ACUERDO SUGEF 18-16

REGLAMENTO SOBRE GESTIÓN DEL RIESGO OPERATIVO

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante artículo 5 del acta de la sesión 1242-2016, celebrada el 5 de abril del 2016.

Rige a partir de su publicación en el Diario Oficial La Gaceta.

VER REGLAMENTO
VER CONSIDERANDOS DEL REGLAMENTO
VER LINEAMIENTOS GENERALES
VER HISTORIAL DE CAMBIOS

Versión documento	Fecha de actualización
04	9 de agosto 2016

CONSIDERANDOS >

consideraciones legales y reglamentarias

De conformidad con inciso c), el artículo 131 de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558, el Superintendente General de Entidades Financieras propuso al Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) para su aprobación, el Acuerdo SUGEF 18-16 "Reglamento sobre Gestión del Riesgo Operativo", el cual establece los requerimientos mínimos que deben observar las entidades supervisadas en la gestión del riesgo operativo. Asimismo, el párrafo segundo del artículo 119 de la citada ley, en relación con la operación propia de las entidades fiscalizadas, establece que se podrán dictar las normas generales que sean necesarias para el establecimiento de sanas prácticas bancarias, todo en salvaguarda del interés de la colectividad.

El inciso b), del artículo 171 de la Ley Reguladora del Mercado de Valores, Ley 7732, dispone que son funciones del CONASSIF aprobar las normas atinentes a la autorización, regulación, supervisión, fiscalización y vigilancia que conforme a la ley, deben ejecutar la Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia General de Valores (SUGEVAL) y la Superintendencia de Pensiones (SUPEN).

El párrafo segundo del artículo 28 de la Ley Reguladora del Mercado de Seguros, Ley 8653, indica que a la Superintendencia General de Seguros (*SUGESE*) le son aplicables las disposiciones establecidas, de manera genérica y de aplicación uniforme, para las demás superintendencias bajo la dirección del CONASSIF y sus respectivos superintendentes e intendentes.

Las disposiciones que se emiten son complementarias a las establecidas en los Acuerdos: SUGEF 2-10 "*Reglamento sobre Administración Integral de Riesgos*", SUGEF 16-09 "*Reglamento de Gobierno Corporativo*" y SUGEF 14-09 "*Reglamento sobre la Gestión de la Tecnología de Información*". Además, son congruentes con los principios referenciados como buenas prácticas para la gestión de riesgos, divulgados mediante la Resolución del Superintendente R-008-2010, del 22 julio del 2010. En virtud de esta condición, a lo largo del reglamento, se introducen las respectivas referencias con el objeto de preservar su concordancia, limitar duplicidades y mejorar la integridad del marco normativo.

consideraciones prudenciales

El Pilar 2 del documento sobre Convergencia internacional de medidas y normas de capital: marco revisado (Basilea II) y las recomendaciones del Comité de Basilea, contenidas en los *"*Principios Básicos para una Supervisión Bancaria Eficaz*" (setiembre 2012)*, señalan los principios a seguir para la mejora y fortalecimiento de las prácticas de regulación y supervisión. El principio 25 indica que los supervisores deben determinar que las entidades cuentan con un marco adecuado de gestión del riesgo operativo que considere su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados. Este marco incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operativo en el momento oportuno.

Conforme los nuevos enfoques de gestión del riesgo, las acciones que se desarrollan, sean correctivas o preventivas, deben armonizarse con la estrategia global de la entidad; por tal razón, las autoridades de las entidades supervisadas deben velar para que el marco de gestión para el riesgo operativo esté integrado, tanto desde el aspecto formal como en la práctica, al proceso de administración integral de riesgos de la entidad; asimismo, que incorpore y atienda oportunamente las recomendaciones derivadas del proceso supervisor.

El riesgo operativo es transversal a la organización, por lo que cualquier área de la entidad es generadora potencial de eventos de riesgo operativo. Esta condición requiere que la estrategia para su gestión involucre a todo el personal. Asimismo, debido a que el entorno empresarial está en constante cambio, la Junta Directiva o autoridad equivalente y la Administración Superior deben velar porque el marco para gestionar el riesgo operativo sea robusto en relación con la idoneidad y capacitación del personal involucrado y los sistemas de información, en línea con los requerimientos planteados por el Acuerdo SUGEF 2-10, dentro de la estructura de soporte para la administración de riesgos.

La incorporación de mejores prácticas en la gestión del riesgo operativo por parte de las entidades supervisadas es imperativo para lograr una mejora en la gestión del riesgo. Con el propósito de avanzar en ese sentido, es necesario establecer un conjunto de requerimientos regulatorios que promuevan dicha gestión.

Este reglamento cubre un conjunto de tópicos que la industria financiera internacional ha reconocido como relevante en la gestión de riesgo operativo. El CONASSIF reconoce que la extensión y profundidad en la implementación de este reglamento debe ser proporcional tanto con el perfil de riesgo y tamaño de cada entidad, como con el volumen y complejidad de sus actividades; por tanto, los requerimientos han sido consignados de manera que se brinde espacio para la aplicación del juicio crítico de las autoridades de la entidad, en el diseño de su marco para gestionar el riesgo operativo. Esta condición de proporcionalidad requiere,

consecuentemente, un compromiso de la entidad para realizar una evaluación rigurosa y meticulosa de su propia realidad.

Con el objeto de estimular la implementación, mejora y mantenimiento de estos marcos de gestión para el riesgo operativo, se brinda una gradualidad que permita balancear los esfuerzos requeridos por las entidades y la Superintendencia en el proceso de implementación de estas disposiciones. Asimismo, vía Lineamientos Generales la Superintendencia establece los aspectos técnicos operativos que se estiman necesarios al efecto.

El CONASSIF considera factible a futuro introducir estímulos asociados al grado de intensidad del proceso supervisor o al cargo de capital regulatorio para riesgo operativo actualmente en vigor; sin embargo, este tipo de estímulos estará sujeto a una valoración más integral sobre la evolución de los marcos de gestión, su efectividad y rigor. En ese sentido, el CONASSIF ha señalado (inciso iii del considerando c. del artículo 5, del acta de la sesión 852-2010, celebrada el 20 de mayo del 2010) que, una condición necesaria para dar este tipo de pasos, es el desarrollo de las destrezas y capacidades relacionadas con el juicio informado y criterio valorativo, en las entidades y en el órgano supervisor, aunado a la necesidad de evidenciar la consolidación de los procesos para la gestión integral de riesgos; por tanto, el reglamento que se aprueba a continuación no contempla cambios tendientes a modificar el cargo de capital por riesgo operativo.

La emisión de este reglamento propicia la creación de bases de datos sobre incidencias y eventos potenciales de riesgo operativo que permitan a las entidades, cuyo perfil de riesgo así lo amerite, evolucionar desde metodologías para valoración del riesgo operativo relativamente simples a otras más sofisticadas. Asimismo, establece requerimientos respecto a continuidad del negocio, procesos de tercerización y seguridad de la información que son aspectos inherentes a la gestión de riesgo operativo.

Mediante artículo 10 del acta de la sesión 1162-2015, del 20 de abril del 2015, el CONASSIF sometió a consulta el presente Reglamento. Asimismo, mediante artículo 17, del acta de la sesión 1171-2015, celebrada el 1 de junio del 2015, extendió el plazo otorgado a los consultados para remitir comentarios y observaciones.

Los comentarios y observaciones obtenidos fueron tomados en consideración para el texto final.

ACUERDO SUGEF 18-16

REGLAMENTO SOBRE GESTIÓN DEL RIESGO OPERATIVO >

CAPITULO I DISPOSICIONES GENERALES

Artículo 1. Objeto

Este reglamento establece los requerimientos mínimos que deben observarse en la gestión de riesgo operativo.

Artículo 2. Ámbito de aplicación

Las disposiciones de este reglamento son de aplicación para las entidades supervisadas por la Superintendencia General de Entidades Financieras.

Artículo 3. Definiciones

Para efecto de la aplicación de las disposiciones contenidas en este reglamento se entiende como:

Acuerdo SUGEF 2-10: Reglamento sobre Administración Integral de Riesgos.

Acuerdo SUGEF 16-09: Reglamento de Gobierno Corporativo.

Acuerdo SUGEF 14-09: Reglamento sobre la Gestión de la Tecnología de Información.

Administración Superior: Cualquier persona física que, por su función, cargo o posición, ejerza o represente la máxima autoridad administrativa de una persona jurídica, así como cualquier persona física que, por su función, cargo o posición en una entidad, intervenga o tenga la posibilidad de intervenir en la toma de decisiones importantes dentro de la entidad.

Administración Integral de Riesgos: Proceso por medio del cual una entidad financiera identifica, mide, evalúa, monitorea, controla, mitiga y comunica los distintos tipos de riesgo a que se encuentra expuesta.

Cuasipérdida: Eventos de riesgo que no resultan en pérdidas financieras, cuyo resultado no depende de la efectividad o funcionamiento de un indicador, control u otra medida preventiva, sino por cuestiones puramente circunstanciales.

Evento de riesgo: Suceso o serie de sucesos, de origen interno o externo, que pueden derivar en pérdidas financieras para la entidad. Puede ser de dos tipos: incidencias, eventos que se han producido; o eventos potenciales, aquellos que podrían producirse.

Factor de riesgo: Causa u origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos.

Frecuencia: Número de eventos o resultados por unidad de tiempo definida.

Indicador de riesgo: medida cuantitativa o cualitativa que permite determinar prospectivamente la posibilidad de un evento, como de sus consecuencias.

Línea de negocio: Especialización que agrupa procesos encaminados a generar productos y servicios para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad.

Perfil de riesgo: Naturaleza y magnitud de las exposiciones al riesgo de la entidad.

Plan de contingencia (o Planificación de contingencias): Proceso de desarrollar acuerdos y procedimientos avanzados que permiten a una organización responder a un evento no deseado que repercute negativamente en la organización.

Plan de continuidad (o Plan de continuidad del negocio): Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación tras la interrupción.

Probabilidad: Medición de la posibilidad de ocurrencia, expresada como un número comprendido entre 0 y 1, donde 0 es la imposibilidad y 1 la certeza absoluta.

Proceso: Es el conjunto de actividades que transforman, bajo determinadas condiciones y plazo, insumos en productos o servicios con valor para el usuario, sea interno o externo.

Proceso crítico: Proceso indispensable para la continuidad del negocio y sus operaciones.

Riesgo inherente: es aquél intrínseco de un producto, actividad, proceso o sistema, entre otros, al que se enfrenta una entidad en ausencia de acciones o controles tendientes a modificar su probabilidad o impacto.

Riesgo legal: Es la posibilidad de pérdidas económicas debido a la inobservancia o aplicación incorrecta o inoportuna de disposiciones legales o normativas, instrucciones emanadas de los organismos de control o como consecuencia de resoluciones judiciales, extrajudiciales o administrativas adversas, o de la falta de claridad o redacción deficiente en los textos contractuales que pueden afectar la formalización o ejecución de actos, contratos o transacciones.

Riesgo operativo: Posibilidad de sufrir pérdidas económicas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal y el riesgo de tecnologías de información, pero excluye el riesgo estratégico y el de reputación.

Subprocesos: Son agrupaciones de actividades dentro de un proceso. Su identificación puede resultar útil para aislar los tratamientos específicos que pueden presentarse dentro de un mismo proceso.

Subcontratación: Modalidad de contratación en la que una empresa requiere a otra para que realice determinados servicios, asignados originalmente a la primera.

Tercerización: Modalidad en la que se contrata a un tercero para que éste desarrolle o suministre un determinado producto o servicio, de forma permanente, temporal o intermitente.

Tolerancia al riesgo: La tolerancia es el nivel máximo de riesgo que la entidad está dispuesta a soportar.

CAPÍTULO II MARCO GENERAL PARA LA GESTIÓN DEL RIESGO OPERATIVO

Artículo 4. Contexto de la gestión del riesgo operativo

La entidad, de conformidad con lo dispuesto en el Acuerdo SUGEF 2-10, debe contar con una estructura organizativa que le permita implementar efectivamente su estrategia para la gestión del riesgo operativo.

La Junta Directiva o autoridad equivalente, junto con la Administración Superior, deben velar por que las acciones y herramientas que desarrolle la entidad para la gestión del riesgo operativo, estén plenamente integradas a su proceso institucional de administración integral de riesgos y que sean acordes con su tamaño, complejidad, volumen de sus operaciones y perfil de riesgo. En este sentido deben asignar los recursos necesarios para su implementación, sostenibilidad y mejora a través del tiempo.

Artículo 5. Estrategia para la gestión del riesgo operativo

La entidad debe definir la estrategia para gestionar su riesgo operativo. La estrategia debe ser actualizada periódicamente en función al nivel de tolerancia al riesgo, a los cambios en el mercado y en el entorno económico que puedan afectar la operatividad de la entidad. Asimismo, debe estar debidamente aprobada por la Junta Directiva o autoridad equivalente, en línea con las responsabilidades asignadas en el Acuerdo SUGEF 2-10.

La estrategia debe considerar el establecimiento y mantenimiento de límites de tolerancia al riesgo operativo conforme al artículo 9 del Acuerdo SUGEF 2-10 y de un marco o proceso que comprenda las siguientes etapas:

- Identificación.
- Medición y evaluación.
- Control y mitigación.
- Monitoreo e información.

Artículo 6. Políticas para la gestión del riesgo operativo

La Junta Directiva o autoridad equivalente debe aprobar y mantener actualizadas las políticas sobre riesgo operativo, dichas políticas deben considerar como mínimo los siguientes aspectos:

a) Las responsabilidades de la Junta Directiva o autoridad equivalente, de la Administración Superior, del Comité de Riesgos y de la función o unidad de riesgos.
b) Las pautas generales que observará la entidad en el manejo del riesgo operativo.
c) La periodicidad con la que se debe informar a las diferentes instancias de gobierno, sobre la exposición al riesgo operativo de la entidad y de cada unidad de negocio.
d) El nivel de riesgo aceptable por la entidad, en función de probabilidad (frecuencia) e impacto.
e) El proceso que se debe cumplir para la aprobación de propuestas de nuevas operaciones, productos, servicios y sistemas de información.
f) Indicadores de riesgo operativo.

En el marco de las funciones que establece el Acuerdo SUGEF 2-10, la Junta Directiva o autoridad equivalente y la Administración Superior deben velar por que se definan claramente las funciones que deben acometer el Comité de Riesgos y la unidad o función de riesgos en relación con el riesgo operativo.

Artículo 7. Gestión del riesgo operativo

En consonancia con el marco normativo establecido en el Acuerdo SUGEF 16-09 y el Acuerdo SUGEF 2-10, la entidad debe considerar al riesgo operativo como un riesgo relevante, inherente a la actividad financiera y objeto de gestión en su proceso de administración integral de riesgos.

La entidad debe considerar en su gestión del riesgo operativo los siguientes factores de riesgo:

a) Procesos,
b) Recursos humanos (personas),
c) Tecnología de información , y
d) Eventos externos.

Artículo 8. Identificación

La entidad debe establecer un proceso para identificar, catalogar y posteriormente documentar en su Manual de Administración Integral de Riesgos las líneas de negocio que desarrolla en su actividad comercial, junto con los procesos y subprocesos relacionados, a un nivel de detalle que le permita una adecuada identificación de los eventos de riesgo y la distinción de sus procesos críticos.

El Superintendente, mediante Lineamientos Generales, establecerá las líneas de negocio y categorías de eventos de riesgo operativo que pueden ser utilizados como referencia por la entidad.
En el proceso de identificación de riesgos, la entidad debe velar que se provea de información suficiente para determinar la exposición al riesgo operativo, la cual debe incluir lo correspondiente al riesgo legal.

A efecto de garantizar las condiciones e información necesarias para este ejercicio, la Administración Superior debe velar por que exista una comunicación efectiva entre las áreas de negocio y la unidad o función de riesgos; esta última responsable de coordinar los aspectos necesarios en torno a la identificación de los eventos de riesgo de la organización.

La entidad debe realizar una evaluación del riesgo operativo inherente a los productos, actividades, procesos y sistemas que previo análisis y clasificación, resulten relevantes para la entidad. Asimismo, la Administración Superior debe asegurar que, antes de introducir nuevos productos, se emprendan nuevas actividades o se establezcan nuevos procesos y sistemas, el riesgo operativo inherente a ellos esté sujeto a un procedimiento de evaluación. La unidad o función de riesgos, previo al lanzamiento o prestación de nuevos productos y servicios, debe rendir a la Junta Directiva o autoridad equivalente una opinión sobre la evaluación efectuada. Este requerimiento es obligatorio también cuando se trate del relanzamiento de un producto, servicio, proceso o sistema.

Artículo 9. Medición y evaluación

La entidad debe evaluar los eventos de riesgo, esto implica la medición de las pérdidas potenciales en términos de probabilidad de ocurrencia (frecuencia) e impacto.

La metodología que implemente la entidad para la medición y evaluación debe ser cualitativa y cuantitativa en función al avance que vaya teniendo en su proceso de implementación de la gestión de riesgo operativo. La evaluación cualitativa busca desarrollar los criterios para

priorizar la atención de los riesgos y la periodicidad para su seguimiento. La evaluación cuantitativa debe realizarse a través de la información histórica de eventos de riesgo para el caso de las incidencias de riesgo y en estimaciones para el caso de los eventos potenciales. La metodología utilizada debe constar en el Manual de Administración Integral de Riesgos.

Asimismo, la entidad debe considerar el establecimiento y mantenimiento de un proceso de recopilación y registro de eventos de riesgo considerando los procesos y líneas de negocio identificados. Dicho proceso debe garantizar que la información se computa oportunamente.

Artículo 10. Control y mitigación

El control y mitigación se refiere a las acciones o mecanismos de cobertura y a los controles implementados por la entidad con el propósito de modificar la probabilidad (frecuencia) de ocurrencia y/o el impacto de los eventos de riesgo operativo que conforme el análisis de riesgo excedan su apetito de riesgo operativo.

Para dichos eventos de riesgo, la entidad debe implementar y mantener un plan que establezca las acciones a efectuar, el plazo estimado de ejecución, el grado de avance y los responsables directos de dicha ejecución.

Asimismo, la entidad debe contar con un sistema de control interno que permita verificar el acatamiento de las políticas y procedimientos, incluyendo los planes de acción definidos por la entidad para la mitigación del riesgo operativo. La Administración Superior es responsable de tomar las acciones necesarias para subsanar debilidades del sistema de control interno de la entidad.

Las acciones y controles definidos deben ser proporcionales al riesgo identificado por la entidad de manera que se asegure que los costos de las acciones de mitigación y control no sean mayores a las pérdidas definidas o estimadas.

Artículo 11. Monitoreo e Información

La entidad debe establecer, en su sistema de información, los indicadores y reportes que estime necesarios para realizar un seguimiento de su perfil de riesgo operativo. La periodicidad establecida del seguimiento debe permitir una adecuada retroalimentación sobre las acciones ejecutadas y sobre los cambios del perfil de riesgo operativo, de lo cual la entidad debe mantener evidencia. Dicha periodicidad no podrá ser mayor a seis meses.

CAPÍTULO III OTRAS DISPOSICIONES SOBRE LA GESTIÓN

Artículo 12. Continuidad del Negocio

Como parte de una adecuada gestión del riesgo operativo, la entidad debe implementar y mantener un sistema que le permita la continuidad del negocio, con el propósito de brindar respuestas efectivas, para que la operatividad de la entidad continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en sus operaciones.

El sistema para la continuidad del negocio debe ser congruente con el perfil de riesgo, el tamaño, la complejidad y el volumen de las operaciones de la entidad. El sistema para la continuidad del negocio, al menos, debe considerar:

a) Determinación de los procesos críticos del negocio, incluyendo procesos o servicios provistos por terceros.
b) Análisis de impacto al negocio.
c) Plan de continuidad.
d) Planes de contingencia.
e) Ejecución de pruebas periódicas y evaluación de sus resultados. La periodicidad de estas pruebas no debe ser mayor a los 12 meses.
f) Divulgación y entrenamiento.
g) Establecimiento de un equipo de gestión de la continuidad del negocio, cuyos integrantes cuenten con el conocimiento e información del plan de continuidad, el cual evaluará el problema operativo que se está enfrentando, decidirá las acciones a seguir y monitoreará los eventos y tomará acciones correctivas cuando sea necesario. Las responsabilidades y autoridad de cada miembro del equipo deben ser establecidas de manera detallada.
h) Dentro del sistema para la continuidad del negocio, la entidad debe incorporar el plan para la continuidad de la tecnología de información.

Artículo 13. Seguridad de la información

La entidad debe contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información. Para ello, debe cumplir como mínimo con los requerimientos establecidos en el Acuerdo SUGEF 14-09 "*Reglamento Sobre la Gestión de la Tecnología de Información*".

Asimismo, con el propósito de resguardar la calidad de la información, su confidencialidad, integridad y disponibilidad, la entidad debe contar con políticas y procedimientos de gestión y seguridad de la información, que consideren entre otros aspectos:

a) La autenticación para el acceso lógico a los sistemas y servicios informáticos internos y externos.
b) La conservación ordenada, completa, íntegra, oportuna de la información y documentación (registros) que soporta las operaciones de la entidad.
c) La divulgación y uso no autorizado de información confidencial o protegida por ley.

El Superintendente establecerá, mediante Lineamientos Generales, requerimientos mínimos respecto a la autenticación de clientes y autorización de transacciones en la prestación de servicios financieros en ambientes de banca en línea.

Artículo 14. Base de Datos

La entidad debe conformar una base de datos para incidencias y una base de datos para eventos potenciales. Ambas bases deben contener, al menos, la información que establezca el Superintendente mediante Lineamientos Generales. La entidad, adicionalmente, puede incluir otros campos que requiera para su gestión; asimismo, la Junta Directiva o autoridad equivalente de la entidad debe definir en sus políticas un monto mínimo de pérdida a partir del cual se registra una incidencia o evento potencial en la base de datos. En este último caso, la entidad debe definir los criterios que le permitan imputar un valor al evento en función de la información que se disponga.

Artículo 15. Tercerización

La entidad debe, según la complejidad, naturaleza y criticidad de los servicios contratados o subcontratados, establecer las políticas, procedimientos y controles necesarios para conducir el proceso de selección y contratación de proveedores de servicios, así como para monitorear los procesos o servicios subcontratados. La entidad debe cubrir, como mínimo, los siguientes aspectos:

a) Definición de los criterios para la calificación y adecuada selección de proveedores.
b) En el proceso de contratación:
    i. Legalidad y formalidad de los contratos.

ii. Definición de los acuerdos del nivel de servicio, brindando especial cuidado al establecimiento de cláusulas referentes a la seguridad de la información, así como cláusulas ante incumplimientos a éstas.
iii. Definición de las responsabilidades del proveedor y de la entidad.
iv. Establecimiento de planes de contingencia y continuidad del servicio por parte del proveedor. La entidad debe considerar la inclusión de cláusulas sobre la disponibilidad del proveedor, de ser objeto de pruebas por parte de la entidad, sobre dichos planes, principalmente para el caso de los servicios críticos que están siendo tercerizados sean o no relacionados con Tecnologías de Información (*TI*).

c) La gestión de los riesgos asociados con la subcontratación o con la tercerización.

La entidad debe aplicar la diligencia debida al seleccionar posibles proveedores de servicios. Adicionalmente, la entidad debe considerar los controles aplicables a los servicios de tecnología de información suministrados por terceros, de conformidad con lo dispuesto en el Acuerdo SUGEF 14-09.

Artículo 16. **Riesgo de Tecnologías de Información (TI)**

La entidad, en su gestión del riesgo operativo, debe considerar el riesgo de Tecnologías de Información (*TI*). Para ello, la Administración Superior debe velar que el marco de trabajo de administración de riesgos de TI esté alineado a su proceso de administración de riesgos. Dicho marco de trabajo debe cumplir con los requerimientos dispuestos por el respectivo proceso de conformidad con lo dispuesto en el Acuerdo SUGEF 14-09.

Artículo 17. Riesgos operativos asociados a actividades específicas

La entidad debe considerar, en el ámbito de la gestión del riesgo operativo, los riesgos operativos asociados a las actividades de titularización, fideicomiso y de toma u ofrecimiento de productos derivados. En tales casos, la entidad debe considerar las leyes y reglamentos que al respecto regulan dichas actividades.

Artículo 18. Divulgación

La entidad debe incluir, en su informe anual de riesgos, los aspectos referidos a su gestión del riesgo operativo, de conformidad con lo dispuesto por el artículo 18 del Acuerdo SUGEF 2-10.

Artículo 19. Reporte para la SUGEF

La entidad debe remitir anualmente, por el medio y en el plazo que defina la SUGEF en el Manual de Información-SICVECA, los datos sobre incidencias y eventos potenciales contenidos en las respectivas bases de datos a que hace mención este reglamento en el artículo 14.

Transitorio 1

La entidad debe presentar a la SUGEF, dentro de los seis meses siguientes a la entrada en vigencia de esta norma, un plan de actividades para la implementación de las disposiciones de este reglamento, que incluya el cronograma de ejecución y los responsables a cargo.

Transitorio 2

La entidad cuenta con dieciocho meses, contados a partir de la entrada en vigencia de este reglamento para poner en funcionamiento las bases de datos de incidencias y de los eventos potenciales de riesgo operativo.

La primera remisión de los datos de las bases de datos, será un año posterior a su puesta en funcionamiento.

Transitorio 3

La identificación de eventos de riesgo operativo, requerida a la entidad en el artículo 8 de este reglamento, puede realizarse por áreas o unidades organizacionales por el lapso que le tome finalizar su proceso para identificar, catalogar y documentar las líneas de negocio que desarrolla en su actividad comercial.

DISPOSICIÓN FINAL ÚNICA: Entrada en vigencia.

Rige a partir de su publicación en el Diario Oficial La Gaceta.

REGRESAR AL INICIO

LINEAMIENTOS GENERALES >

SGF-R-1812-2016. Superintendencia General de Entidades Financieras. Despacho del Superintendente General de Entidades Financieras. Santa Ana, del 06 de junio del 2016.

El Superintendente General de Entidades Financieras,

Considerando que:

1. Mediante artículo 5 del acta de la sesión 1242-2016, del 5 de abril del 2016, el Consejo Nacional de Supervisión del Sistema Financiero aprobó el Acuerdo SUGEF 18-16 "Reglamento sobre Gestión del Riesgo Operativo".

2. Los artículos 8, 13 y 14 del citado reglamento requieren la emisión de lineamientos respecto a líneas de negocio y las categorías de eventos de riesgo operativo; sobre los requerimientos mínimos a la autenticación de clientes y autorización de transacciones en los medios y dispositivos de los canales electrónicos utilizados en la prestación de servicios financieros (en particular en ambientes de banca en línea); y la información de la base de datos de eventos de riesgo operativo y de la base de datos para eventos de riesgos potenciales; por lo que se hace necesario emitir dichos lineamientos generales.

3. El Artículo 131, inciso b) de la Ley Orgánica del Banco Central de Costa Rica, Ley número 7558, establece que corresponde al Superintendente tomar las medidas necesarias para ejecutar los acuerdos del Consejo Nacional de Supervisión.

Dispone:

1. Dejar sin efecto el SGF-1557-2016, del 11 de mayo del 2016.

2. Emitir los "Lineamientos Generales" del Acuerdo SUGEF 18-16 "Reglamento sobre Gestión del Riesgo Operativo" de conformidad con el siguiente texto:

LINEAMIENTOS GENERALES DEL ACUERDO SUGEF 18-16
REGLAMENTO SOBRE GESTIÓN DEL RIESGO OPERATIVO

Objetivo general: Suministrar las guías necesarias que permitan a la entidad observar lo dispuesto por el Acuerdo SUGEF 18-16.

I. LÍNEAS DE NEGOCIO GENÉRICAS PARA INTERMEDIARIOS FINANCIEROS DEL SISTEMA FINANCIERO NACIONAL.

Las líneas de negocio que de seguido se presentan son de carácter orientativo.

Línea	Nivel 1	Nivel 2	Grupo de actividades
1	**Finanzas corporativas**	1.1 Finanzas corporativas	Fusiones y adquisiciones, suscripción y colocación de emisiones (capital y deuda), sindicaciones de préstamos, colocaciones de deuda en mercados secundarios.
		1.2 Finanzas de administraciones locales y públicas	Financiamiento al sector público, participación en licitación de emisiones de deuda, administración de fondos públicos, colocación de deuda pública.
		1.3 Banca de inversión	Asesoramientos en inversiones (fondos comunes de inversión, obligaciones negociables, acciones, títulos.
		1.4 Servicios de asesoramiento	Servicio de asesoramiento en productos estructurados de inversión y cobertura de riesgos.
2	**Tesorería**	2.1 Tesorería por cuenta de terceros	Distribución y venta a clientes, desde las áreas de tesorería y mercado de capitales, de valores de renta fija y variable, forex, préstamo de valores, repos, derivados y otros productos propios del área de tesorería que

			no implican posición por cuenta propia, siendo el resultado de las mismas una comisión.
		2.2 Tesorería posiciones propias	Operaciones que implican posiciones tomadas por cuenta propia en renta fija, en renta variable, forex, derivados y otros productos.
		2.3 Tesorería tradicional	Actividades cotidianas de fondeo llevadas a cabo por la Tesorería (préstamos interbancarios, operaciones de reporto, etc.), administración de la liquidez y otros.
3	**Banca minorista**	3.1 Banca de Personas	Hipotecas, créditos personales, prendarios, adelantos en cuenta corriente, descuento de documentos, leasing, depósitos vista (cuenta corriente y caja de ahorro), depósitos a plazo, fideicomisos y otros servicios bancarios (débitos en cuenta, fondos comunes de inversión, participación en fideicomisos, compra y venta de títulos y acciones, etc.)
		3.2 Banca Privada (personas alto poder adquisitivo)	Hipotecas, créditos personales, prendarios, adelantos en cuenta corriente, descuento de documentos, leasing, depósitos vista (cuenta corriente y caja de ahorro), depósitos a plazo, fideicomisos y otros servicios bancarios (débitos en cuenta, fondos comunes de inversión, participación en fideicomisos, compra y venta de títulos y acciones, etc.)
		3.3 Banca de Desarrollo Minorista	Productos y servicios a Mipymes (personas físicas).

4	**Banca comercial**	4.1 Banca Corporativa	Crédito directo, líneas de crédito, garantías de participación y cumplimiento, cartas de crédito, financiación de importaciones y exportaciones, descuento de documentos, factoreo, certificados de inversión, cuentas corrientes y de ahorro y otros servicios bancarios, fianzas, avales y otras garantías.
		4.2 Banca Empresarial	Crédito directo, líneas de crédito, garantías de participación y cumplimiento, cartas de crédito, financiación de importaciones y exportaciones, descuento de documentos, factoreo, certificados de inversión, cuentas corrientes y de ahorro y otros servicios bancarios, fianzas, avales y otras garantías.
		4.3 Banca de Desarrollo Comercial	Productos y servicios a Mipymes (personas jurídicas)
		4.4 Banca de Segundo Piso	Financiamiento a entidades
5	**Tarjetas**	5.1 Tarjetas de crédito y débito (marcas propias o administradas)	Actividades y servicios relacionados con tarjetas de crédito o débito, comerciales, corporativas, prepagadas y otras, independientemente del tipo de cliente usuario.
		5.2 Administración y adhesión de comercios	Actividades y servicios relacionados con administración y adhesión de comercios donde se pueden utilizar las tarjetas.
6	**Cobros, Pagos y liquidación**	6.1 Cobros, Pagos y liquidación	Servicios de cobranza (recaudaciones en general). Servicios de pagos (a proveedores, compañías de seguro, etc.). Transferencias y compensaciones electrónicas,

			Pago de planillas, Servicio de remesas y otros.
7	**Administración de Activos**	7.1 Administración de Fondos de Cesantía	Administración de Fondos de Cesantía por parte de Cooperativas.
		7.2 Administración del peaje bancario y otros	Administración del peaje bancario (Artículo 59 de la Ley Orgánica del Sistema Bancario Nacional) y otros.
		7.3 Administración de fideicomisos	Servicios por cobranza de las cuotas de los préstamos de la cartera del fideicomiso y pago de los servicios de los títulos de deuda y certificados de participación.
		7.4 Administración de fondos de pensión	Servicios de inversión de los fondos administrados.
8	**Otros servicios**	8.1 Custodia	Servicios de custodia (efectivo, títulos y acciones, monedas, documentos, etc.). Servicios de custodia en caja de valores. Servicios de caja de seguridad. Servicios pignoración y consignación. Servicios de Custodia Auxiliares de Numeración (CAN).
		8.2 Comercialización de Seguros autoexpedibles	Comercialización de seguros autoexpedibles (venta de seguros individuos, hogar, automotor, entre otros),
		8.3 Tecnología de información y comunicación 8.4 Cambios y transformaciones organizacionales 8.5 Otros procesos transversales a la organización	

De seguido se presentan orientaciones generales para la asignación de las líneas de negocio:

a) La entidad, cuando sea pertinente, puede desagregar sus líneas de negocio a subcategorías de actividades que desarrolla y que sean particulares a su giro de negocio o naturaleza, dicha desagregación constituye el nivel 3 y debe mantener la secuencia numérica dispuesta. Por ejemplo, para la línea 5 "Tarjetas" es posible que exista la necesidad de identificar los eventos de riesgo por separado, según los tipos de tarjeta, en tal caso, el ajuste consiste en abrir un tercer nivel como se ilustra:

5	**Tarjetas**	5.1 Tarjetas de crédito y débito (marcas propias o administradas)	5.1.1 Tarjeta de crédito
			5.1.2 Tarjeta de débito

b) Cualquier actividad que no pueda asignarse con facilidad a las líneas de negocio, pero que representa una función auxiliar a una actividad incluida en el nivel 2, debe ser asignada a la línea de negocio en que se ubica dicha actividad principal.

c) Si una actividad auxiliar presta apoyo a más de una línea de negocio, debe utilizarse un criterio de asignación objetivo.

d) El nivel de desagregación del nivel 3 debe permitir a la entidad asignar e imputar de forma razonable los eventos de riesgo, tal condición implica que la Administración Superior de la entidad deba establecer un proceso para definir la asignación de nuevas actividades o productos.

e) La segregación de nivel 3 debe mantener un registro descriptivo que permita comprender claramente el tipo de actividades que involucra, de manera tal que limite la posibilidad de duplicación y que facilite la asignación de nuevas actividades o productos.

II. CATEGORÍAS DE EVENTOS DE PÉRDIDA POR RIESGO OPERATIVO

Corresponden a los eventos de pérdida dispuestos por el Comité de Basilea, que la entidad puede ajustar de acuerdo a sus características y abriendo subcategorías cuando sea pertinente.

a. **Fraude interno**.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.

b. **Fraude externo**.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c. **Relaciones laborales y seguridad en el puesto de trabajo**.- Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.

d. **Clientes, productos y prácticas empresariales**.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

e. **Daños a activos materiales**.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

f. **Interrupción del negocio y fallos en los sistemas**.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.

g. **Ejecución, entrega y gestión de procesos.-** Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores

III. CAMPOS DE LA BASE DE DATOS SOBRE INCIDENCIAS Y EVENTOS DE RIESGO OPERATIVO

La base de datos de incidencias y eventos de riesgo permite establecer de forma cuantitativa la exposición al riesgo operativo de la entidad. Esta herramienta suministra información sobre cuáles son los eventos más relevantes y en qué líneas de negocio se originan.

La entidad de conformidad con el artículo 19 del Acuerdo SUGEF 18-16 debe remitir a la SUGEF la información contenida en la base de datos conforme los términos del respectivo capítulo del Manual de Información-SICVECA.

De conformidad con lo dispuesto en el artículo 14 del Acuerdo SUGEF 18-16, la entidad debe consignar en su base de datos sobre incidencias y eventos de riesgo operativo los siguientes campos:

Campos - Incidencias

1. Código interno de identificación del incidente (secuencial y asignado por la entidad).

2. Categoría de evento de pérdida (según las categorías de eventos señalados en el apartado II de estos lineamientos).
3. Línea de negocio asociado, según líneas señaladas en el apartado I de estos lineamientos.
4. Título del riesgo. Corresponde a la frase con que se da a conocer el nombre o asunto distintivo.
5. Descripción del riesgo.
   5.1 Carácter del riesgo
      5.1.1 Pérdida ocurrida individual
      5.1.2 Pérdida ocurrida repetitiva
      5.1.3 Pérdida estimada contablemente
   5.2 Detalle.
6. Proceso o área a la que pertenece el riesgo.
   6.1 Área de negocio
   6.2 Proceso
      6.2.1 Subproceso
   6.3 Producto
7. Fecha de ocurrencia (o de inicio del riesgo).
8. Fecha de conclusión del riesgo.
9. Fecha de descubrimiento del riesgo.
10. Fecha de registro contable del riesgo.
11. Monto bruto de la pérdida, moneda y tipo de cambio.
12. Monto total recuperado.
13. Monto neto de la pérdida, moneda y tipo de cambio.
14. Cuenta(s) contable(s) asociada(s) (cuando aplique).
15. Acción correctiva asociada.
16. Vínculo con otro riesgo.
    16.1 Crédito
    16.2 Mercado
    16.3 Crédito y Mercado
    16.4 Otros

Campos – Eventos Potenciales

1. Código interno de identificación del evento (secuencial y asignado por la entidad).
2. Categoría de evento de pérdida (según las categorías de eventos señalados en el apartado II de estos lineamientos).
3. Línea de negocio asociado, según líneas señaladas en el apartado I de estos lineamientos.
4. Título del evento. Corresponde a la frase con que se da a conocer el nombre o asunto distintivo.
5. Descripción del evento.

5.1 Carácter del evento
5.1.1 Cuasipérdida
5.2 Detalle
6. Proceso o área a la que pertenece el evento.
6.1 Área de negocio.
6.2 Proceso
6.2.1 Subproceso
6.3 Producto
7. Monto estimado de la pérdida, moneda y tipo de cambio.

De seguido se presentan orientaciones generales en relación a la información que se debe consignar en la base de datos de incidencias y para eventos potenciales de riesgo operativo:

a) En las bases de datos se deben registrar todos los eventos que, siendo cuantificables, hayan generado pérdidas o hayan sido provisionados contablemente en el caso de incidencias. Asimismo, en la medida que puedan ser claramente identificados y cuantificados, se deben informar las cuasipérdidas de eventos potenciales.

b) Para las incidencias se deben incluir aquellos eventos cuyo importe o monto, sin considerar el recupero, supere el umbral mínimo establecido por la Junta Directiva o autoridad equivalente de la entidad. No obstante, aquellos eventos de similar naturaleza que individualmente no alcancen el monto mínimo pero su sumatoria lo exceda y se produzcan en el mismo mes (pérdidas repetitivas), deben ser incluidos e informados en forma consolidada.

c) El monto recuperado debe asociarse y vincularse al riesgo original (causa raíz) y corresponde al importe obtenido.

d) En el caso de riesgos con pérdidas múltiples (impactos múltiples), la entidad debe tener en cuenta la causa original (causa raíz) que ocasionó las pérdidas subsiguientes, de manera que la registre como si se tratase de un único incidente.

e) Se puede registrar información parcial de un riesgo, en tanto se obtengan los demás datos requeridos. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

f) No deben ser incluidos costos indirectos que sean cubiertos internamente sin incurrir en un gasto adicional.

g) Una incidencia o un evento potencial de carácter operativo que afecte también a otro

tipo de riesgos (crédito o mercado) deberá registrarse en la base de datos, cuando la principal causa de la pérdida sea de naturaleza operativo; asimismo, debe especificarse el vínculo con el otro riesgo.

h) En caso que la pérdida involucre algún activo con valor de mercado conocido, este será el valor a tener en cuenta, más los gastos adicionales que correspondan.

IV. REQUERIMIENTOS MÍNIMOS RESPECTO A LA AUTENTICACIÓN DE CLIENTES Y AUTORIZACIÓN DE TRANSACCIONES EN LOS MEDIOS Y DISPOSITIVOS DE LOS CANALES ELECTRÓNICOS UTILIZADOS EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS DE BANCA EN LINEA.

4.1 Definiciones

Banca electrónica: Servicios financieros suministrados a través de medios electrónicos. Comprende un conjunto de canales de comunicación compuestos por hardware y software, mediante los cuales las personadas físicas o jurídicas pueden acceder vía remota a los servicios de una entidad financiera, para obtener información o realizar transacciones bancarias.

Banca en línea es uno de los canales de banca electrónica que comprende aquellas herramientas que ofrece una entidad para que sus clientes hagan sus transacciones bancarias utilizando para ello una computadora con conexión a la red Internet.

Certificado Digital de Persona Física (Autenticación): Archivo electrónico que permite a las personas físicas realizar procesos de autenticación (demostración de la identidad) que las vinculan jurídicamente al amparo de la Ley número 8454.

Certificado Digital de Persona Física (Firma): Archivo electrónico que permite a las personas físicas realizar procesos de firma digital (manifestación de la voluntad) que las vinculan jurídicamente al amparo de la Ley número 8454.

Certificado Digital de Persona Jurídica (Sello Electrónico): Archivo electrónico que permite a las personas jurídicas realizar procesos de sello electrónico que las comprometen jurídicamente al amparo de la Ley número 8454

Dirección de Certificadores de Firma Digital (DCFD): Dirección adscrita al MICITT, creada por la Ley número 8454, encargada de la emisión de las políticas de certificación en el país.

Firma digital: mecanismo criptográfico que permite al receptor de un medio electrónico identificar formalmente a su autor, garantiza la autoría (identidad del firmante) y la integridad del documento electrónico (no alterado desde que fue firmado por el originador).

Medios o Canales electrónicos: Dispositivos, redes y servicios informáticos dispuestos por las entidades financieras, por sí o por intermedio de terceros, para la instrucción, consulta, registro, protección, procesamiento y/o almacenamiento de datos de clientes y sus transacciones bancarias.

Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT): Con base en la Ley Nº 8454, el ente regulador y supervisor del Sistema Nacional de Certificación Digital.

Política de formatos oficiales de los documentos electrónicos firmados digitalmente: directrices sobre los requisitos que deben cumplir los formatos avanzados de documentos electrónicos firmados digitalmente, los cuales permiten que se consigne en ellos, una "firma de larga duración". Implica que la verificación de la firma perdura en el tiempo, para lo cual, además del correspondiente hash (resumen criptográfico del documento), se consigna, previa consulta a la Autoridad Certificadora, la validez del certificado en el momento de la firma y una estampa de tiempo mediante la que, un tercero de confianza (una autoridad de estampado), ubica fehacientemente el documento en el tiempo, publicados por el Ministerio de Ciencia, Tecnología y Telecomunicaciones y la Dirección de Certificadores de Firma Digital.

Productos y servicios financieros: Cualquier transacción que se manifieste en activos o pasivos financieros independientemente de la figura jurídica o contractual que se utilice y del tipo de documento, registro electrónico u otro análogo en el que dichas transacciones se formalicen.

Sistema Nacional de Certificación Digital (SNCD): En atención a lo estipulado en la Ley número 8454, el MICITT, a través de la DCFD, implementó el SNCD como una jerarquía nacional que emite certificados para Persona Física (con propósitos de Autenticación y Firma), certificados para Persona Jurídica (con propósitos de Sello Electrónico y Agente Electrónico) y certificados de Estampado de Tiempo. El SNCD contempla las Políticas de Certificación, los Estándares de Certificación, las Autoridades Certificadoras (incluida la Autoridad Raíz Nacional), y las Oficinas de Registros requeridas para la emisión de certificados a personas físicas y jurídicas.

4.2 Autenticación y Autorización de Transacciones

Con el fin de dotar de una mayor seguridad jurídica a las transacciones realizadas mediante la banca en línea, las entidades supervisadas que ofrezcan servicios por este canal electrónico, sin detrimento de otros medios de autenticación y autorización de transacciones implementados por la entidad, deben tener preparada dicha plataforma para que toda persona física o jurídica que posea un certificado digital emitido a través de la infraestructura del Sistema Nacional de Certificación Digital, y que acceda por medio de computadoras pueda alternativamente, autenticarse en el sitio web y firmar digitalmente las transacciones mediante dicho mecanismo, a más tardar, 24 meses a partir de la entrada en vigencia del reglamento. Las acciones para su puesta en marcha deben formar parte del plan de actividades a que se refiere el Transitorio I del Reglamento del Acuerdo SUGEF 18-16.

Las entidades no deben requerir el uso de ningún medio de autenticación y autorización de transacciones adicional, para aquellos usuarios que elijan utilizar el certificado digital emitido por el Sistema Nacional de Certificación Digital, en las plataformas de banca en línea de la entidad.

4.3 Emisión de comprobantes de transacciones

La entidad supervisada debe emitir un comprobante de confirmación para cada una de las transacciones que realicen con sus clientes, ya sea por medio de su plataforma de banca en línea o por cualquier otro medio.

Independientemente de cuál haya sido el mecanismo de seguridad utilizado por el cliente para autenticarse y autorizar las transacciones en el sitio web, las transacciones consideradas de riesgo, conforme los criterios definidos por la propia entidad, deben estar sujetas a un protocolo de confirmación que haga uso del certificado de Persona Jurídica (Sello Electrónico) emitido a través de la infraestructura del Sistema Nacional de Certificación Digital.

En la medida de lo posible, se debe procurar que la transacción autorizada por el cliente y el respectivo comprobante de confirmación (que la entidad debe emitirle a su cliente) sea un solo archivo, no obstante, en caso de que éstos sean archivos separados, los mismos deben estar asociados lógicamente de modo que se pueda establecer la relación directa entre ambos.

4.4 Conservación de los comprobantes de las transacciones

Sin detrimento de cualquier otra disposición legal aplicable, para todas las transacciones autorizadas por los clientes por medio del servicio de banca en línea, las entidades supervisadas deben mantener, como mínimo, durante 48 meses, el registro histórico de esas transacciones, así como el registro de los respectivos comprobantes de confirmación.

Las entidades supervisadas deben tener a disposición de sus clientes los comprobantes de las transacciones de modo que éstos puedan obtenerlos al momento de concluir la operación y en cualquier momento posterior, dentro de los 48 meses a su realización. Para los efectos, la entidad debe definir el lapso en que podrán ser consultados directamente en la plataforma de banca en línea, superado dicho plazo, debe dar a conocer el trámite que el cliente debe realizar para obtener la respectiva información.

4.5 Formato de los archivos de los comprobantes firmados digitalmente

Todos los archivos electrónicos firmados digitalmente por la entidad supervisada o por sus clientes deben cumplir con los requisitos estipulados en la "Política de formatos oficiales de los documentos electrónicos firmados digitalmente", emitida por la Dirección de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Adicionalmente, las entidades supervisadas deben ofrecer a sus clientes las herramientas necesarias para que puedan visualizar la información contenida en estos archivos, así como para que puedan verificar la validez de las firmas digitales consignadas en estos.

4.6 Desarrollo de nuevos trámites firmados digitalmente

Las entidades supervisadas deben incentivar el desarrollo de nuevos servicios que posibiliten que todo trámite o gestión que requiera ser firmado por sus clientes, esté disponible en su plataforma de banca en línea y pueda ser firmado digitalmente por éstos, evitando así, que tengan que trasladarse físicamente a la entidad con este propósito.

Transitorio I

La entidad cuenta con 24 meses a partir de la entrada en vigencia del Acuerdo SUGEF 18-16, para implementar todas las funcionalidades necesarias que le permitan atender los requerimientos relacionados con el apartado IV de estos lineamientos.

Transitorio II

Firma digital para personas jurídicas:

De acuerdo con lo establecido en el punto "4.3 Emisión de comprobantes de transacciones" de la Sección "IV. REQUERIMIENTOS MÍNIMOS RESPECTO A LA AUTENTICACIÓN DE CLIENTES Y AUTORIZACIÓN DE TRANSACCIONES EN LOS MEDIOS Y DISPOSITIVOS DE LOS CANALES ELECTRÓNICOS UTILIZADOS EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS DE BANCA EN LINEA.", se requiere que todas las personas jurídicas efectúen sus trámites utilizando el certificado de Persona Jurídica (Sello Electrónico) emitido a través de la infraestructura del Sistema Nacional de Certificación Digital. Sin embargo, a la fecha de emisión de esta norma, el uso de este dispositivo está limitado a personas jurídicas del sector público. Por tanto, el uso del dispositivo será obligatorio a partir de los doce meses siguientes a la implementación del mismo por parte del Sistema Nacional de Certificación Digital.

Transitorio III

En los puntos "4.2 Autenticación y Autorización de Transacciones" y "4.3 Emisión de comprobantes de transacciones" de la Sección "IV. REQUERIMIENTOS MÍNIMOS RESPECTO A LA AUTENTICACIÓN DE CLIENTES Y AUTORIZACIÓN DE TRANSACCIONES EN LOS MEDIOS Y DISPOSITIVOS DE LOS CANALES ELECTRÓNICOS UTILIZADOS EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS DE BANCA EN LINEA.", se hace referencia al sitio web. Sin embargo, en el momento a partir del cual la entidad utilice una plataforma alternativa, ésta deberá informarlo a la SUGEF, aplicándole los mismos requerimientos estipulados en los puntos mencionados.

Rige a partir de su publicación en el Diario Oficial La Gaceta.

>HISTORIAL DE CAMBIOS<

Versión 01:	Texto del Reglamento, aprobado por CONASSIF. Oficio CNS 1242/05 del 12 de abril del 2016.
Versión 02:	Texto del Acuerdo SUGEF 18-16 *Reglamento sobre Gestión del Riesgo Operativo,* publicado en el Diario Oficial La Gaceta No. 97 del 20 de mayo del 2016. - Inclusión de los Lineamientos Generales del Acuerdo SUGEF 18-16 *Reglamento sobre Gestión del Riesgo Operativo*, aprobados por el Superintendente General de Entidades Financieras, según Resolución SGF-R-1557-2016 del 11 de mayo del 2016.
Versión 03:	Texto del Acuerdo SUGEF 18-16 *Reglamento sobre Gestión del Riesgo Operativo,* publicado en el Diario Oficial La Gaceta No. 97 del 20 de mayo del 2016. - Inclusión de los Lineamientos Generales del Acuerdo SUGEF 18-16 *Reglamento sobre Gestión del Riesgo Operativo*, aprobados por el Superintendente General de Entidades Financieras, según Resolución SGF-R-1812-2016 del 06 de Junio del 2016 que deja sin efecto la Resolución SGF-1557-2016 del 11 de mayo de 2016. Pendiente de publicación en el Diario Oficial La Gaceta.
Versión 04:	Publicación en el Alcance Nº 133 del Diario Oficial La Gaceta Nº 146 del 29 de julio del 2016, de los Lineamientos Generales del Acuerdo SUGEF 18-16 *Reglamento sobre Gestión del Riesgo Operativo*, aprobados por el Superintendente General de Entidades Financieras, según Resolución SGF-R-1812-2016 del 06 de Junio del 2016, que dejó sin efecto la Resolución SGF-1557-2016 del 11 de mayo de 2016.