les proporcione una visión clara sobre su exposición al riesgo legal, debiendo tener como referencia para el efecto los tipos de evento de riesgo operativo indicados en dicho artículo.

Las fallas o insuficiencias de orden legal deben ser establecidas por las instituciones de acuerdo con su propia percepción y perfil de riesgos, pero deben enfocar por lo menos los siguientes campos: actos societarios; gestión de crédito; operaciones del giro financiero;

actividades complementarias no financieras; y, cumplimiento legal y normativo, entendiéndolos dentro de las siguientes conceptualizaciones:

9.1 **Actos societarios**.- Son todos aquellos procesos jurídicos que debe realizar la institución en orden a ejecutar y perfeccionar las decisiones de la junta general de accionistas o de socios o representantes, según sea del caso, y del directorio o cuerpo colegiado que haga sus veces, necesarios para el desenvolvimiento societario de la institución del sistema financiero, atenta su naturaleza jurídica;

9.2 **Gestión de crédito**.- Es el conjunto de actividades que debe ejecutar la institución del sistema financiero relacionadas con el otorgamiento de operaciones crediticias. Se inicia con la recepción de la solicitud de crédito y termina con la recuperación del valor prestado, sus intereses y comisiones. Incluye la gestión de recuperación de cartera tanto judicial como extrajudicial, la misma que debe proseguir aún cuando la operación crediticia hubiere sido castigada;

9.3 **Operaciones del giro financiero**.- Es el conjunto de actividades o procesos que realiza la institución del sistema financiero para la ejecución de operaciones propias del giro financiero, distintas a la gestión de crédito;

9.4 **Actividades complementarias de las operaciones del giro financiero**.- Es el conjunto de actividades o procesos que debe ejecutar la institución del sistema financiero que sin ser propias del giro financiero, son necesarias para el cumplimiento y desarrollo de su objeto social; y,

9.5 **Cumplimiento legal y normativo.-** Es el proceso mediante el cual la institución del sistema financiero controla que sus actividades y sus operaciones se ajusten a las disposiciones legales y normativas vigentes, así como la capacidad de adecuarse rápida y efectivamente a nuevas disposiciones legales y normativas. (artículo incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 10.- Una vez identificados los eventos de riesgo operativo y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la institución, los niveles directivos están en capacidad de decidir si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos.

La identificación antes indicada permitirá al directorio u organismo que haga sus veces y a la alta gerencia de la entidad contar con una visión clara de la importancia relativa de los diferentes tipos de exposición al riesgo operativo y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, que entre otras, pueden ser: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencias y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda.

ARTÍCULO 11.- En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente, será necesario que adicionalmente las instituciones controladas conformen bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de riesgo operativo; fallas o insuficiencias incluidas las de orden legal; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que las instituciones controladas consideren necesaria y oportuna, para que a futuro se pueda estimar las

pérdidas esperadas e inesperadas atribuibles a este riesgo. (artículo reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 12.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las instituciones controladas cuenten con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.

ARTÍCULO 13.- El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente.

La función de auditoría interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo.

ARTÍCULO 14.- Las instituciones controladas deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna.

Los reportes deberán contener al menos lo siguiente:

14.1 Detalle de los eventos de riesgo operativo, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operativo y clasificados por líneas de negocio;

14.2 Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución; y,

14.3 Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Estos informes deben ser dirigidos a los niveles adecuados de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, entre otros.

SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO

ARTÍCULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio. (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:

15.1 La definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad;

15.2 Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad.

El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, al menos una vez cada trimestre, y sus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos.

El comité de continuidad del negocio debe tener al menos las siguientes responsabilidades:

15.2.1. Monitorear la implementación del plan y asegurar el alineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente;

.

15.2.2. Proponer cambios, actualizaciones y mejoras al plan;

.

15.2.3. Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos;

15.2.4. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,

15.2.5. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones;

15.3 Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.

El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados;

15.4 Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos;

15.5 Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas

de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso;

15.6 Realización de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una (1) vez al año;

15.7 Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento; e,

15.8 Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continúa del plan de continuidad del negocio.

ARTÍCULO 16.- El plan de continuidad del negocio debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente. (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

16.1 Escenarios de riesgos y procesos críticos cubiertos y alertas de los escenarios y procesos críticos no cubiertos por el plan;

16.2 Roles y responsabilidades de las personas encargadas de ejecutar cada actividad;

16.3 Criterios de invocación y activación del plan;

16.4 Responsable de su actualización;

16.5 Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal;

16.6 Tiempos máximos de interrupción y de recuperación de cada proceso;

16.7 Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas o para el restablecimiento de los procesos críticos de manera urgente;

16.8 Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros);

16.9 Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros);

16.10 Interacción con los medios de comunicación;

16.11 Comunicación con los grupos de interés;

16.12 Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alterno); y,

16.13 Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.

SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 17.- Las responsabilidades del directorio, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", de este título. (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Adicionalmente, el directorio tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

17.1 Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;

17.2 Aprobar las políticas y estrategias relacionadas con la administración y gestión del riesgo operativo que permitan el cumplimiento de las disposiciones establecidas en este capítulo;

17.3 Podrá delegar la aprobación de los procesos, procedimientos y metodologías para la gestión de procesos, personas, tecnología de la información y servicios provistos por terceros a la instancia que considere pertinente, la misma que debe velar que los mismos estén alineados al cumplimiento de las políticas y estrategias de la administración del riesgo operativo aprobadas por el directorio; y,

17.4 Aprobar el proceso, metodología y plan para la administración de la continuidad del negocio.

ARTÍCULO 18.- Las funciones y responsabilidades del comité de administración integral de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos". (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Adicionalmente, el comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

18.1 Evaluar y proponer para la aprobación del directorio las políticas para la administración del riesgo operativo;

18.2 Evaluar y proponer mejoras al proceso de administración de riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;

18.3 Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;

18.4 Evaluar y someter a aprobación del directorio el proceso, metodología y plan de continuidad del negocio a los que se refiere la sección IV, del este capítulo; asegurar su aplicabilidad; y, cumplimiento del mismo; y,

18.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de continuidad del negocio.

ARTICULO 19.- Las funciones y responsabilidades de la unidad de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos".

Adicionalmente, la unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

19.1 Diseñar las políticas y el proceso de administración del riesgo operativo;

19.2 Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de la información y los eventos externos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

19.3 Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de la información, especialmente aquellas relacionadas con la seguridad de la información; (sustituido con resolución No. JB-2008-1202 de 23 de octubre del 2008 y reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

19.4 Liderar el desarrollo, la aplicabilidad y cumplimiento del proceso y plan de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer el nombre de los líderes de las áreas que deban cubrir el plan de continuidad del negocio, para lo cual debe designar de manera formal, un responsable del proceso de la administración de la continuidad, el cual debe tener a su cargo, entre otras, las siguientes funciones: (reformado con resolución No. JB-2008-1202 de 23 de octubre del 2008 y sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

19.4.1 Proponer las políticas, procedimientos y metodologías para la administración de la continuidad del negocio, incluyendo la asignación de roles y responsabilidades;

19.4.2 Proponer cambios, actualizaciones y mejorar al plan de continuidad; e,

19.4.3 Informar al comité de continuidad los aspectos relevantes de la administración de la continuidad del negocio para una oportuna toma de decisiones; y,

19.5 Analizar, monitorear y evaluar los procedimientos de orden legal de la institución; y, en coordinación con las áreas legales, emitir informes que determinen su real exposición al riesgo legal, los cuales deben ser puestos en conocimiento del comité de administración integral de riesgos. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS (incluida con resolución No. JB-2014-2798 de 19 de febrero del 2014)

ARTÍCULO 20.- Para mantener un adecuado control de los servicios provistos por terceros, incluidos las instituciones de servicios auxiliares del sistema financiero, las instituciones controladas deberán contar con un proceso integral para la administración de proveedores de servicios que incluya las actividades de pre contratación, suscripción, cumplimiento y renovación del contrato, para lo cual deberán por lo menos cumplir con lo siguiente: (sustituido con resolución No. JB-2014-2798 de 19 de febrero del 2014)

20.1 Establecer políticas, procesos y procedimientos efectivos que aseguren una adecuada selección, calificación y evaluación de los proveedores, tales como:

20.1.1 Evaluación de la experiencia de la empresa o de su personal técnico en el mercado;

20.1.2 Desempeño de los proveedores en relación con los competidores;

20.1.3 Análisis de costo beneficio;

20.1.4 Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto;

20.1.5 Análisis de informes de auditoría externa, si los tuviere;

20.1.6 Respuesta del proveedor a consultas, solicitudes de presupuesto y de ofertas;

20.1.7 Capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos;

20.1.8 Capacidad logística del proveedor incluyendo las instalaciones y recursos humanos;

20.1.9 La reputación comercial del proveedor en la sociedad así como de sus accionistas;

20.1.10 Identificación de proveedores de servicios críticos; y,

20.1.11 La exigencia de planes de contingencias del proveedor para los servicio a ser contratados;

20.2 Establecer políticas, procesos y procedimientos efectivos que aseguren una adecuada contratación de servicios, que garantice que los contratos incluyan como mínimo lo siguiente:

20.2.1 Niveles mínimos de calidad del servicio acordado;

20.2.2 Garantías técnicas y financieras, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros;

20.2.3 Multas y penalizaciones por incumplimiento;

20.2.4 Personal suficiente y calificado para brindar el servicio en los niveles acordados;

20.2.5 Transferencia del conocimiento del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio;

20.2.6 La confidencialidad de la información y datos;

20.2.7 Derechos de propiedad intelectual del conocimiento, productos, datos e información, cuando aplique;

20.2.8 Definición del equipo de contraparte y administrador del contrato tanto de la institución del sistema financiero como del proveedor;

20.2.9 Definición detallada de los productos y servicios a ser entregados por el proveedor;

20.2.10 Cumplimiento por parte del proveedor de las políticas que establezca la institución del sistema financiero, las cuales deberán incluir al menos, la normativa expedida por la Superintendencia de Bancos y Seguros, aplicable en función del servicio a ser contratado; y,

20.2.11 Facilidades para la revisión y seguimiento del servicio prestado a las instituciones del sistema financiero, ya sea, por parte de la unidad de auditoría interna u otra área que la institución del sistema financiero designe, así como, por parte de los auditores externos.

20.3 Las instituciones del sistema financiero deberán aplicar metodologías para administrar los riesgos a los que se expone al contratar servicios provistos por terceros, particularmente de aquellos identificados como críticos;

20.4 Establecer políticas, procesos y procedimientos efectivos que aseguren un adecuado control y monitoreo de los servicios contratados, que incluyan como mínimo lo siguiente:

20.4.1 La evaluación, gestión y vigilancia de las actividades de prestación de los servicios contratados con terceros, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados; y,

20.4.2 El monitoreo de los riesgos inherentes, particularmente del riesgo operacional y legal respecto del funcionamiento de aquellos servicios provistos por terceros, para lo cual deberán mantener una matriz de riesgos y evidencias de la gestión de los mismos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

20.5 Contar con proveedores alternos de los servicios críticos calificados bajo las disposiciones de esta normativa, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un sólo proveedor; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

20.6 Si las instituciones del sistema financiero desean contratar la ejecución de los procesos productivos y/o servicios críticos en el exterior, deben notificar a la Superintendencia de Bancos y Seguros, adjuntando la documentación de respaldo que asegure el cumplimiento de este artículo. Además, las instituciones deben exigir al proveedor del servicio en el exterior, se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio; y, que los servicios objeto de contratación en el exterior sean sometidos anualmente a un

examen de auditoría independiente, por una empresa auditora de prestigio. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para cumplir con lo establecido en este capítulo, se deberá observar las disposiciones relativas a conflicto de intereses contenidas en el capítulo VIII "Principios de un buen gobierno corporativo", del título XIV "Código de transparencia y de derechos del usuario; y, en el capítulo IX "Principios de un buen gobierno corporativo para las instituciones financieras públicas", del título XXIII "De las disposiciones especiales para las instituciones financieras publicas", de este libro.

SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN (incluida con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

ARTÍCULO 21.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos: (artículo incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

21.1 Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información.

El comité debe estar conformado como mínimo por: el miembro del directorio delegado al comité integral de riesgos, quien lo presidirá, el representante legal de la institución y el funcionario responsable de la seguridad de la información.

El organismo de control puede requerir la creación del comité y de una unidad especializada para la gestión de los sistemas de seguridad de la información en las instituciones del sistema financiero que por su complejidad y volumen de negocio lo requieran, así como en aquellas que no hubieren puesto en práctica de una manera adecuadas las disposiciones de este sección;

21.2 Establecer las políticas, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la institución, así como las consecuencias de violación de éstas.

Los procesos, procedimientos y metodologías de seguridad de la información deben ser revisados por el comité de seguridad de la información y en caso de no tener dicho comité, por el comité de administración integral de riesgos; y,

21.3 Difundir las políticas de seguridad de la información y propiciar actividades de concienciación y entrenamiento en estos temas.

ARTÍCULO 22.- Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente: (artículo incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

22.1 Disponer de un inventario de la información con la designación de sus propietarios, mismos que deben tener como mínimo las siguientes responsabilidades:

22.1.1 Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y criticidad para la entidad, éste debe ser revisado periódicamente con la finalidad de mantenerlo actualizado;

22.1.2 Definir y revisar periódicamente las restricciones y clasificaciones de acceso tomando en cuenta las políticas de control de acceso aplicables;

22.1.3 Autorizar los cambios funcionales a las aplicaciones; y,

22.1.4 Monitorear el cumplimiento de los controles establecidos;

22.2 Identificar y documentar los requerimientos mínimos de seguridad para cada tipo de información, con base en una evaluación de los riesgos que enfrenta la institución, aplicando la metodología de gestión de riesgo operativo de la entidad; y, con los controles de seguridad de la información;

22.3 Establecer procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios;

22.4 Mantener segregación de funciones y responsabilidades para mitigar los riesgos de modificación no autorizada o no intencionada o un mal uso de los activos de la organización;

22.5 Definir los procedimientos de gestión de cambios en los sistemas de información, hardware y software base, elementos de comunicaciones, entre otros, que consideren su registro, manejo de versiones, segregación de funciones y autorizaciones, e incluyan los cambios emergentes;

22.6 Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores, y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad del cambio;

22.7 Determinar los sistemas de control y autenticación tales como: sistemas de detección de intrusos (IDS), sistemas de prevención intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros, para evitar accesos no autorizados, inclusive de terceros y, ataques externos especialmente a la información crítica;

22.8 Gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la institución, por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las instituciones deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

22.9 Controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso;

22.10 Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal o de terceros;

22.11 Un procedimiento para el control de accesos a la información que considere la concesión; administración de derechos y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios;

22.12 Establecer un procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas, intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;

22.13 Implementar procedimientos que permitan contar con pistas de auditoría a nivel de aplicativos y bases de datos que registren los cambios realizados a la información crítica de la entidad. Los administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades

22.14 Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible;

22.15 Considerar en la definición de requerimientos para nuevos sistemas o mantenimiento, aquellos relacionados con la seguridad de la información;

22.16 Establecer procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos su registro, priorización, análisis, escalamiento y solución;

22.17 Definir y mantener un sistema de registros históricos que permitan verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información; y,

22.18 Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información, a fin de tomar acciones orientadas a mejorarlo."

SECCIÓN VIII.- DISPOSICIONES GENERALES

ARTÍCULO 23.- El manual que contempla el esquema de administración integral de riesgos, de que trata el artículo 15 del capítulo I "De la gestión integral y control de riesgos", incluirá la administración del riesgo operativo.

ARTÍCULO 24.- La Superintendencia de Bancos y Seguros podrá disponer la adopción de medidas adicionales a las previstas en el presente capítulo, con el propósito de atenuar la exposición al riesgo operativo que enfrenten las instituciones controladas.

Adicionalmente, la Superintendencia de Bancos y Seguros podrá requerir a las instituciones controladas, la información que considere necesaria para una adecuada supervisión del riesgo operativo.

ARTÍCULO 25.- En caso de incumplimiento de las disposiciones contenidas en este capítulo, la Superintendencia de Bancos y Seguros aplicará las sanciones correspondientes de conformidad con lo establecido en el capítulo I "Normas para la aplicación de sanciones pecuniarias", del título XVI.

ARTICULO 26.- Los casos de duda y los no contemplados en el presente capítulo, serán resueltos por Junta Bancaria o el Superintendente de Bancos y Seguros, según el caso.

SECCIÓN IX.- DISPOSICIONES TRANSITORIAS

PRIMERA.- Las disposiciones reformadas de esta norma deberán cumplirse conforme al siguiente cronograma: (disposición transitoria sustituida con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

1. Hasta el 31 de diciembre del 2014, debe cumplirse con los numerales: 4.3.5.1, 4.3.5.2, 4.3.5.4, 4.3.5.5, 4.3.5.7, 4.3.5.9, 4.3.5.13, 4.3.5.23, 4.3.5.28, 4.3.5.29, 4.3.6.1, 4.3.6.6, 4.3.7.2, 4.3.8.10, 4.3.8.11; (reformado con resolución No. SB-2014-1201 de 30 de diciembre del 2014)

2. Hasta junio del 2015, debe cumplirse con los numerales: 4.3.6.3 y 4.3.7.3; y, (incluido con resolución No. SB-2014-1201 de 30 de diciembre del 2014)

3. Hasta el 31 de diciembre del 2015, debe cumplirse con los todos los numerales de los siguientes numerales: 4.3.1, 4.3.2, 4.3.3, 4.3.4; con los numerales: 4.3.5.3, 4.3.5.10, 4.3.5.11, 4.3.5.12, 4.3.5.24; con las disposiciones normativas reformadas y contenidas en los artículos: 15, 16, 17, 18, 19, 21 y 22.

SEGUNDA.- Las instituciones del sistema financiero para dar cumplimiento a las disposiciones de la sección VI, de este capítulo, tendrán un plazo de trescientos sesenta (360) días, a partir de la publicación de esta reforma en el Registro Oficial. (reformada con resolución No. JB-2008-1223 de 18 de diciembre del 2008 y sustituida con resolución No. JB-2009-1491 de 26 de octubre del 2009, resolución No. JB-2011-1983 de 26 de agosto del 2011, resolución No. JB-2012-2358 de 25 de octubre del 2012 y resolución No. JB-2014-2798 de 19 de febrero del 2014)

TERCERA.- Las instituciones del sistema financiero deben reportar el nivel de cumplimiento de las disposiciones referidas en la primera y segunda transitoria en las siguientes fechas: 31 de enero del 2015, 31 de julio del 2015 y 31 de diciembre del 2015. (incluida con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

CUARTA.- El Banco del Instituto Ecuatoriano de Seguridad Social - BIESS implementará las disposiciones del numeral 4.3 Tecnología de la información" del artículo 4, conforme al siguiente cronograma: (incluida con resolución No. JB-2014-3033 de 6 de agosto del 2014)

1. Las disposiciones relacionadas con los factores: procesos, administración del riesgo operativo, servicios provistos por terceros y los numerales de canales electrónicos: 4.3.8.2, 4.3.8.3, 4.3.8.4, 4.3.8.11, 4.3.8.12, 4.3.8.18, 4.3.11.2, deben ser implementados hasta diciembre de 2014;

2. Las disposiciones relacionadas con el factor personas y los numerales de canales electrónicos: 4.3.8.1, 4.3.8.25, 4.3.8.16, 4.3.8.15, 4.3.8.7, 4.3.8.6, 4.3.11.10, 4.3.11.3, 4.3.11.9 y 4.3.11.11, deben ser implementados hasta junio de 2015; y,

3. Las disposiciones normativas relacionadas con el factor tecnología de la información, deben ser implementadas hasta el mes de diciembre de 2015.

Adicionalmente, las disposiciones relacionadas con la continuidad del negocio, deben ser implementadas hasta el mes de octubre de 2016.

El ente de control en cualquier momento puede realizar una supervisión in situ a fin de verificar el avance del cumplimiento de acuerdo al cronograma enviado por la entidad.

ANEXO No.1

IDENTIFICACIÓN DE EVENTOS, FALLAS O INSUFICIENCIAS Y FACTORES DEL RIESGO OPERATIVO

LINEAS DE NEGOCIO:

TIPOS DE EVENTOS	FALLAS O INSUFICIENCIAS	FACTORES DE RIESGO DE OPERATIVO	NUMERO DE VECES (FRECUENCIA)	EFECTO CUANTITATIVO PERDIDA PRODUCIDA
FRAUDE INTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Operaciones no reveladas adecuadamente	Mal diseño de proceso	Procesos		
Operaciones no registradas intencionalmente	Inadecuada selección de personal	Personas		
Inadecuada utilización de información confidencial	Ausencia de control en los perfiles de usuario	Tecnología de Información		
Apropiación indebida de activos	Inadecuada segregación de funciones	Personas		
Falsificación	Inexistencia de controles	Procesos		
Destrucción maliciosa de activos	Inadecuadas medidas de seguridad	Procesos		
Evasión de impuestos	Falta de ética	Personas		
Robo	Inadecuada segregación de funciones	Personas		
FRAUDE EXTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Robo	Falta de seguridades físicas	Procesos		
Emisión de cheques sin fondos	Inadecuada capacitación del Personal	Personas		
Perjuicios por intrusión o ataque de terceros	Falta de seguridades en la teconología de información para prevenir ataques de terceros	Tecnología de Información		
Falsificación	Falta de seguridades de la tecnología de información	Tecnología de Información		
PRACTICAS DE EMPLEO Y SEGURIDAD DEL AMBIENTE DE TRABAJO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Reclamos por compensación e indemnización al personal	Inadecuada contratación del personal	Procesos		
Violación de las normas de salud o seguridad	Falta de difusión y comunicación de políticas	Personas		
Todo tipo de discriminación	Inadecuada política de administración de personal	Personas		
PRACTICAS RELACIONADAS CON CLIENTES, LOS PRODUCTOS Y EL NEGOCIO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Mal manejo de la información confidencial de clientes	Falta de defininición de políticas y procedimientos	Procesos		
Prácticas contrarias a la competencia, prácticas inadecuadas de negociación	Falta de defininición de políticas	Personas		
Actividades no autorizadas	Incursión en nuevas actividades sin considerar riesgos	Procesos		
Abuso de información privilegiada a favor de la institución	Falta de ética	Personas		
DAÑOS A LOS ACTIVOS FÍSICOS PROVOCADOS POR				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Terrorismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Vandalismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Pérdidas por desastres naturales	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
INTERRUPCIÓN DEL NEGOCIO Y FALLAS EN LOS SISTEMAS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Fallas en el software	Deficiencia en el proceso de desarrollo y/o implantación	Tecnología de Información		
Fallas en el hadware	Falta de previsión de la capacidad de los recursos para el volumen de operaciones. Falta de mantenimiento preventivo de los servidores centrales	Tecnología de Información		
Problemas de telecomunicación	Caída en los enlaces de telecomunicaciones	Tecnología de Información		
Cortes en los servicios públicos	Falta de planes de contingencia	Eventos externos		
DEFICIENCIAS EN LA EJECUCIÓN DE PROCESOS, EN EL PROCESAMIENTO DE OPERACIONES Y EN LAS RELACIONES CON PROVEEDORES Y OTROS EXTERNOS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Errores en el ingreso de los datos	Falta de controles de ingreso de datos en las aplicaciones	Tecnología de Información		
Falla en la administración de colaterales	Inadecuada segregación de funciones	Procesos		
Documentación legal incompleta	Falta de verificación del área legal	Procesos		
Acceso no aprobado a las cuentas de clientes	Proceso no definido	Procesos		
Disputa con los proveedores	Deficiencias en la contratación	Procesos		
Incumplimiento en la entrega de la información hacia terceros	Falta de controles en el proceso de envio de información	Procesos		

NOTAS:

1.- En el presente Anexo constan ejemplos de eventos agrupados por tipo, los cuales consideran los lineamientos establecidos por el Comité de Basilea

2.- Los eventos que se produjeren que no esté alineados a los tipos de eventos especificados en este Anexo, deberán constar bajo la denominación "información no alineada, concepto bajo el cual constarán únicamente por excepción.

3.- Frecuencia, se refiere al número de veces que se repite cada evento