República de Panamá
Superintendencia de Bancos

ACUERDO No. 003-2012
(de 22 de mayo de 2012)

"Por el cual se establecen lineamientos para la gestión del riesgo de la tecnología de la información"

LA JUNTA DIRECTIVA
En uso de sus facultades legales, y

CONSIDERANDO

Que a raíz de la emisión del Decreto Ley 2 de 22 de febrero de 2008, el Órgano Ejecutivo elaboró una ordenación sistemática en forma de texto único del Decreto Ley 9 de 1998 y todas sus modificaciones, la cual fue aprobada mediante el Decreto Ejecutivo No. 52 de 30 de abril de 2008, en adelante la Ley Bancaria;

Que de conformidad con el numeral 1 del artículo 5 de la Ley Bancaria es objetivo de esta Superintendencia de Bancos velar porque se mantenga la solidez y eficiencia del sistema bancario;

Que de conformidad con el numeral 2 del artículo 5 de la Ley Bancaria es objetivo de esta Superintendencia de Bancos fortalecer y fomentar condiciones propicias para el desarrollo de Panamá como centro financiero internacional;

Que de conformidad con el artículo 11, numeral 5 de la Ley Bancaria, corresponde a la Junta Directiva fijar, en el ámbito administrativo, la interpretación y alcance de las disposiciones legales o reglamentarias en materia bancaria;

Que de conformidad artículo 11 numeral 10 de la Ley Bancaria, es una atribución de carácter técnico de esta Junta Directiva dictar las normas técnicas necesarias para el cumplimiento de la Ley Bancaria;

Que de conformidad con lo establecido en el artículo 16, numeral 22, son atribuciones de carácter técnico del Superintendente, evaluar los indicadores financieros de los bancos y de los grupos bancarios que permitan dar seguimiento a los principales riesgos bancarios, tales como adecuación de capital, crédito, liquidez, operacional, mercado y otros que la Superintendencia estime conveniente;

Que mediante Acuerdo No. 008-2010 de 1 de diciembre de 2010, esta Superintendencia dictó las disposiciones sobre Gestión Integral de Riesgo, por el cual se requiere a los bancos la identificación y gestión de todos los riesgos a los que se encuentran expuestos de acuerdo al tamaño y complejidad de sus operaciones productos y servicios;

Que mediante Acuerdo No. 005-2011 de 20 de septiembre de 2011, esta Superintendencia actualizó las disposiciones sobre Gobierno Corporativo, estableciendo lineamientos claros para la organización del gobierno corporativo de las entidades bancarias;

Que mediante Acuerdo No. 7-2011 se dictaron los parámetros mínimos para la gestión del riesgo operativo, el cual en su artículo 7 establece la tecnología de la información como un factor o categoría de riesgo, la cual por su naturaleza debe ser gestionada de forma especializada;

Que el Principio No. 7 para una supervisión bancaria efectiva del Comité de Basilea, establece que los bancos deben contar con un proceso integral de gestión de riesgo, que incluya la vigilancia por la junta directiva y la gerencia superior, para identificar, evaluar, vigilar y controlar o mitigar todos los riesgos sustanciales y evaluar su suficiencia de capital global con respecto a su perfil de riesgo;

Que el rápido desarrollo de tecnologías conlleva beneficios y riesgos en la operación de los bancos, por lo cual es necesario establecer lineamientos mínimos para llevar a cabo la gestión de los riesgos asociados con la tecnología de la información, acorde a las mejores prácticas internacionales;

Que en sesiones de trabajo de esta Junta Directiva, se ha puesto de manifiesto la necesidad y conveniencia de establecer criterios mínimos para la gestión de los riesgos asociados con la tecnología de la información.

ACUERDA

CAPÍTULO I
ASPECTOS GENERALES

ARTÍCULO 1. ÁMBITO DE APLICACIÓN. Las disposiciones del presente Acuerdo se aplicarán a los bancos oficiales, a los bancos de licencia general y a los bancos de licencia internacional de los cuales esta Superintendencia sea el supervisor de origen.

ARTICULO 2. DEFINICIONES. Para los efectos del presente Acuerdo los siguientes términos se entenderán así:

1. **Gobierno de tecnología de la información:** conjunto de procesos, responsabilidades, políticas, procedimientos, relaciones y controles que apoyan las metas del negocio, optimizan las inversiones y administran los riesgos y oportunidades asociados a la tecnología de la información.
2. **Riesgo de tecnología de la información**. es la posibilidad de pérdidas económicas derivadas de un evento relacionado con la infraestructura tecnológica, el acceso o el uso de la tecnología, que afecta el desarrollo de los procesos del negocio o de la gestión de riesgos del banco, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad, cumplimiento o uso oportuno de la información.
3. **Tecnología de la información o "TI":** conjunto de instrumentos tecnológicos que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro, acceso y presentación de información.
4. **Seguridad de la información:** es la preservación de la confidencialidad, integridad y disponibilidad de la información en sí y de los demás recursos informáticos de la organización. Adicionalmente incluye el cumplimiento de las leyes, regulaciones, convenios, acuerdos y contratos asociados al uso y administración de los recursos informáticos y el manejo en general de la información.

CAPÍTULO II
GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN

ARTICULO 3. GOBIERNO DE TI. Los bancos deberán contar con una estructura organizacional acorde a su tamaño, complejidad de sus operaciones y perfil de riesgo, que les permita gestionar la TI y sus riesgos asociados.

El gobierno de TI deberá establecer políticas, planes estratégicos y procedimientos, así como la asignación de recursos necesarios para la gestión de TI, que serán revisadas de manera permanente y continua, enfocándose como mínimo en los siguientes aspectos:

1. **Alineación estratégica**: elaborar un plan estratégico de TI en el que se defina las iniciativas de TI alineadas con las metas del negocio, sus planes y operaciones, para lo cual debe contar con la identificación de los objetivos a corto, mediano y largo plazo de las actividades y proyectos de TI.

2. **Entrega de valor**: gestionar la TI asegurándose que genere los beneficios proyectados en el plan estratégico.
3. **Administración de recursos**: administrar de forma óptima y adecuada los recursos de TI, tales como el recurso humano y la infraestructura tecnológica, asegurando el desarrollo y monitoreo de un presupuesto para la administración de dichos recursos.
4. **Administración de riesgos**: identificar, comprender y administrar los riesgos a los que se encuentra expuesto, así como determinar su tolerancia al riesgo. Para ello debe contar con una metodología de administración de riesgos de TI que incluya el diseño de una matriz de riesgos y que garantice la seguridad de los sistemas, incluyendo, como mínimo, medidas de control de la seguridad lógica (permisología para acceso a los sistemas), de seguridad física y de seguridad de las redes.
5. **Medición del desempeño**: dar seguimiento permanentemente a la implementación de la estrategia de TI mediante la revisión continua del desempeño de los procesos y el logro de los objetivos y metas de TI, así como a la terminación de sus proyectos, uso de los recursos y entrega del servicio.

ARTÍCULO 4. CRITERIOS DE CONTROL DE TI. Los bancos deberán definir los objetivos de TI, los que deberán estar alineados con los objetivos del negocio. Para tales efectos, deberán implementar controles específicos relacionados a la TI, que se ajusten a los siguientes criterios:

1. **Efectividad:** la información y los procesos relacionados deberán ser pertinentes y adecuados para cumplir con sus objetivos. La información debe presentarse de forma precisa y de manera que pueda utilizarse oportunamente.
2. **Eficiencia:** los recursos en la aplicación de los procesos relacionados a la información deben optimizarse.
3. **Confidencialidad**: la información deberá estar protegida del acceso y uso no autorizado.
4. **Integridad:** la información deberá ser completa, exacta, fiable y veraz.
5. **Disponibilidad**: acceso oportuno y en forma organizada de la información.
6. **Cumplimiento normativo**: que la información cumpla con las políticas internas, estipulaciones contractuales y las leyes y regulaciones aplicables.

ARTICULO 5. RESPONSABILIDAD DE LA JUNTA DIRECTIVA. La junta directiva del banco es responsable de:

1. Aprobar el plan estratégico de TI y el plan de continuidad de negocios.
2. Velar porque se defina y se mantenga una estructura organizacional, las políticas y los procedimientos que permitan gestionar la TI y sus riesgos asociados, acorde a su tamaño, naturaleza y complejidad de las operaciones que realiza.
3. Velar que el gobierno de TI, como parte del gobierno corporativo, se maneje de forma adecuada.
4. Velar para que se realicen auditorías periódicas para la evaluación, revisión y seguimiento permanente de la función y operación de la TI.
5. Aprobar las prioridades de inversión de TI de conformidad con los objetivos del negocio.

ARTÍCULO 6. COMITÉ DE TI. Todo banco deberá constituir un comité de TI, el cual velará por la gestión de la TI del banco.

El comité de TI deberá estar conformado por la gerencia superior, las áreas de negocios y área responsable de TI. La cantidad de miembros que conformen dicho comité dependerá del tamaño y complejidad del banco.

El comité de TI elaborará su reglamento interno de trabajo, y contendrá las políticas y procedimientos para el cumplimiento de sus funciones. Dicho reglamento se adecuará a las disposiciones emitidas por esta Superintendencia, incluyendo el presente Acuerdo, y establecerá entre otros aspectos, la periodicidad de sus reuniones así como la información que deberá ser remitida a la junta directiva que sea pertinente al gobierno de TI.

Por razones de su estructura organizativa, un banco podrá solicitar al Superintendente dispensa de lo establecido en el presente artículo, siempre que éste evidencie, a satisfacción de esta

Superintendencia, que en todo caso las responsabilidades que corresponden al comité de TI quedan cubiertas por una instancia responsable.

ARTÍCULO 7. RESPONSABILIDADES DEL COMITÉ DE TI. Son funciones del comité de TI las siguientes:

1. Proponer a la junta directiva, para su aprobación, el plan estratégico de TI alineado a la estrategia de negocio del banco.
2. Proponer a la junta directiva, para su aprobación, las prioridades de inversión de TI de conformidad con los objetivos de negocio del banco.
3. Dar seguimiento a los proyectos de TI que se ejecuten en el marco del plan estratégico de TI.
4. Supervisar los niveles de servicio de TI.

CAPÍTULO III
GESTIÓN DE RIESGO DE TI

ARTÍCULO 8. GESTIÓN DE RIESGOS DE TI. Los bancos deberán identificar, medir, dar seguimiento, controlar, mitigar e informar a las áreas operativas de los riesgos de TI a los que se encuentran expuestos, de acuerdo al tamaño y complejidad de sus operaciones, productos y servicios.

ARTÍCULO 9. COMITÉ DE RIESGOS. El comité de riesgos, establecido en el Acuerdo sobre Gestión Integral de Riesgos, estará a cargo de la dirección de la administración del riesgo tecnológico, además de los otros riesgos, para lo cual deberá encargarse de la implementación, adecuado funcionamiento y ejecución de las políticas y procedimientos aprobados para dicho propósito y tendrá las funciones siguientes:

1. Proponer a la junta directiva, para su aprobación, las políticas y procedimientos para la administración del riesgo de TI y el plan de continuidad de negocios.
2. Proponer a la junta directiva el manual de gestión del riesgo de TI y sus actualizaciones.
3. Analizar las propuestas sobre actualización de las políticas, procedimientos, plan estratégico de TI, plan de continuidad de negocio y su plan de pruebas, y proponer a la junta directiva las actualizaciones que se ameriten.
4. Definir la estrategia para la implementación de las políticas y procedimientos aprobados para la gestión del riesgo de TI y su adecuado cumplimiento.
5. Revisar, al menos anualmente, las políticas y procedimientos sobre la gestión del riesgo de TI y proponer su actualización, cuando proceda.

ARTÍCULO 10. UNIDAD RESPONSABLE DE LA ADMISTRACIÓN DEL RIESGO. La unidad de administración de riesgo u otra unidad equivalente responsable existente en el banco, tendrá entre sus funciones la gestión de los riesgos de TI, debiendo cumplir, además de las responsabilidades establecidas en el Acuerdo sobre Gestión Integral de Riesgo, con lo siguiente:

1. Gestionar el riesgo de TI.
2. Analizar, revisar e implementar los controles tecnológicos y operativos necesarios para la debida administración del riesgo inherente de las innovaciones de TI que se implementen en el banco, así como de los nuevos productos y servicios propuestos por las unidades de negocios.

ARTÍCULO 11. UNIDAD DE SEGURIDAD DE LA INFORMACIÓN. Para velar por la seguridad de la información, la Unidad de Seguridad de la Información, constituida de conformidad con lo establecido en el Acuerdo sobre Banca Electrónica, tendrá entre sus funciones, como mínimo, las siguientes:

1. Establecer, revisar y actualizar las políticas, normas, procedimientos según los estándares internacionales de seguridad de la información.
2. Velar por la seguridad del entorno tecnológico, realizando análisis de riesgos de las aplicaciones y equipos tecnológicos de la institución.
3. Mantener los sistemas protegidos ante nuevas amenazas y vulnerabilidades existentes.

4. Velar que el banco no se vea afectado por nuevas amenazas, garantizando la disponibilidad de los sistemas para brindar el servicio.
5. Mantener actualizado y capacitado al personal de seguridad de la información.
6. Establecer comunicación con los miembros de seguridad de la información de otros bancos con la finalidad de trabajar en conjunto para fortalecer la seguridad del sistema bancario.
7. Coordinar la realización de análisis y de pruebas de intrusión y vulnerabilidad en el entorno tecnológico del Banco.
8. Establecer los lineamientos y estándares para controlar el acceso a los sistemas de información y la modificación de privilegios o perfiles de los usuarios.
9. Participar en el mantenimiento y actualización de los planes de contingencia, planes de continuidad del negocio y planes de recuperación de desastre para mantener el nivel de seguridad durante las actividades de recuperación.
10. Monitorear y atender los incidentes de seguridad de la información.
11. Notificar, en caso de sufrir ataques, a la Superintendencia mediante el formulario establecido.

ARTÍCULO 12. PLAN DE CONTINUIDAD DE NEGOCIOS Y RECUPERACIÓN DE DESASTRES. Los bancos deben asegurarse que en su plan de continuidad de negocios, según lo establecido en el Acuerdo sobre Gestión de Riesgo Operativo, se incluyan los siguientes aspectos relacionados a la TI:

1. Pruebas de resistencia diseñadas para mitigar el impacto de una interrupción mayor de las funciones y de los procesos clave del negocio.
2. El procesamiento alternativo, incluyendo el debido respaldo de la información y los sistemas.
3. La capacidad de recuperación de los servicios críticos de TI.
4. Los procesos de comunicación y el enfoque de pruebas.

ARTICULO 13. AUDITORÍA INTERNA. Todo banco deberá asegurarse, de acuerdo al tamaño y complejidad de sus operaciones, que su auditoría interna cuenta con los recursos y herramientas necesarias para llevar a cabo la auditoría y evaluación de todos los elementos de la TI, con la finalidad de determinar las deficiencias y sus posibles soluciones.

ARTÍCULO 14. TERCERIZACIÓN. Todo banco que tercerice las funciones o procesos de TI, deberá asegurarse que las mismas se ajusten a lo establecido en el Acuerdo sobre Tercerización emitido por esta Superintendencia de Bancos.

Adicionalmente, el banco se asegurará que en el contrato de tercerización se incluyan las siguientes condiciones:

1. La obligación de la empresa contratada de permitir a la Superintendencia de Bancos, cuando ésta así lo requiera, el acceso a la infraestructura de TI, a los sistemas de información y bases de datos (en la medida de lo permitido en la Ley Bancaria), en lo que se refiere al servicio tercerizado por el banco.
2. La obligación de la empresa contratada de remitir al banco toda la información que requiera la Superintendencia respecto al servicio tercerizado por el banco, en la medida de lo permitido en la Ley Bancaria.

CAPITULO IV
DISPOSICIONES FINALES

ARTÍCULO 15. SANCIONES. El incumplimiento de las disposiciones contenidas en el presente Acuerdo será sancionado por el Superintendente con arreglo a lo dispuesto en el Título IV de la Ley Bancaria.

ARTÍCULO 16. VIGENCIA. El presente Acuerdo comenzará a regir a partir del primero (1) de enero de dos mil trece (2013).

Dado en la ciudad de Panamá, a los veintidós (22) días del mes de mayo de dos mil doce (2012).

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

EL PRESIDENTE **EL SECRETARIO**

Arturo Gerbaud De La Guardia Félix B. Maduro