REFORMA CODIFICACION SUPERINTENDENCIA DE BANCOS, LIBRO PRIMERO TOMO I, Resolución de la Superintendencia de Bancos 810, Registro Oficial Suplemento 123, 31/10/2017

Resolución de la Superintendencia de Bancos 771
Registro Oficial Suplemento 325 de 12-sep.-2018
Estado: Vigente

TITULO III.- DE LA ORGANIZACION

DETALLE HISTORICO DE LAS RESOLUCIONES EXPEDIDAS EN EL TITULO III:

Nota: Para leer Detalle, ver Registro Oficial Suplemento 123 de 31 de Octubre de 2017, página 76.

TITULO III.- DE LA ORGANIZACION

CAPITULO I.- NORMA DE CONTROL PARA LA APERTURA Y CIERRE DE OFICINAS Y CANALES DE LAS ENTIDADES BAJO EL CONTROL DE LA SUPERINTENDENCIA DE BANCOS (expedida mediante resolución No. SB-2016-940, de 6 de octubre de 2016)

SECCION I.- DEFINICIONES

Art. 1.- Los términos utilizados en la presente norma, deberán entenderse de acuerdo con las siguientes definiciones:

a. AGENCIA.- Oficina que depende de la matriz o de una sucursal; y, puede efectuar todas las operaciones y servicios establecidos en el Código Orgánico Monetario y Financiero, autorizados por el directorio de la entidad financiera; no está autorizada a llevar contabilidad;
b. BANCA ELECTRONICA.- Servicio ofrecido por los bancos que permite a sus clientes efectuar ciertas operaciones bancarias desde cualquier medio electrónico que cuente con acceso a internet;
c. CANALES ELECTRONICOS.- Se refiere a todas las vías o formas a través de las cuales los clientes o usuarios financieros pueden efectuar transacciones con las entidades financieras, 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 PINPAD), sistemas de audio- respuesta (IVR), banca electrónica, banca móvil y corresponsales no bancarios, entre otros,

d. CORRESPONSALES NO BANCARIOS.- Son canales mediante los cuales las entidades de los sectores financieros público y privado, bajo su entera responsabilidad, pueden prestar sus servicios a través de terceros que estén conectados a la entidad financiera mediante sistemas de transmisión de datos, previamente autorizados por el organismo de control, identificados y que cumplan con todas las condiciones de control interno, seguridades físicas y de tecnología de información, entre otras.

Podrán actuar como corresponsales no bancarios las personas naturales o jurídicas que, a través de instalaciones propias o de terceros, atiendan al público, las mismas que deben estar domiciliadas en el país;

Nota: Literal d reformado por artículo 2 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

e. MATRIZ.- Oficina principal, constituida como domicilio legal de la entidad financiera y que debe constar en el estatuto social, puede realizar cualquiera de las operaciones y servicios establecidos

en el Código Orgánico Monetario y Financiero. Incluye a la sucursal principal de las entidades financieras del exterior domiciliadas en el Ecuador;
f. OFICINA MOVIL.- Establecimiento que depende orgánicamente de la matriz o de una sucursal, autorizada a movilizarse, utilizando para ello un vehículo con capacidad y seguridad para transportar valores; y, puede efectuar todas las operaciones y servicios determinados en el artículo 6 de la presente norma, así como la aprobación y desembolso de créditos y apertura de cuentas, conforme lo autorizado por el directorio de la entidad financiera;
g. OFICINA ESPECIAL.- Establecimiento que depende orgánicamente de la matriz o de una sucursal, con una duración indefinida y puede realizar únicamente las operaciones determinadas en et artículo 6, de esta norma;
h. OFICINA TEMPORAL.- Establecimiento que depende orgánicamente de la matriz o de una sucursal y funciona en ferias nacionales o internacionales, exposiciones o cualquier tipo de evento, con el objeto exclusivo de entregar información al público de los servicios y productos ofertados por la entidad financiera. El tiempo de duración de funcionamiento de estas oficinas será notificado a la Superintendencia de Bancos con quince días de anticipación y su funcionamiento no podrá ser mayor a treinta (30) días;
i. SUCURSAL.- Oficina que depende de la matriz, que puede tener bajo su control a agencias u otro tipo de oficinas; lleva contabilidad propia y puede efectuar todas las operaciones y servicios establecidos en el Código Orgánico Monetario y Financiero y autorizados por el directorio. De ser el caso, puede centralizar la contabilidad de las oficinas bajo su control;
j. VENTANILLA DE EXTENSION DE SERVICIOS.- Funciona dentro de las instalaciones de las personas jurídicas que son clientes de las entidades financieras y puede prestar los servicios previstos en el artículo 7 de esta norma, acordados en los correspondientes contratos. Pueden ser usuarios de esta ventanilla, únicamente, los funcionarios, empleados, obreros, estudiantes y proveedores de la empresa pública o privada que la solicite, por lo que no podrá tener acceso directo al público en general.

CAPITULO V
NORMA DE CONTROL PARA LA GESTION DEL RIESGO OPERATIVO

Nota: Capítulo, secciones y artículos sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Nota: Capítulo reformado por artículo 6 de Resolución de la Superintendencia de Bancos No. 66, publicada en Registro Oficial 184 de 20 de Febrero del 2018 .
Nota: Resolución 66 derogada por Resolución de la Superintendencia de Bancos No. 865, publicada en Registro Oficial 337 de 28 de Septiembre del 2018 .

SECCION I.- AMBITO, DEFINICIONES Y ALCANCE

Art. 1.- Las disposiciones de la presente norma son aplicables a las entidades de los sectores financieros público y privado, cuyo control le compete a la Superintendencia de Bancos, a las cuales, en el texto de esta norma se las denominará entidades controladas.

Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en la presente norma, las entidades controladas observarán las disposiciones de la "Política para la gestión integral y administración de riesgos de las entidades de los sectores financieros público y privado", emitida por la Junta de Política y Regulación Monetaria y Financiera y la "Norma de control para la gestión integral y administración de riesgos de las entidades de los sectores financieros público y privado" emitida por la Superintendencia de Bancos.

Nota: Sección y artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 2.- Para efectos de la aplicación de las disposiciones de la presente norma, se considerarán las siguientes definiciones:

a. Actividad.- Es el conjunto de tareas que ejecutan las entidades controladas;
b. Actividades complementarias de las operaciones del giro financiero.- Es el conjunto de tareas que deben ejecutar las entidades controladas, que sin ser propias del giro financiero, son necesarias para el cumplimiento y desarrollo de su objeto social;
c. Actos societarios.- Son todos aquellos procesos que debe realizar la entidad controlada en orden a ejecutar y perfeccionar las decisiones de la junta general de accionistas, del directorio y de aquellos que requieren de resolución por parte de la autoridad competente, necesarios para el desenvolvimiento societario;
d. Administración de la continuidad del negocio.- Es un proceso permanente que garantiza la continuidad de las operaciones de las entidades controladas, a través del mantenimiento efectivo del plan de continuidad del negocio;
e. 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, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;
f. Alfanumérico.- Es el conjunto de caracteres conformado por letras y números;
g. Aplicación informática.- 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;
h. Banca electrónica.- Son los servicios suministrados por las entidades controladas a los clientes y/o usuarios, a través de protocolos de internet, indistintamente del dispositivo tecnológico del cual se acceda;
i. Banca móvil.- Son los servicios suministrados por las entidades controladas a los clientes y/o usuarios, a través de aplicaciones propias de los dispositivos móviles mediante los protocolos de estos equipos;
j. Cajeros automáticos (ATM).- Son máquinas conectadas informáticamente a una entidad controlada que permite efectuar al cliente ciertas transacciones;
k. Canales electrónicos.- Se refiere a todas las vías o formas a través de las cuales los clientes y/o usuarios pueden efectuar transacciones con las entidades controladas, 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), banca electrónica, banca móvil, u otros mecanismos electrónicos similares;
l. Centro de procesamiento de datos.- Es la infraestructura que permite alojar los recursos relacionados con la tecnología que admite el procesamiento, almacenamiento y transmisión de la información;
m. Cifrar.- 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;
n. Computación en la nube.- Es la provisión de servicios informáticos accesibles a través de la internet, estos pueden ser de infraestructura, plataforma y/o software;
o. Confiabilidad.- Es el atributo de que la información es la apropiada para la administración de la entidad, la ejecución de transacciones y el cumplimiento de sus obligaciones;
p. Confidencialidad.- Es el atributo de que sólo el personal autorizado accede a la información preestablecida;
q. Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las entidades controladas están sujetos;
r. Corresponsales no bancarios (CNB).- Son canales mediante los cuales las entidades de los sectores financieros público y privado, bajo su entera responsabilidad, pueden prestar sus servicios a través de terceros que estén conectados a la entidad financiera mediante sistemas de transmisión de datos, previamente autorizados por el organismo de control, identificados y que cumplan con todas las condiciones de control interno, seguridades físicas y de tecnología de información, entre otras;
s. Cumplimiento legal y normativo.- Es el proceso mediante el cual la entidad controlada vigila 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;
t. Datos.- Es cualquier forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;
u. Disponibilidad.- Es el atributo de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios que satisfagan sus necesidades;
v. Evento de riesgo operativo.- Es el hecho que deriva en pérdidas para las entidades controladas, originado por fallas o insuficiencias en los factores de riesgo operativo;
w. Estándar TIA-942.- Guía que proporciona una serie de recomendaciones y directrices para la instalación de las infraestructuras de centros de procesamiento de datos en los aspectos de: telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico;
x. Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son: procesos, personas, tecnología de la información y eventos externos;
y. Gestión de crédito.- Es el conjunto de actividades que debe ejecutar la entidad controlada relacionadas con las operaciones crediticias. Se inicia con la recepción de la solicitud de crédito y termina con la recuperación del valor prestado, sus intereses y cargos. Incluye la gestión de recuperación de cartera tanto judicial como extrajudicial, la misma que debe proseguir aun cuando la operación crediticia hubiere sido castigada;
z. 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;

aa. Incidente de tecnología de la información.- Es el evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad de comprometer las operaciones del negocio;
bb. Incidente de seguridad de la información.- Es el evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información;
cc. Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;
dd. Insumo.- Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;
ee. Integridad.- Es el atributo de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;
ff. 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;
gg. Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;
hh. Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos, bases de datos, sistemas operativos y demás elementos tecnológicos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;
ii. Plan de continuidad del negocio.- Es el conjunto de procedimientos orientados a mantener la operatividad de la entidad, a pesar de eventos inesperados;
jj. POS y PIN Pad.- Son dispositivos de hardware y/o software fijos o móviles ubicados en puntos de venta que permiten realizar transacciones con tarjetas;
kk. Procedimiento.- Es la forma específica para llevar a cabo una actividad o un proceso;
ll. Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente interno o externo utilizando recursos de la entidad;
mm. Proceso crítico.- Es el conjunto de actividades indispensables para la continuidad del negocio y las operaciones de la entidad controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo;
nn. Propietario 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 responsabilidades;
oo. Punto de recuperación objetivo (RPO).- Es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo;

pp. Seguridad de la información.- Es el conjunto de medidas que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información;
qq. Seguridades lógicas.- Son los mecanismos de protección en el uso del software, de los datos, procesos y programas, que permiten el acceso autorizado de los usuarios a la información;
rr. Sistema de audio respuesta (IVR).- Es un sistema automatizado de respuesta interactiva, orientado a entregar o recibir información a través del teléfono;
ss. Tarea.- Es el conjunto de pasos que conducen a un resultado final visible y mesurable;
tt. 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 y comunicaciones, entre otros;
uu. Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;
vv. Tarjeta con chip.- Es la tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores;
ww. Transacciones.- Son movimientos que realizan los clientes y/o usuarios a través de los canales que brindan las entidades; y pueden ser monetarias y no monetarias;

i. Transacciones monetarias.- Son las que implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: transferencias, depósitos, retiros, pagos, recargas de telefonía móvil, entre otras;
ii. Transacciones no monetarias.- Son las que no implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: consultas, cambios de clave, personalización de condiciones para realizar transacciones, actualización de datos, entre otras;

xx. Tiempo de recuperación objetivo (RTO).- Es el período de tiempo transcurrido después de un incidente, para reanudar una actividad o recuperar los recursos antes de que la entidad controlada genere pérdidas significativas; y,
yy. TIER III.- Certificación o clasificación de los centros de datos que permite el mantenimiento concurrente, con una disponibilidad de 99.982% al año, y un tiempo de parada de 1.6 horas, e incluye redundancia en sus componentes de infraestructura así como fuentes alternativas de electricidad y refrigeración en caso de emergencia.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 3.- Para efectos de la presente norma, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas por eventos derivados de fallas o insuficiencias en los factores de: procesos, personas, tecnología de la información y por eventos externos.

El riesgo operativo incluye el riesgo legal, pero excluye los riesgos sistémico, estratégico y de reputación.

El riesgo legal es la probabilidad de que las entidades controladas sufran pérdidas debido a que los activos y contingentes se encuentren expuestos a situaciones de mayor vulnerabilidad; que sus pasivos puedan verse incrementados más allá de los niveles esperados, o 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.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771,

publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SECCION II.- ADMINISTRACION DEL RIESGO OPERATIVO

Art. 4.- En el marco de la administración integral de riesgos, las entidades controladas definirán políticas, procesos, procedimientos y metodologías para la administración del riesgo operativo como un riesgo específico, considerando su objeto social, tamaño, naturaleza, complejidad de sus operaciones y demás características propias.

La administración del riesgo operativo deberá permitir a las entidades controladas identificar, medir, controlar, mitigar y monitorear su exposición a este riesgo en el desarrollo de sus negocios y operaciones.

Nota: Sección y Artículo sustituidos por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 5.- Las entidades controladas deben identificar los riesgos operativos por línea de negocio, tipo de evento, factor de riesgo operativo y las fallas o insuficiencias, utilizando para el efecto una metodología debidamente documentada y aprobada que incorporará la utilización de herramientas que se ajusten a las necesidades de la entidad, tales como: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

Los tipos de eventos de riesgo son los siguientes:

a. Fraude interno;
b. Fraude externo;
c. Prácticas laborales y seguridad del ambiente de trabajo;
d. Prácticas relacionadas con los clientes, los productos y el negocio;
e. Daños a los activos físicos;
f. Interrupción del negocio por fallas en la tecnología de la información; y,
g. Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 6.- Una vez identificados los riesgos operativos y las fallas o insuficiencias en relación con los factores de este riesgo, se debe medir el riesgo determinando su probabilidad de ocurrencia e impacto para la entidad, permitiendo al directorio y a la alta gerencia contar con una visión clara de la exposición al riesgo operativo, con el objetivo de alertarlos en la toma de decisiones y acciones, de manera que el directorio esté en capacidad de decidir si mitiga, transfiere, asume o evita el riesgo reduciendo sus efectos.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 7.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las entidades controladas cuenten con planes de mitigación formalmente establecidos y validados periódicamente, mediante la revisión de estrategias y políticas; actualización o modificación de procesos y procedimientos establecidos; implementación o modificación de límites de riesgo; implementación, o modificación de controles; plan de continuidad del negocio; revisión de términos de pólizas de seguro contratadas; contratación de servicios provistos por terceros; u otros, según corresponda. 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.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 8.- Las entidades controladas deben realizar un monitoreo permanente de las actividades y contar con un esquema organizado de reportes que permita tener información suficiente, pertinente y oportuna para la toma de decisiones, el cual debe incluir como mínimo:

a. Reporte de indicadores claves de riesgo operativo que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;
b. Reporte del grado de cumplimiento de los planes de mitigación;
c. Reporte de la matriz y mapas de riesgos operativos, que incluya como mínimo: línea de negocio, proceso, subproceso, tipo de evento, riesgo / evento de riesgo, factor de riesgo operativo, fallas o insuficiencias, impacto inicial, probabilidad inicial, frecuencia, riesgo inherente/ inicial, controles existentes/ planes de mitigación, impacto final, probabilidad final y riesgo residual.

La Superintendencia de Bancos a través de circular determinará el formato de reporte de la matriz de riesgos operativos.

Además, la entidad controlada en los informes trimestrales dirigidos al comité de administración integral de riesgos, debe incluir los niveles de exposición al riesgo operativo, la evolución de los riesgos reflejados en sus respectivos indicadores clave de riesgos; la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas; el grado de cumplimiento de los planes de mitigación; y, conclusiones y recomendaciones; 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, y metodologías, entre otros.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 9.- En razón que la administración del riesgo operativo constituye un proceso continuo y permanente; y, para una gestión efectiva del riesgo, las entidades controladas deben conformar bases de datos centralizadas, que permitan registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo incluidos los de orden legal, de seguridad de la información y de continuidad del negocio, el efecto cuantitativo de pérdida producida y estimada así como la frecuencia y probabilidad, y otra información que las entidades controladas consideren necesaria y oportuna, para que se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo. La administración de la base de datos es responsabilidad de la unidad de riesgo operativo.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SECCION III.- FACTORES DEL RIESGO OPERATIVO

Art. 10.- Con el propósito de minimizar la probabilidad de incurrir en pérdidas atribuibles al riesgo operativo, las entidades controladas deben administrar los siguientes factores:

a. Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las entidades controladas adoptarán un enfoque por procesos, tomando como referencia la norma ISO 9001, y deben:

i. Definir el mapa de procesos de conformidad con la estrategia y las políticas adoptadas, mismos que deben ser agrupados de la siguiente manera:

- Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices y políticas a los demás, procesos cuya responsabilidad compete al directorio y la alta gerencia para

poder cumplir con los objetivos institucionales. Se refieren a la planificación estratégica, la administración integral de riesgos, entre otros;
- Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permiten ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,
- 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.

ii. Agrupar sus procesos por líneas de negocio, de acuerdo con una metodología establecida de manera formal, para lo cual deben observar los siguientes lineamientos:

- Asignar los procesos productivos 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,
- Asignar los procesos gobernantes y habilitantes a las líneas de negocio donde intervengan. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar una metodología formalmente establecida para esta asignación.

iii. Definir formalmente una metodología para el diseño, control, actualización, seguimiento y medición de los procesos.

La metodología debe referirse por lo menos a:

- Descripción y diagramación en secuencia lógica y ordenada de las actividades, tareas, y controles;
- Determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento. Para el efecto se deben establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir el alcance, mantener el contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas;
- Identificación de los clientes internos y externos;
- Productos y servicios que genera;
- Difusión y comunicación de los procesos buscando garantizar su total aplicación; y,
- Actualización y mejora continua a través del seguimiento permanente en su aplicación, al menos una vez al año para los procesos productivos; y, para los procesos gobernantes y habilitantes de soporte y de apoyo al menos una vez cada dos años.

iv. 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, línea de negocio, fecha de aprobación y fecha de actualización.
v. Mantener separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas, como aquellas tareas cuya ejecución por una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.
vi. Definir indicadores para cada uno de los procesos que le permitan a la entidad medir la efectividad de los mismos.

b. Personas.- Las entidades controladas deben administrar el capital humano de forma que les permita gestionar los riesgos asociados a este factor.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las entidades controladas deben:

i. Definir formalmente políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal al servicio de la entidad, soportados técnicamente y ajustados a las

disposiciones legales, de manera que aseguren la planificación y administración del capital humano, mismos que corresponden a:

- Incorporación.- Comprende la planificación de necesidades, el reclutamiento y la selección, la contratación e inducción de nuevo personal. Las entidades controladas deben evaluar su organización con el objeto de definir el personal mínimo 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.
- Permanencia.- Comprende la creación de condiciones laborales idóneas mediante la planificación y ejecución de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; un sistema de evaluación del desempeño que permita medir y estimular la gestión del personal de la entidad y a su vez aplicar incentivos que motiven la adhesión a los valores institucionales; identificar los puestos críticos y el personal clave de la entidad y definir el personal de reemplazo en el caso de ausencia temporal o definitiva, con la finalidad de dar continuidad a las operaciones del negocio.
- Desvinculación.- Comprende la planificación de la salida del personal por causas regulares o irregulares a través de la preparación de aspectos jurídicos para llegar al finiquito y a la finalización de la relación laboral.

ii. Mantener un archivo digital centralizado con información actualizada del capital humano, misma que deberá detallar: formación académica y experiencia; forma y fechas de reclutamiento, selección y contratación; información histórica sobre los eventos de capacitación en los que ha participado; cargos que ha desempeñado en la entidad; resultados de evaluaciones de desempeño realizadas; fechas y causas de separación del personal que se ha desvinculado; con la finalidad de permitir la toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.

c. Tecnología de la información.- Las entidades controladas deben contar con 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, esté disponible para la toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo tecnológico, las entidades controladas deben:

i. Contar con un área de tecnología de la información en función del tamaño y complejidad de las operaciones, y conformar el comité de tecnología, que es el responsable de evaluar, y supervisar las actividades estratégicas de carácter tecnológico.

Dicho comité estará integrado como mínimo por: un miembro del directorio, quien lo presidirá, el representante legal de la entidad, el funcionario responsable del área de riesgo operativo y el funcionario responsable del área de tecnología, quienes no podrán delegar su participación. Mantendrá un reglamento en donde se establezcan sus funciones y responsabilidades. Las reuniones de este comité se realizarán al menos trimestralmente dejando evidencia de las decisiones adoptadas.

El comité de tecnología sesionará con la mitad más (1) uno de sus integrantes, cuyo quorum no deberá ser menor a tres (3) y las decisiones serán tomadas por mayoría de votos. El presidente del comité tendrá voto dirimente.

ii. Con el objeto de garantizar que la administración de la tecnología de la información soporte los requerimientos de operación actuales y futuros de la entidad, debe contar al menos con lo siguiente:

- El apoyo y compromiso formal del directorio, a través de la aprobación de un plan estratégico de

tecnología de la información alineado con el plan estratégico institucional; y, un plan operativo anual que establezca las actividades a ejecutar en el corto plazo, traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos tecnológicos propuestos; y,
- Políticas, procesos, procedimientos y metodologías de tecnología de la información, alineados a los objetivos y actividades de la entidad, así como las consecuencias de su incumplimiento.

Las políticas, procesos, procedimientos y metodologías de tecnología de la información deben ser revisados y aceptados por el comité de tecnología y propuestos para la posterior aprobación del directorio; deben ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento.

iii. Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de las entidades controladas, se debe implementar al menos lo siguiente:

- Procedimientos que establezcan las actividades y responsable de la operación y el uso de los centros de datos, que incluyan controles que eviten accesos no autorizados;
- Procedimientos de gestión de incidentes y problemas de tecnología de la información, que considere al menos su registro, priorización, análisis, escalamiento y solución; y,
- Procedimientos de respaldo de información periódicos, acorde a los requerimientos legales y de continuidad del negocio, que incluyan: la frecuencia de verificación, eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesta a los mismos riesgos del sitio principal y mantenga las condiciones físicas y ambientales necesarias para su preservación y posterior recuperación.

iv. Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las entidades controladas deben implementar:

- Una metodología que permita la administración y control del ciclo de vida de desarrollo y mantenimiento de aplicaciones, que describa las etapas del proceso, la documentación entregable en cada una de ellas, estándares de desarrollo y aseguramiento de la calidad y considere al menos lo siguiente:

- Requerimientos funcionales aprobados por el área solicitante;
- Requerimientos técnicos y el análisis de la relación y afectación a la capacidad de la infraestructura tecnológica actual, aprobados por el área técnica;
- Técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades;
- Levantamiento y actualización de la documentación técnica y de usuario de las aplicaciones de la entidad;
- Aseguramiento de la calidad de software que incluya pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados, así como la verificación del cumplimiento de estándares de desarrollo definidos por la entidad, aspectos que deben ser ejecutados por personal independiente al área de desarrollo y mantenimiento de software;
- Controles para el paso a producción y versionamiento de las aplicaciones, que considere su registro y autorizaciones respectivas e incluya los cambios emergentes;
- Seguimiento post-producción que permita verificar que el sistema puesto en producción funciona de manera estable;
- Para los casos de migración de información, la entidad debe determinar y aplicar controles para garantizar las características de integridad, disponibilidad y confidencialidad; y,
- En caso de que la entidad controlada contrate el servicio de desarrollo de software o adquiera un sistema informático, debe verificar que el proveedor cumple con las disposiciones descritas en los numerales precedentes.

v. Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las entidades controladas deben implementar al menos:

- Infraestructura que soporta los procesos críticos con la redundancia necesaria para evitar puntos únicos de falla; de la cual se debe mantener el inventario y respaldos de la configuración actualizada e informes de su mantenimiento periódico; en el caso de los enlaces de comunicación, debe considerar que la trayectoria de los enlaces principal y alterno sean diferentes;
- Procedimientos que permitan la administración y monitoreo de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas;
- 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 las alertas que hayan sobrepasado los límites 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;
- Para los casos de migración de la plataforma tecnológica crítica, controles para garantizar la continuidad del servicio, previa notificación a la Superintendencia de Bancos;
- Centros de procesamiento de datos, principal y alterno, 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. La ubicación del centro de procesamiento de datos alterno no debe estar expuesta a los mismos riesgos del sitio principal;
- 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; y,
- Para el caso de infraestructura provista por terceros, asegurar el cumplimiento de las disposiciones incluidas en los numerales precedentes.

vi. Con la finalidad de asegurar que los cambios a los aplicativos e infraestructura que soportan las operaciones, estén debidamente autorizados, documentados, probados, y aprobados por el propietario de la información previo a su paso a producción, las entidades controladas deben implementar procedimientos de control de cambios que consideren al menos lo siguiente:

- Mecanismos mediante los cuales se iniciarán las solicitudes de cambio;
- Una metodología para analizar, dar prioridad y aprobar las solicitudes de cambio;
- Evaluación del impacto de los cambios sobre los aplicativos e infraestructura de producción;
- Mecanismos de marcha atrás, de modo que el impacto por cualquier falla pueda ser minimizado;
- Librerías de desarrollo separadas de las librerías de producción, para evitar que una versión de prueba pueda contener código no autorizado;
- Mecanismos que aseguren que los cambios a los aplicativos y a su documentación, se realizan sobre las versiones fuente de los elementos en producción, y que los cambios realizados al código de las aplicaciones corresponden a aquellos solicitados por el propietario de la información;
- El responsable de aseguramiento de la calidad supervisa el mantenimiento de versiones de programa, código fuente o registros de configuración de la infraestructura, para garantizar su integridad;
- El responsable del aseguramiento de la calidad debe realizar conjuntamente con el propietario de información, las pruebas y certificación sobre los cambios para garantizar que: ejecuten las funciones requeridas, que la funcionalidad y desempeño existente no se vean afectadas por el cambio, que no se hayan generado riesgos de seguridad debido al cambio y que se cuente con toda la documentación actualizada; una vez concluidas exitosamente las pruebas, se debe registrar la aprobación del cambio;
- Mecanismos para garantizar que el paso de programas desde el ambiente de desarrollo a pruebas y de producción, sea realizado por un grupo independiente a los programadores; y,
- Procedimientos de cambios de emergencia para casos excepcionales en donde no sea posible seguir el proceso completo de control de cambios que incluya su posterior regularización y que permitan asegurar que no se compromete la integridad del sistema e infraestructura.

d. Eventos externos.- En la administración del riesgo operativo, las entidades 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 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.

i. Administración de la Continuidad del Negocio.- Las entidades controladas deben establecer un proceso de administración de la continuidad del negocio, que permita planificar, mantener y mejorar la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:

- Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: un miembro del directorio, quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las unidades de: riesgos, tecnología de la información, seguridad de la información, talento humano, continuidad del negocio quien actuará como secretario, los máximos representantes de cada una de las áreas relacionadas con los procesos críticos de la entidad; y, auditoría interna sólo con voz. Mantendrá un reglamento en donde se establezcan sus funciones y responsabilidades. Las reuniones de este comité se realizarán al menos trimestralmente.

El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, 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:

- Velar por la permanente administración de la continuidad del negocio;
- Monitorear la implementación del plan de continuidad del negocio y asegurar el alineamiento de éste con la metodología;
- Proponer para la revisión y aceptación del comité de administración integral de riesgos, el plan de continuidad del negocio y sus actualizaciones;
- Revisar el presupuesto del plan de continuidad del negocio y ponerlo en conocimiento del comité de administración integral de riesgos;
- Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,
- Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad del negocio;

Las funciones del comité de Continuidad del Negocio podrán ser asumidas por el Comité de Administración Integral de Riesgos, dependiendo del tamaño de la entidad y complejidad de las operaciones y previa notificación y aceptación del organismo de control;

- Definición de políticas, estrategias, objetivos, metodología, planes operativos y presupuesto para la administración de la continuidad del negocio;
- Análisis de impacto que tendría una interrupción de los procesos que soportan los productos y servicios de la entidad. Para ello, deben aplicar los parámetros para la identificación de los procesos críticos, su punto de recuperación objetivo y tiempos de recuperación objetivo definidos por el negocio; una vez identificados los procesos críticos, deben determinar las dependencias internas y externas; y, recursos de soporte para estos procesos, incluyendo tecnología, personal, proveedores, y otras partes interesadas.

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;

- Identificación de 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;
- Evaluación y selección de estrategias de continuidad por cada proceso crítico que permitan mantener su operatividad, 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, información necesaria para el proceso; proveedores y aplicativos relacionados;
- Procedimientos 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 vez al año; las pruebas deben incluir el alcance y el detalle de los aspectos a probar así como las conclusiones y recomendaciones obtenidas como resultado de su ejecución;
- Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan de continuidad del negocio; e,
- Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continua del plan de continuidad del negocio.

ii. Plan de continuidad del negocio.- Las entidades controladas deben contar con un plan de continuidad del negocio que considere como mínimo lo siguiente:

- Escenarios de riesgos y procesos críticos cubiertos por el plan;
- Tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO) de cada proceso crítico;
- Estrategias de continuidad por cada proceso crítico con el detalle de al menos lo siguiente: el personal asociado al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento, información vital para el proceso y cómo acceder a ella (información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros); proveedores y aplicativos relacionados;
- Procedimientos operativos que incluyan las acciones para trasladar las actividades de la entidad controlada a ubicaciones transitorias alternativas y para restablecer los procesos críticos de manera urgente; para lo cual deben establecer un centro alterno de operaciones que no esté expuesto a los mismos riesgos del sitio principal;
- Procedimientos de comunicaciones que incluyan: las estrategias de comunicación con el personal involucrado, sus familiares y contactos de emergencia, con información tal como: direcciones, teléfonos, correos electrónicos, entre otros; interacción con los medios de comunicación; y, comunicación con los grupos de interés;
- Procedimientos de emergencias que describan las acciones a ejecutar para preservar la seguridad del personal;
- Plan de recuperación de desastres que detalle los procedimientos tecnológicos de restauración en una ubicación remota de los servicios de tecnología de la información, mismos que deben estar dentro de los parámetros establecidos en el plan de continuidad del negocio, 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;
- Roles y responsabilidades de las personas encargadas de ejecutar cada actividad en los procedimientos operativos, de comunicaciones, de emergencia y plan de recuperación de desastres;
- Criterios de invocación y activación del plan de continuidad del negocio; y,
- Responsable de la actualización del plan de continuidad de negocio.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SECCION IV.- RIESGO LEGAL

Art. 11.- Con la finalidad de gestionar el riesgo legal y minimizar la probabilidad de incurrir en pérdidas por este tipo de riesgo, las entidades controladas identificarán, medirán, controlarán, mitigarán y monitorearán los eventos que podrían ocasionar la materialización del riesgo legal de acuerdo con su propia percepción y perfil de riesgos.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .
Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 814, publicada en Registro Oficial 322 de 7 de Septiembre del 2018 .

Art. 12.- Las áreas de asesoría jurídica de las entidades controladas tendrán atribuciones formales para gestionar el riesgo legal y contarán con el personal capacitado y con la debida experiencia, en relación al tamaño y complejidad de las operaciones de la entidad.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .
Nota: Artículo sustituido por artículo 2 de Resolución de la Superintendencia de Bancos No. 814, publicada en Registro Oficial 322 de 7 de Septiembre del 2018 .

SECCION V.- ADMINISTRACION DE PROYECTOS

Art. 13.- Con el objeto de administrar los proyectos institucionales, las entidades controladas deben:

a. Determinar funciones y responsables de la administración de proyectos, considerando como mínimo lo siguiente:

i. Desarrollo de políticas, procesos, procedimientos; y, una metodología basada en mejores prácticas o estándares para la administración de proyectos;
ii. Capacitar al personal de la entidad sobre el proceso y metodología de administración de proyectos; y,
iii. Monitorear el cumplimiento de las políticas, procesos, procedimientos y metodología.

b. Implementar una metodología institucional de administración de proyectos que considere al menos las etapas de inicio, planificación, ejecución, monitoreo y control, y cierre de los proyectos; enfocados en la optimización de los recursos y la gestión de los riesgos, que involucre:

i. Definición del acta de constitución, el alcance, los interesados y entregables por etapas;
ii. Gestión del cronograma, los recursos humanos, costos y las adquisiciones;
iii. Administración de la calidad, los riesgos, la comunicación y actividades de monitoreo; y,
iv. Acta de cierre.

c. Implementar un repositorio centralizado con las seguridades necesarias para almacenar la documentación resultante de cada etapa de los proyectos.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SECCION VI.- SERVICIOS PROVISTOS POR TERCEROS

Art. 14.- Para mantener el control de los servicios provistos por terceros, incluidas las empresas de servicios auxiliares del sistema financiero, las entidades controladas deben implementar un proceso integral para la administración de proveedores de servicios que incluya las actividades previas a la contratación, suscripción, cumplimiento y renovación del contrato, para lo cual deben por lo menos cumplir con lo siguiente:

a. Para las actividades previas a la contratación, las entidades controladas deben establecer e

implementar políticas, procesos y procedimientos que aseguren la evaluación, calificación y selección de los proveedores, tales como:

i. Evaluación de la experiencia de la empresa y de su personal;
ii. Evaluación financiera para asegurar la viabilidad de la empresa durante todo el período de contratación previsto;
iii. Análisis de informes de auditoría externa, si los tuviere;
iv. Evaluación de la capacidad del servicio, instalación y soporte e historial del desempeño en base a los requisitos de la entidad controlada;
v. Evaluación de la capacidad logística de la empresa, incluyendo las instalaciones y recursos humanos;
vi. Análisis de la reputación comercial de la empresa en la sociedad así como de sus accionistas; y,
vii. La existencia de planes de contingencia de la empresa para los servicios a ser contratados y que soportan los procesos críticos de la entidad controlada.

b. Establecer políticas, procesos y procedimientos que aseguren la contratación de servicios en función de los requerimientos de la entidad controlada, y garanticen que los contratos incluyan como mínimo las siguientes cláusulas:

i. Niveles mínimos de calidad del servicio acordado;
ii. Garantías financieras y técnicas, tales como: buen uso del anticipo, fiel cumplimiento del contrato, buen funcionamiento y disponibilidad del servicio, entre otros;
iii. Multas y penalizaciones por incumplimiento;
iv. Detalle del personal suficiente y calificado para brindar el servicio en los niveles acordados;
v. Transferencia del conocimiento del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio esencialmente en aquellos definidos como críticos;
vi. Confidencialidad de la información y datos;
vii. Derechos de propiedad intelectual, cuando aplique;
viii. Definición del equipo de contraparte y administrador del contrato tanto de la entidad controlada como del proveedor;
ix. Definición detallada de los productos y servicios a ser entregados por el proveedor;
x. Cumplimiento por parte del proveedor de las políticas que establezca la entidad controlada, las cuales deben incluir al menos, la norma expedida por la Superintendencia de Bancos, aplicable en función del servicio a ser contratado; y,
xi. Facilidades para la revisión y seguimiento del servicio prestado a las entidades controladas, por parte de la unidad de auditoría interna u otra área que éstas designen, así como de los auditores externos y la Superintendencia de Bancos.

c. Administrar los riesgos a los que se exponen al contratar servicios provistos por terceros, particularmente de aquellos que soportan los procesos críticos;
d. Establecer políticas, procesos y procedimientos que aseguren el control y monitoreo de los servicios contratados, mediante la evaluación, gestión y vigilancia de los mismos, a fin de garantizar que se cumplan en todo momento con los niveles mínimos de servicio acordados;
e. Contar con proveedores alternos de los servicios que soportan a los procesos críticos, que tengan la capacidad de prestar el servicio para mitigar el riesgo de dependencia en un sólo proveedor;
f. Para el caso de contratación de servicios de infraestructura, plataforma y/o software, conocido como computación en la nube, adicionalmente las entidades controladas deben:

i. Informar a la Superintendencia de Bancos sobre el detalle de los servicios a ser contratados que incluya el análisis de los riesgos operativos, legales, tecnológicos, de seguridad y continuidad a los que se exponen al adoptar este servicio; así como los controles para mitigarlos;
ii. Los centros de procesamiento de datos principal y/o alterno, contratados en la nube deben haber sido implementados siguiendo el estándar TIA-942 y contar como mínimo con la certificación TIER III para diseño, implementación y operación y así garantizar la disponibilidad de los servicios brindados; y,
iii. El proveedor de servicios en la nube debe contar como mínimo con certificación ISO 27001 en

seguridad de la información para los servicios ofertados.

Si los servicios provistos por terceros son de carácter financiero, estos están sujetos al cumplimiento de la normativa que emita la Junta de Política y Regulación Monetaria y Financiera y la Superintendencia de Bancos, en lo que corresponda.

Para contratar la ejecución de los procesos productivos y/o servicios que soportan los procesos críticos en el exterior, deben notificar a la Superintendencia de Bancos, adjuntando la documentación de respaldo que asegure el cumplimiento de este artículo, así como el detalle de los servicios contratados. Además, las entidades 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.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SECCION VII.- SEGURIDAD DE LA INFORMACION

Art. 15.- 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 entidades controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y contar al menos con:

a. Funciones y responsables de la seguridad de la información que permitan cumplir con los criterios de confidencialidad, integridad y disponibilidad de la información, acorde al tamaño y complejidad de los procesos administrados por el negocio.

Las entidades controladas deben conformar un comité de seguridad de la información que se encargue de evaluar, y supervisar el sistema de gestión de seguridad de la información.

El comité debe estar conformado como mínimo por: el miembro del directorio quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las unidades de: riesgos y seguridad de la información. Mantendrá un reglamento en donde se establezcan sus funciones y responsabilidades. Las reuniones de este comité se realizarán al menos trimestralmente dejando evidencia de las decisiones adoptadas.

El comité de seguridad sesionará con la mitad más uno de sus integrantes, cuyo quórum no deberá ser menor a tres (3) y las decisiones serán tomadas por mayoría de votos. El presidente del comité tendrá voto dirimente.

b. Un área independiente y especializada con personal capacitado y experiencia en gestión de seguridad de la información, acorde al tamaño y complejidad de sus operaciones, que lidere el establecimiento, implementación, operación, monitoreo, mantenimiento y mejora continua del sistema de gestión de seguridad de la información de la entidad que debe mantener la independencia funcional del: área de tecnología, riesgos, áreas del negocio y función de auditoría.

Nota: Sección y Artículo sustituidos por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 16.- Las entidades controladas deben establecer, implementar, operar, monitorear, mantener y mejorar un sistema de gestión de seguridad de la información que incluya al menos lo siguiente:

a. Alcance del sistema de gestión de seguridad de la información;
b. Políticas, objetivos, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación, alineados a los objetivos y actividades de la

entidad, así como las consecuencias de su incumplimiento.

Las políticas, procesos, procedimientos y metodologías de seguridad de la información deben ser revisados y aceptados por el comité de seguridad de la información; y, propuestos para la posterior aprobación del directorio; así como ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento;

c. Inventario de activos de información, con su clasificación en términos de: valor, requerimientos legales, sensibilidad y criticidad para la entidad, propietario, custodio y ubicación;
d. La designación de los propietarios de los activos de información, que deben tener como mínimo las siguientes responsabilidades:

i. Clasificar los activos de información y revisar periódicamente el inventario de activos de información, con la finalidad de mantenerlo actualizado;
ii. Definir y revisar periódicamente las restricciones y accesos a los activos de información, tomando en cuenta las políticas de control de acceso aplicables; y,
iii. Autorizar los cambios funcionales a las aplicaciones y modificaciones a la información a través de accesos directos a la base de datos.

e. Identificación y documentación de los requerimientos y controles mínimos de seguridad para cada activo de información, con base en una evaluación de los riesgos que enfrenta la entidad, aplicando la metodología de gestión de riesgo operativo;
f. Plan de seguridad de la información que permita la implementación de los controles identificados y acciones de mejora;
g. Información que permita verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información;
h. Monitoreo con una frecuencia al menos semestral, del cumplimiento y efectividad de los controles establecidos y generar informes dirigidos al comité de seguridad de la información;
i. Evaluación al menos una vez al año, del desempeño del sistema de gestión de la seguridad de la información, considerando los resultados de: auditorias de seguridad, gestión de incidentes de seguridad, monitoreo de los controles, resultados de las evaluaciones de riesgos, sugerencias, retroalimentación de las partes interesadas, entre otros aspectos; a fin de tomar acciones orientadas a mejorarlo. El resultado de estas evaluaciones así como las acciones de mejora deben ser conocidas y aprobadas por el comité de seguridad de la información; y,
j. Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información, la unidad responsable de la seguridad de la información debe implementar:

i. 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;
ii. Procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios;
iii. Procedimientos para el control de accesos a la información que considere la concesión; administración de usuarios 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, tanto de aplicativos, software base, red, dispositivos de seguridad perimetral, bases de datos, entre otros. También se deberá controlar el acceso de los proveedores a la información de la entidad;
iv. Procedimientos para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para las cuales han sido autorizados;
v. 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;
vi. Procedimientos para el uso, protección y tiempo de vida de las llaves criptográficas utilizadas para

cifrar la información;
vii. Técnicas de cifrado sobre la información que lo requiera como resultado del análisis de riesgos de seguridad;
viii. Políticas y controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia; y, para instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso;
ix. La realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la entidad, 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 entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;
x. Con base en un análisis de riesgos, realizar la segmentación de la red de datos y la implementación de sistemas de control y autenticación tales como: sistemas de prevención de 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;
xi. Procedimientos para la definición de requerimientos de seguridad de la información para nuevos sistemas o su mantenimiento;
xii. Escaneo automatizado de vulnerabilidades en código fuente para mitigar los riesgos de seguridad de las aplicaciones previo a su liberación, y de aquellas que se encuentran en producción;
xiii. Procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos: reporte de eventos, su evaluación, registro de incidentes, comunicación, priorización, análisis, respuesta y recolección de evidencias; y,
xiv. 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.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SECCION VIII.- SEGURIDAD EN CANALES ELECTRONICOS

Art. 17.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles y mecanismos para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad de la información de los usuarios así como los bienes de los clientes a cargo de las entidades controladas, éstas deben cumplir como mínimo con lo siguiente:

a. Las entidades controladas deben 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;
b. 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; se debe generar informes trimestrales dirigidos al comité de seguridad;
c. Canales de comunicación seguros mediante la utilización de técnicas de cifrado acorde con los estándares internacionales vigentes;
d. Realizar como mínimo una vez al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por canales electrónicos; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de los canales, se deberá efectuar una prueba adicional.

Las pruebas de vulnerabilidad y penetración deben ser efectuadas por personal independiente a la

entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

Los informes de las pruebas de vulnerabilidad deben estar a disposición de la Superintendencia de Bancos, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior;

e. 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;
f. 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 cifrado acordes con los estándares internacionales vigentes y deberá evaluarse con regularidad la efectividad del mecanismo utilizado;
g. Las entidades controladas deben 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 entidad;
h. Las entidades controladas deben 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 cifrada;
i. 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;
j. Ofrecer a los clientes y/o usuarios los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones monetarias a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad y se debe validar o verificar la autenticidad del cliente a través de métodos de autenticación fuerte;

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; y, montos máximos por transacción diaria;

k. 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, o bajo condiciones de seguridad que incluyan métodos de autenticación fuertes tales como biometría facial o de huella dactilar, o a través de call center previa validación de la identidad del cliente; además no se debe mostrar en texto claro esta información por ningún canal electrónico;
l. Para permitir transacciones desde el exterior por cualquier canal electrónico y tarjetas las entidades controladas deben tener la notificación expresa del cliente a través de llamada telefónica, página web, presencial u otro canal, señalando el período y los países en los cuales realizará sus transacciones;
m. Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez al año de las claves de acceso a los canales electrónicos, la clave de banca electrónica y banca móvil debe ser diferente de aquella por la cual se accede a otros canales electrónicos;
n. Las entidades deben levantar procedimientos de control y mecanismos que permitan establecer el perfil de los clientes sobre sus comportamientos transaccionales 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 monetarias que no correspondan a los perfiles definidos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;

o. 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 intentos de acceso fallido. Además, se deben 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;
p. Las entidades controladas deben mantener sincronizados todos los relojes de sus sistemas de información y dispositivos que estén involucrados con el uso de canales electrónicos;
q. 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 entidad controlada de origen y destino, número de transacción, número de teléfono y correo electrónico al que se notificaron las transacciones y claves de una sola vez; además, 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 artículo 225, sección 7, capítulo 3, título II, del Código Orgánico Monetario y Financiero;
r. 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, mediante los aplicativos y bases de datos. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta debe ser enmascarada o codificada por personal independiente al área de desarrollo. Todos estos procedimientos deben estar debidamente documentados en los manuales respectivos.

Además, la entidad debe 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 debe conservarse por lo menos por doce (12) meses;

s. Las entidades controladas deben poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) u otro medio, para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana;
t. Mantener por lo menos durante doce 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; o, se reporten emergencias bancarias; para lo cual se deben establecer procedimientos que permitan validar de manera segura la identidad del cliente. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales;
u. Las entidades controladas deben enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo, notificando la ejecución de transacciones monetarias realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas;
v. Las tarjetas emitidas por las entidades controladas deben contar con microprocesador o chip; y, deben adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo;
w. 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;
x. 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;
y. En todo momento en donde se solicite el ingreso de una clave, ésta debe aparecer enmascarada; y,
z. Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las entidades controladas deben implementar en sus canales electrónicos.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 18.- Cajeros automáticos.- Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las entidades controladas deben cumplir con las disposiciones de la "Norma de Control para la apertura y cierre de oficinas y canales de las entidades bajo el control de la Superintendencia de Bancos" y con lo siguiente:

a. Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben cifrar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento;
b. La entidad controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la entidad controlada a la que pertenece;
c. Los cajeros automáticos deben ser capaces de procesar la información de tarjetas con chip;
d. Los cajeros automáticos deben estar instalados con los estándares de seguridad definidos en las políticas de la entidad controlada, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad;
e. Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una 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 deben ser ejecutados por personal independiente, capacitado y con experiencia; y,
f. Para la ejecución de transacciones monetarias de clientes, se deben 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".

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 19.- 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 entidades controladas deben cumplir como mínimo con lo siguiente:

a. 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;
b. A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones monetarias 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,
c. Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas con chip.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 20.- Banca electrónica.- Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las entidades controladas que ofrezcan servicios por medio de este canal electrónico deben cumplir como mínimo con lo siguiente:

a. Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades 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 cifrado de los datos transmitidos acordes con los estándares internacionales vigentes;
b. Implementar mecanismos de control, y monitoreo que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las entidades controladas;
c. Enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro

mecanismo, notificando el acceso a la banca electrónica;
d. 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;
e. Informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica;
f. 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);
g. 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. El nombre de usuario y clave de acceso deben combinar caracteres alfanuméricos con una longitud mínima de seis (6) caracteres; y,
h. Para la ejecución de transacciones monetarias, se deben implementar métodos de autenticación fuerte que contemplen por lo menos dos (2) de tres (3) 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. Para la ejecución de transacciones monetarias a cuentas registradas como usuales por el cliente, las entidades controladas deben validar la autenticidad del cliente al menos en las seis (6) primeras transacciones por cada cuenta; mientras que para el caso de cuentas no registradas por el cliente se debe solicitar siempre el segundo factor de autenticación adoptado.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 21.- Banca móvil.- Las entidades controladas que presten servicios a través de banca móvil deben sujetarse en lo que corresponda a las medidas de seguridad dispuestas en canales electrónicos y banca electrónica de esta norma e implementar mecanismos que permitan la ejecución de transacciones desde dispositivos autorizados únicamente.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 22.- Sistemas de audio respuestas (IVR).- Las entidades controladas que presten servicios a través de IVR deben sujetarse en lo que corresponda a las medidas de seguridad dispuestas en canales electrónicos y banca electrónica de esta norma; y,

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

Art. 23.- Corresponsales no bancarios.- Las entidades controladas que presten servicios a través de corresponsales no bancarios deben sujetarse en lo que corresponda a las medidas de seguridad dispuestas en los canales electrónicos, banca electrónica, POS y PIN Pad de esta norma.

Nota: Artículo sustituido por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

DISPOSICIONES GENERALES

PRIMERA.- Las entidades controladas contratarán anualmente con las compañías de seguro privado pólizas de los ramos autorizados por el organismo de control pertinente, que incluyan coberturas que aseguren a las entidades contra fraudes generados a través de: sistemas de cómputo, programas electrónicos de computadoras, datos y medios electrónicos, virus de computadoras, comunicaciones electrónicas o telefax, transmisiones electrónicas, valores electrónicos y similares, como mínimo ante los siguientes riesgos:

a. Revelación ilegal de bases de datos;
b. Interceptación ilegal de datos;

c. Transferencia electrónica del activo patrimonial; y,
d. Ataque a la integridad a los sistemas informáticos.

Nota: Disposición sustituida por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SEGUNDA.- La Superintendencia de Bancos, como resultado de las evaluaciones que realice, podrá disponer la adopción de medidas adicionales a las previstas en la presente norma, con el propósito de reducir la exposición al riesgo operativo que enfrenten las entidades controladas.

Nota: Disposición sustituida por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

TERCERA.- El ente de control en cualquier momento puede realizar una supervisión in situ a fin de verificar la implementación de la presente norma.

Nota: Disposición sustituida por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

CUARTA.- Los casos de duda y los no contemplados en la presente norma, serán resueltos por la Superintendencia de Bancos.

Nota: Disposición sustituida por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

DISPOSICIONES TRANSITORIAS

PRIMERA.- Las siguientes disposiciones deben cumplirse en el plazo de ciento ochenta (180) días posteriores a la publicación de esta norma en el Registro Oficial:

a. Los artículos: 12 y 13;
b. Los sub numerales: i., iii. y vi., de la letra a.; sub numeral ii., de la letra b.; y sub numerales i. y vi. de la letra c, del artículo 10; y letra f. del artículo 14; y,
c. La sub viñeta novena, de la viñeta primera, del sub numeral iv, de la letra c, del artículo 10.

Nota: Disposición dada por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .

SEGUNDA.- Las siguientes disposiciones deben cumplirse en el plazo de trescientos (300) días posteriores a la publicación de esta norma en el Registro Oficial:

a. La sección VII "Seguridad de la información"
b. Primera disposición general;
c. Los sub numerales i. y ii., de la letra d. "Eventos externos", del artículo 10;
d. La letra l., del artículo 17; y,
e. Las viñetas primera y quinta, del sub numeral v, de la letra c, del artículo 10.

Nota: Disposición dada por artículo 1 de Resolución de la Superintendencia de Bancos No. 771, publicada en Registro Oficial Suplemento 325 de 12 de Septiembre del 2018 .