NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO

RESOLUCIÓN No. CD-SIBOIF-437-1-AGOS14-2006
De fecha 14 de Agosto de 2006

Publicada en La Gaceta No. 183 del 21 de Septiembre del 2006

EL CONSEJO DIRECTIVO DE LA SUPERINTENDENCIA DE BANCOS Y DE OTRAS INSTITUCIONES FINANCIERAS

CONSIDERANDO

I

Que es objetivo de esta Superintendencia promover que las instituciones supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, limitar, controlar y reportar los riesgos que enfrentan, con el fin de mitigar o eliminar el posible impacto negativo de dichos riesgos;

II

Que entre los riesgos que enfrentan las instituciones supervisadas en el desarrollo de sus actividades se encuentran los riesgos operativos, los cuales pueden generarse por deficiencias o fallas en los procesos internos, en la Tecnología de Información (TI), en las personas o por ocurrencia de eventos externos;

III

Que es necesario establecer los criterios mínimos prudenciales para la identificación y administración de los riesgos asociados a la Tecnología de Información, a fin de contribuir positivamente a la estabilidad y eficiencia del sistema financiero;

IV

Que con base en las facultades que le confiere el artículo 3, numeral 13 y el artículo 10 de la Ley No. 316, Ley de la Superintendencia de Bancos y de Otras Instituciones Financieras, reformados por la Ley No. 552, Ley de Reformas a la Ley No. 316, Ley de la Superintendencia de Bancos y de Otras Instituciones Financieras; y los artículos 40 y 134 de Ley No. 561, Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros;

En uso de sus facultades,

HA DICTADO

La siguiente:

NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO

RESOLUCIÓN No. CD-SIBOIF-437-1-AGOS14-2006

CAPÍTULO I
OBJETO, ALCANCE Y CONCEPTOS

Artículo 1.- Objeto
La presente norma tiene como objeto establecer los criterios mínimos para la identificación y administración de los riesgos asociados a la TI, a fin de contribuir positivamente a la seguridad, estabilidad, y eficiencia del uso de dicha tecnología por el sistema financiero.

Artículo 2.- Alcance
Las disposiciones de la presente norma son aplicables a todas las instituciones financieras sujetas ala autorización, supervisión y vigilancia de la Superintendencia de Bancos y de Otras Instituciones Financieras, en lo que les sea conducente.

Artículo 3.- Conceptos
Para efectos de la presente norma se establecen los siguientes conceptos:

a) Alta Gerencia: La persona que en las instituciones financieras ocupe el cargo de ejecutivo principal (Director General, Director Ejecutivo, Gerente General).

b) Análisis de Impacto de Negocio: Etapa de la planeación de continuidad de negocio en la que se identifican los eventos que podrían tener un impacto sobre la continuidad de operaciones y su impacto financiero, humano y de reputación sobre la institución.

c) Base de Datos: Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de la institución.

d) Bitácora: Registro manual o electrónico que provee información necesaria para identificar e investigar alguna actividad, problema o incidente.

e) BS17799 (British Standards 17799): Mejor Práctica para la Seguridad de la Tecnología de la Información creado por el Instituto de Estándares del Gobierno de Gran Bretaña y retomado luego por ISO con el nombre ISO 7799.

f) COBIT (Control Objectives for Information and Related Technology): Estándar o Mejor Práctica generalmente aplicable y aceptada en el control y seguridad de las TI, emitido por ISACA (*Information Systems Audit and Control Foundation*).

g) Control: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para procurar que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos, detectados y corregidos.

h) Denegación de Servicios: Es un ataque a un servicio o recursos que provoca que este mismo sea inaccesible a sus usuarios.

i) Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

j) Instituciones: Los bancos e instituciones financieras no bancarias sujetas a la autorización, supervisión, vigilancia y fiscalización de la Superintendencia de Bancos y de Otras Instituciones Financieras.

k) Manual de Funciones: Contiene las funciones y responsabilidades de cada uno de los puestos que conforman la estructura organizativa del área a cargo de la Tecnología de Información, puede considerarse como manual de funciones la colección de fichas ocupacionales del personal.

l) Muro de Fuego (Firewall): Todo Hardware o Software y sus políticas que son utilizados como medida de control sobre el tráfico entrante y saliente entre una red y otra.

m) Objetivo de Control: Definición del propósito o resultado que se desea alcanzar mediante la implementación de controles específicos en una actividad de TI.

n) Plan de Contingencia: Documento donde se detallan los procedimientos por seguir en caso de una contingencia, con el fin de no afectar el funcionamiento normal de la institución. Tiene como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

o) Políticas: Conjunto de prácticas establecidas por la Junta Directiva de la institución, por medio de las cuales se definen los cursos de acción a seguir por la Administración.

p) Procedimiento: Método o sistema estructurado para ejecutar instrucciones. Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.

q) Proceso Crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la institución, y cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la institución.

r) Riesgo Operativo: Es el riesgo de pérdida debido a la inadecuación o fallos de los procesos, personal y los sistemas internos o bien a causa de acontecimientos externos.

s) Riesgos de Tecnología de Información: Perdida potencial por daño, interrupción, alteración o fallas derivadas del uso o dependencia en la TI que soporta los procesos críticos de la Institución Financiera.

t) Seguridad Lógica: Seguridad a nivel del Software para proteger los datos, procesos y sistemas.

u) Tecnología de Información (TI): Se traduce en hardware, software, sistemas de información, investigación

tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática.

CAPÍTULO II
PLANEACIÓN, ORGANIZACIÓN Y GESTIÓN

Artículo 4.- Responsabilidad de la Junta Directiva y Alta Gerencia
La Junta Directiva de cada institución será responsable de aprobar los objetivos, lineamientos y políticas para administrar de manera adecuada y prudente los riesgos de tecnología de información, incidiendo positivamente en los procesos críticos asociados a dicho riesgo. También será su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos, y de las disposiciones contenidas en la presente norma. Para tales efectos la Junta Directiva deberá considerar lo establecido en las mejores prácticas Internacionales para control y seguridad de la TI tales como COBIT e BS17799, además de las guías sobre la materia que emita el Superintendente.

Así mismo, la Junta Directiva deberá revisar cuando menos una vez al año los objetivos, lineamientos y políticas antes referidos. Corresponderá a la Alta Gerencia la implementación de las políticas y procedimientos generales establecidos por la Junta Directiva.

Artículo 5.- Estructura Organizacional y Procedimientos
Las instituciones deberán definir y mantener una estructura organizacional y procedimientos que les permita administrar adecuadamente los riesgos asociados a la TI, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan. El área a cargo de TI debe tener una ubicación dentro de la organización que le asegure independencia, autoridad y una adecuada segregación de funciones.

El área encargada de TI deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico. La gerencia deberá asegurarse que el personal lleve acabo únicamente aquellas tareas estipuladas para sus respectivos puestos.

El área encargada de TI deberá definir e implementar procedimientos relevantes para controlar las actividades de consultores y demás personal externo contratado para asegurar la protección de los activos de información de la organización.

Artículo 6.- Planeación Estratégica y Operativa
El área encargada de TI será responsable de desarrollar planes de largo y corto plazo de TI que apoyen el logro de la misión y las metas generales de la Institución. Dichos planes deben estar debidamente aprobados por la Junta Directiva o el órgano competente.

La Institución Financiera debe crear y actualizar regularmente un plan de Infraestructura Tecnológica de acuerdo a las mejores prácticas internacionales y en concordancia con los planes a largo y corto plazo de TI. Dicho plan deberá abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración. Este Plan deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura). De igual manera deberá establecerse un marco de referencia general referente a la adquisición y mantenimiento de la infraestructura de tecnología.

Artículo 7.- Administración del Riesgo Tecnológico
Las instituciones deberán administrar apropiadamente los riesgos asociados a TI, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas informáticos y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para este fin, las instituciones deberán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

La administración del riesgo tecnológico debe permitir el adecuado cumplimiento de los siguientes criterios de control interno:

a) Eficacia. La información debe ser relevante y pertinente para los objetivos de la institución y ser entregada en una forma adecuada y oportuna conforme las necesidades de los diferentes niveles de decisión y operación de la institución.

b) Eficiencia. El proceso de la Información debe realizarse mediante una óptima utilización de los recursos.

c) Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.

d) Integridad. La información debe ser completa, exacta y válida.

e) Disponibilidad. La información debe estar disponible en tiempo y en forma organizada para los usuarios autorizados cuando sea requerida.

f) Cumplimiento Normativo. La información debe cumplir con los criterios y estándares internos de la institución, las regulaciones definidas externamente por el marco legal aplicable y las correspondientes entidades reguladoras, así como los contenidos de los contratos pertinentes.

Artículo 8.- Administración de Nuevos Proyectos
La Junta Directiva deberá establecer un marco referencial general para la administración de proyectos que defina el alcance, límites y metodología de administración de proyectos. Dicha metodología deberá cubrir, como mínimo: la asignación de responsabilidades, bases para asignar al equipo de trabajo y sus responsabilidades, participación de las áreas usuarias, determinación de tareas, presupuestos de tiempo y recursos, los avances, los criterios y puntos de revisión y aprobación y de las revisiones post-implementación.

Cada proyecto debe contar con un escrito claro aprobado por la Junta Directiva o el órgano que esta designe, donde se definan la naturaleza y alcance del proyecto, las funciones de los integrantes del proyecto y áreas usuarias y las bases de aprobación de cada fase del proyecto.

Artículo 9.- Administración de las Operaciones y Comunicaciones
Las instituciones deberán establecer medidas de administración de las operaciones y comunicaciones, que entre otros aspectos contendrán lo siguiente:

a) Control sobre los cambios en el ambiente operativo, que incluye cambios en los software, las instalaciones de procesamiento y los procedimientos;

b) Control sobre los cambios del ambiente de desarrollo al de producción;

c) Separación de funciones para reducir el riesgo de error o fraude;

d) Separación del ambiente de producción y el de desarrollo;

e) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares;

f) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas; y

g) Seguridad sobre correo electrónico, banca electrónica e Internet.

Artículo 10.- Administración y Monitoreo de los Niveles de Servicio
Las instituciones deberán establecer estrategias y procedimientos de trabajo orientados a garantizar a los usuarios internos y clientes del banco, los niveles de disponibilidad y respuesta de los servicios soportados en TI, prestados y/o recibidos, ya sean brindados por la Institución o por Terceros.

Artículo 11.- Estándares de Desarrollo y Mantenimiento
El área a cargo de TI deberá definir e implementar estándares de sistemas de información y adoptar una metodología de ciclo de vida del sistema que rija el proceso de adquisición, desarrollo, implementación y mantenimiento de sistemas computarizados y tecnología afín, debiendo incorporar estándares para la documentación de procesos y programas, requerimientos de pruebas, verificación de software, definiendo condiciones bajos las cuales deberán conducirse las pruebas pilotos o en paralelo de los sistemas nuevos y/o actuales y revisiones post-implementación, además de los criterios de certificación, aceptación y aprobación por parte del usuario.

Artículo 12.- Administración de Problemas e Incidentes
El área a cargo de TI debe definir e implementar un sistema de administración de problemas, incidentes y errores para asegurar que los eventos operacionales que no formen parte de la operación normal, sean registrados en una bitácora, analizados y resueltos. Esta bitácora deberá conservarse por tiempo indefinido para utilizarla como memoria del conocimiento y facilite la solución de problemas futuros similares.

Artículo 13.- Documentación
El área a cargo de TI debe elaborar y mantener actualizada, al menos la siguiente documentación:

a) De los sistemas aplicativos; la operación de los procesos informáticos; los procesos de recuperación de datos y archivos; los procesos de copias y resguardo de datos; la seguridad física y lógica; la administración de la red de telecomunicaciones; los procedimientos para la puesta en marcha de programas en producción; el tratamiento de los requerimientos de usuarios; los manuales técnicos y de usuario; los procedimientos de transferencia electrónica de fondos, procesos especiales de cierre de fin de año, etc.

b) El equipamiento informático, que incluya diagramas y distribución física de las instalaciones, inventario de “hardware” y “software” de base, diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos, etc.

Esta información comprende tanto al centro principal de procesamiento de datos como los secundarios, redes departamentales, sucursales, transferencias de fondos y el centro alternativo para contingencias.

Artículo 14.- Subcontratación (Outsourcing)
Cuando ciertas funciones o procesos puedan ser objeto de una subcontratación, la institución deberá proceder conforme la norma que regula la materia.

CAPÍTULO III
ADMINISTRACIÓN DE LA SEGURIDAD

Artículo 15.- Administración de la Seguridad de Información
La Junta Directiva o la instancia delegada por a misma deberá establecer, mantener y documentar un sistema de administración de la seguridad de la información, en adelante “Plan de Seguridad de la Información (PSI)”. El PSI debe incluir los activos de tecnología que deberán ser protegidos, la metodología usada, los objetivos de control, controles y el nivel de seguridad requerido.

Las actividades mínimas que deberán desarrollarse para implementar el PSI, son las siguientes:

a) Definición de una política de seguridad.

b) Evaluación de riesgos de seguridad a los que está expuesta la información.

c) Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.

d) Plan de implementación de los controles y procedimientos de revisión periódicos.

e) Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la institución, así como mantener pistas de auditoría adecuadas.

Artículo 16.- Aspectos de la Seguridad de Información

Para la administración de la seguridad de la información, las instituciones deberán tomar en consideración los siguientes aspectos:

a) Seguridad Lógica
Las instituciones deberán definir una política para el control de accesos, que incluya los criterios para la concesión, administración y revocación de los accesos al software, redes y sistemas operativos, así como los derechos y atributos que se confieren.

Entre otros aspectos, debe contemplarse lo siguiente.

1) Procedimientos formales para la concesión, administración y revocación de derechos, perfiles y usuarios. Deberán efectuarse revisiones periódicas sobre los derechos concedidos a los usuarios.

2) Políticas de uso de Usuarios genéricos y control de no repudiación de responsabilidades.

3) Los usuarios deberán contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.

4) Controles especiales sobre utilidades del sistema, herramientas de auditoría y las funciones realizadas por usuarios con altos privilegios en los Sistemas de Información y Tecnologías relacionadas.

5) Seguimiento sobre el acceso y uso de los sistemas y otras instalaciones físicas, para detectar actividades no autorizadas.

6) Usuarios remotos y computación móvil.

7) Usuarios, componentes y sus privilegios relacionados a los servicios de comercio electrónico y banca por Internet.

b) Seguridad de Personal
Las instituciones deberán definir procedimientos para reducir los riesgos asociados al error humano, robo, fraude o mal uso de activos, vinculados al riesgo de TI. Al establecer estos procedimientos, deberá tomarse en consideración, entre otros aspectos, la adecuada definición de roles y responsabilidades establecidos sobre la información y su procesamiento, verificación de antecedentes, políticas de rotación y vacaciones, control cruzado y compartido de operaciones sensitivas, y entrenamiento constante.

c) Seguridad Física y Ambiental
Las instituciones deberán definir adecuados controles físicos y ambientales al acceso, daño o interceptación de información en dependencia del nivel de protección requerido. El alcance incluirá las instalaciones físicas, áreas de trabajo, equipamiento, cableado, entre otros bienes físicos susceptibles a riesgos de seguridad.

d) Clasificación de Seguridad
Las instituciones deberán realizar un inventario periódico de activos físicos y lógicos asociados a la TI que tenga por objetivo proveer la base para una posterior clasificación de seguridad de acuerdo a la política de clasificación de activos, dictada por la Junta Directiva o la instancia competente. Esta clasificación debe indicar el nivel de criticidad, riesgo existente y seguridad requerida por la institución.

e) Seguridad en el Desarrollo y Mantenimiento de Sistemas
Para la administración de la seguridad en el desarrollo y mantenimiento de sistemas informáticos, se deberá tomar en cuenta, entre otros, los siguientes criterios:

1) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso, procesamiento y salida de la información;

2) Definición e implementación de pistas de auditorías;

3) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida;

4) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción (durante período de pruebas y/o paralelos);

5) Controlar el acceso a las librerías de programas fuente, bases de datos y archivos de respaldos;

6) Mantener un estricto y formal control de cambios; y

7) Velar por la existencia de ambientes separados en el desarrollo y producción.

CAPÍTULO IV
PLANES DE CONTINGENCIA Y DE RECUPERACIÓN

Artículo 17.- Procedimientos de Respaldo
Las instituciones deberán establecer procedimientos de respaldos regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas deben ser probadas periódicamente para verificar su efectividad y ser coherentes con lo requerido en el Plan de Contingencia.

La institución debe conservar la información de respaldo y los procedimientos de restauración, debiendo resguardar con una frecuencia razonable una copia de los mismos en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

La política de respaldos y el mantenimiento de data histórica debe tomar en cuenta: los estudios de criticidad de los procesos e información, los tiempos objetivos de recuperación y restauración y el tiempo de resguardo de registros considerando las disposiciones legales vigentes.

Artículo 18.- Diseño e Implementación del Plan de Contingencia

La Institución debe establecer un proceso de planeación de contingencia que provea los procedimientos y la capacidad de dar continuidad al soporte general y a las aplicaciones críticas durante la contingencia y recuperación de un desastre, considerando una evaluación de riesgos asociados a la seguridad de la información y el desarrollo de sub-planes específicos para proteger, mantener y recuperar los procesos críticos de negocios a la menor brevedad posible.

El proceso de planeación de contingencia debe incluir las siguientes etapas:

a) Creación de una política de contingencia del negocio y de recuperación de desastres.

b) Análisis de impacto de negocio.

c) Clasificación de las operaciones y análisis de criticidad.

d) Análisis de tiempo mínimo de respuesta a los procesos críticos.

e) Definición de las estrategias de recuperación.

f) Desarrollo el plan de contingencia de negocios y procedimientos de recuperación de desastres.

g) Programa de entrenamiento, divulgación y concientización de los planes.

h) Prueba e implementación.

i) Monitoreo y actualización continúa de los planes.

El Plan de Recuperación de Desastres está dirigido a la ocurrencia de catástrofes que no permitan la utilización normal de las instalaciones de procesamiento de una institución por períodos extensos. Este plan debe permitir la restitución de los sistemas, aplicativos críticos y actividades de procesamiento de información en un sitio alterno bajo condiciones de operación adecuadas. El contenido de este plan puede coincidir en parte con el del plan de contingencia sin embargo su alcance es menor ya que no debe abarcar interrupciones menores que no requieran reubicación.

Artículo 19.- Pruebas del Plan de Contingencia
Las instituciones deberán realizar pruebas a su Plan de Contingencia para asegurar la efectividad del mismo (en tiempo y forma). El procedimiento, la frecuencia y profundidad de dichas pruebas debe responder a la evaluación formal y prudente que sobre dicho riesgo realice cada institución, debiendo realizar al menos una prueba al año.

El cronograma de pruebas, los resultados de pruebas efectuadas y el control de cambios sobre el plan derivado de las mismas deben ser formalmente documentados y estar disponibles a la Superintendencia cuando ésta lo requiera.

CAPÍTULO V
REQUERIMIENTOS DE INFORMACIÓN

Artículo 20.- Evaluación Anual del Riesgo Tecnológico
Las instituciones deberán realizar al menos una vez al año la evaluación del riesgo tecnológico que enfrenta la institución por proceso o unidad de negocio y apoyo. El informe de dicha evaluación debe ser presentado a la Junta Directiva o al órgano competente así como estar disponible para el Superintendente cuando este lo requiera. El informe deberá contemplar por lo menos los siguientes aspectos:

a) Metodología empleada para la administración del riesgo tecnológico y su engranaje dentro del marco de la administración del riesgo operacional e integral del banco.

b) Identificación del riesgo tecnológico por proceso o unidad de negocio y apoyo.

c) Medidas adoptadas para administrar los riesgos tecnológicos materiales identificados y plazos para su aplicación.

e) Funcionarios responsables de las actividades de control de riesgos identificadas.

f) Plan de actividades en lo referente a la administración del riesgo tecnológico.

Nota: Error en Gaceta, del inciso c pasa al inciso e; se omitió el inciso d

Artículo 21.- Notificaciones al Superintendente
La institución deberá informar previo a la contratación al Superintendente los siguientes temas y eventos, entre otros:

a) Eventos excepcionales tales como: intentos de ataques y penetraciones significativas, así como todos los incidentes de penetración a los sistemas; inoperatividad del sistema central o de producción; operación del plan de emergencia o cualquier otro similar;

b) La discontinuidad de servicios significativos para sus clientes, como consecuencia de un cierre no planificado de los sistemas computarizados, que dure más de un día de trabajo;

c) La decisión de realizar cambios significativos sobre las políticas de administración de las tecnologías de información, plataforma central de operaciones y sistemas computarizados; y

d) La decisión de expandir los niveles de servicio, un cambio material en los canales de comunicaciones o una nueva iniciativa de proporcionar servicios financieros por medios electrónicos.

Artículo 22.- Vigencia
La presente norma entrará en vigencia tres meses a partir de su notificación, exceptuando las disposiciones contenidas en los artículos 18 y 19 de la misma, los cuales entrarán en vigencia seis meses a partir de su notificación. Lo anterior sin perjuicio de su publicación en La Gaceta, Diario Oficial. **(f) José Rojas R. (f) Víctor Urcuyo V. (f) Antenor Rosales Bolaños (f) Roberto Solórzano Ch. (f) Gabriel Pasos Lacayo (f) A. Cuadra G. (f) U. Cerna B. URIEL CERNA BARQUERO**, Secretario Consejo Directivo SIBOIF.