NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO

RESOLUCIÓN No. CD-SIBOIF-500-1 SEP19-2007. Aprobado el 19 de Septiembre del 2007

Publicado en La Gaceta No. 208 del 30 de Octubre de 2007

El Consejo Directivo de la Superintendencia de Bancos y de Otras Instituciones Financieras,

CONSIDERANDO

I

Que es objeto 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 (TI), 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 Superintendecia de Bancos y de Otras Instituciones Financieras, reformados por la Ley No. 552, Ley de Reformas a la referida Ley 316; 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-500-1-SEP19-2007

CAPÍTULO I
CONCEPTOS, OBJETO Y ALCANCE

Arto. 1. Concepto.- Para efectos de la presente norma, se establecen los siguientes conceptos:

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

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) Cableado estructurado: Es un sistema de cable planificado para hacer frente a las re-configuraciones, la detección de fallas y el crecimiento futuro en una red que toma en cuenta requerimientos de seguridad, etiquetado, ordenamiento y flexibilidad.

f) Gobierno de TI: Estructura de relaciones y procesos para dirigir y controlar la institución con el objeto de lograr sus metas, agregando valor mientras exista un balance entre los riesgos y beneficios de TI y sus procesos.

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

h) Incidente: Cualquier evento que no forma parte de la operación normal de un servicio y que causa o puede causar, una interrupción o una reducción de calidad del mismo. Esto no incluye los requerimientos de cambios a la infraestructura tecnológica.

i) 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.

j) Mejores Prácticas Aplicables: Se entenderán como mejores prácticas, los marcos de referencia de control, estándares internacionales, u otros estudios que ayuden a monitorear y mejorar las actividades críticas de TI, aumentar el valor de negocio, y reducir riesgos tales como; COSO, COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2, entre otros.

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

l) Planeación de continuidad de negocio: Es un proceso diseñado para reducir el riesgo del negocio de la organización que surja de una interrupción inesperada de sus funciones u operaciones críticas, independientemente de si éstas son manuales o autorizadas, las cuales son necesarias para la supervivencia de la organización.

m) 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.

n) 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 cumplimento de una función operativa.

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

Fuente: http://www.leybook.com/doc/12773

p) Riesgos de Tecnología de Información: Daño, interrupción, alteración o fallas derivadas del uso de la TI que soporta los procesos críticos de la Institución y que conllevan a una pérdida financiera potencial.

q) Tecnología de la Información (TI): Hardware, Software, Sistemas de Información, Investigación Tecnológica, Redes Locales, Bases de Datos, Ingeniería de software, Telecomunicaciones, Servicios y Organización de Informática.

Arto. 2. Objeto.- La presente norma tiene por objeto establecer los criterios mínimos de evaluación sobre la administración de los riesgos, la seguridad, la utilización y los controles aplicados a la Tecnología de Información de las entidades supervisadas, con el fin de velar por la estabilidad y la eficiencia del sistema financiero.

Arto. 3. Alcance.- Las disposiciones de la presente norma son aplicables a todas las instituciones financieras sujetas a la autorización, supervisión y vigilancia de la Superintendencia de Bancos, en lo que les sea conducente.

CAPÍTULO II
CRITERIOS DE INFORMACIÓN

Arto. 4 Criterios de información.- Para efectos de la presente norma se deben tomar en consideración los siguientes criterios de información para el control y gestión de las tecnologías de información y sus riesgos asociados:

a) Confiabilidad: Los sistemas deben brindar información correcta, completa, oportuna y exacta, que será utilizada en la operación de la entidad y en la toma de decisiones, la preparación de estados financieros en información gerencial y su remisión a organismos reguladores.

b) Confidencialidad: Se debe brindar protección a la información sensible contra divulgación no autorizada.

c) Disponibilidad: Los recurso y la información deben estar disponibles en tiempo y forma, cada vez que sean requeridos por los usuarios.

d) Efectividad: La información y los procesos deben ser relevantes y pertinentes para el proceso del negocio, además de presentarse en forma correcta, coherentes, completa y que pueda utilizarse oportunamente.

e) Eficiencia: El proceso de la información debe realizarse mediante una óptima (más productiva y económica) utilización de los recursos.

f) Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

g) El cumplimiento: Se tienen que cumplir aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

CAPÍTULO III
PLANEACIÓN, ORGANIZACIÓN Y GESTIÓN

Arto. 5. Responsabilidad de la Junta Directiva y Alta Gerencia.- La Junta Directiva será responsable,

como mínimo, de lo siguiente:
a) Velar por la existencia de un Gobierno de Tecnología de Información.

b) Aprobar los objetivos, lineamientos y políticas generales para administrar de manera adecuada y prudente la seguridad y los riesgos de tecnología de la información, incidiendo positivamente en los procesos críticos asociados a dicho riesgos.

c) Fortalecer el contenido de las políticas referidas considerando lo establecido en las mejores prácticas aplicable y las guías de la materia que emita el superintendente.

d) Proveer los recursos necesarios para lograr cumplimiento de las referidas políticas y de las disposiciones contenidas en la presente norma.

e) Evaluar con una periodicidad no mayor a un (1) año el contenido aplicabilidad de las políticas institucionales de TI.

f) Velar por la implementación de sistemas de información propios o adquiridos que cumplan con los criterios de información mencionados en la presente norma.

g) Aprobar los planes de TI.

h) Asegurar por la disponibilidad, capacidad y el desempeño de los sistemas de información requeridos para la continuidad de procesos críticos de negocio.

i) Velar por el uso responsable de los recursos de TI.

j) Administrar adecuadamente los riesgos de TI.

Estas responsabilidades podrán ser delegadas en un comité o instancia designada, que deberá ser integrada al menos por el encargado de TI, un miembro de la Junta Directiva que no sea el ejecutivo principal, y los principales representantes de las áreas usuarias que se considere necesario de acuerdo a los temas a tratar.

Será responsabilidad de la alta gerencia el cumplimiento de las disposiciones que emanen de los órganos antes mencionados.

Arto. 6. Estructura organizacional y procedimientos.- Las instituciones en las cuales los procesos críticos se encuentren automatizados y cuya continuidad de negocios depende de sus sistemas de información deben al menos:

a) Garantizar la existencia de un área de TI que cuenten con independencia, autoridad y adecuada segregación de funciones ante las áreas a las que brinda servicios.
b) Definir formalmente las funciones del personal de TI garantizando segregación de funciones entre el personal y excluyendo la posibilidad de que una sola persona controle procesos u operaciones críticos relacionados a TI.

c) Definir los procedimientos para la contratación de nuevo personal de TI.

d) Implementar controles para asegurar que el personal de TI lleve a cabo únicamente las funciones correspondientes a sus respectivos puestos.

e) Contar con personal técnicamente calificado o contratarlo externamente.

La institución que por su tamaño o naturaleza de negocio no pueda contar con esta unidad organizacional, podrá solicitar al Superintendente ser exonerada total o parcialmente del cumplimiento de las disposiciones establecidas en el presente artículo.

Artículo 7. Planeación de tecnología de información.- Las instituciones deben realizar una planeación operativa y estratégica de TI (Corto y largo plazo) cuyos objetivos estén conforme a las metas institucionales, Dicha planificación deberá considerar como mínimo:

a) La cooperación de TI con las áreas usuarias relevantes.

b) La definición de cómo la TI dará soporte a los programas de inversión y la entrega de los servicios operacionales.

c) La definición de un plan de infraestructura tecnológica.

d) El cumplimiento de una política preestablecida de adquisición y mantenimiento de la infraestructura tecnológica.

e) La definición de cómo se cumplirán y medirán los objetivos, y como recibirá la autorización formal de los interesados.

f) Un presupuesto de la inversión de TI y las fuentes de financiamiento.

g) Las estrategias de adquisición.

h) Los requerimientos legales y regulatorios.

Arto. 8. Actualización de planes.- Los planes operativos y estratégicos referidos anteriormente, se deberán actualizar y evaluar el desempeño de los mismos, en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades. Dicha evaluación debe realizarse al menos anualmente.

CAPÍTULO IV
ADQUISICIÓN, DESARROLLO E IMPLEMENTACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Arto. 9. Aprobación de nuevos proyectos.- Las instituciones deberán definir sus propias políticas de aprobación de proyectos de TI donde se definan las instancias y niveles de aprobación de los mismos de acuerdo a la naturaleza y alcance del proyecto.

Arto. 10. Administración de nuevos proyectos.- Todo proyecto relacionado con tecnología de la información deberá contar con la documentación debida sobre todas sus etapas básicas; inicio, planificación, ejecución, control/monitoreo, y entrega final y/o recepción final. La gestión del proyecto deberá considerar al menos los siguientes aspectos:

a) Un estudio de viabilidad de proyecto escrito y aprobado tanto por el área de tecnología como por las áreas usuarias afectadas cuando aplique.

b) El establecimiento de un equipo de trabajo con representación del área de tecnología y áreas usuarias afectadas, con responsabilidades asignadas.

c) El establecimiento de un plan formal para la ejecución del proyecto.

d) La determinación de todas las fases requeridas en el proyecto incluyendo las fases de prueba, entrenamiento a usuarios, conversión e implementación

e) Procedimientos para verificar la ejecución del plan en el plazo y presupuesto estimado y que garantice que cualquier desviación del plan inicial sea debidamente aprobado y documentado.

f) Los procedimientos para la gestión de calidad y la gestión de riesgos asociados al proyecto.

g) La participación de la unidad de auditoria de forma pro-activa, realizando la evaluación de los resultados durante la ejecución y post-implementación del proyecto.

h) Criterios de aceptación de resultados y de las revisiones post-implementación.

i) Elaboración de actas de entrega o recepción del proyecto.

Arto. 11. Ciclo de vida del desarrollo de sistemas.- Toda institución cuyo desarrollo de sistemas se efectúe internamente debe contar con la documentación formal de una metodología de desarrollo que rija los procesos, análisis, diseño, desarrollo, implementación y mantenimiento de sistemas computarizados y tecnología.

El ciclo de vida de desarrollo de sistemas, además de las consideraciones para la gestión de proyectos, debe contener como mínimo los siguientes aspectos:

a) La documentación del análisis y diseño detallado del software considerando los requerimientos de usuario.

b) La determinación de requerimientos adicionales de hardware, software u otros elementos auxiliares.

c) Implementación de controles sobre el ingreso, procesamiento y salida de la información.

d) Definición y desarrollo de las pistas de auditoria.

e) La determinación sobre el uso de técnicas de encriptación sobre la información critica que debe ser protegida.

f) La determinación sobre las necesidades de capacitación y los planes de ejecución oportuna de las mismas

g) Existencia de ambientes separados de desarrollo (incluyendo prueba y certificación) y producción.

h) La ejecución de un plan de pruebas integral al software desarrollado, y la documentación de los resultados obtenidos de la prueba como soporte.

i) La determinación de ejecutar pruebas en paralelo y los criterios para terminar este proceso.

j) La determinación sobre la realización de pruebas de volumen de volumen (stress).

k) La determinación de los criterios de certificación, aceptación, y aprobación por parte del usuario.

l) La determinación de los procedimientos de conversión o traslados a producción.

m) Los procedimientos para asegurar la actualización oportuna de información técnica y de usuarios.

Arto. 12. Estándares de desarrollo y mantenimiento.- Toda función de desarrollo de software o programación, debe contar con estándares y convenciones de nomenclatura en sus códigos fuentes a fin de garantizar la continuidad operativa de los procesos de desarrollo y la capacidad de integración entre aplicaciones de software desarrolladas.

Arto. 13. Control de cambios.- Se deben definir adecuados procedimientos de cambios a producción para proteger los programas de aplicación de a cambios no autorizados. Los objetivos de control a considerar son, como mínimo:

a) El acceso a bibliotecas/librerías de programas debe esta restringido.

b) Se deben llevar a cabo revisiones de supervisión.

c) Las solicitudes de cambio deben estar aprobadas y documentadas.

d) Se debe evaluar el impacto potencial de los cambios y documentarlos.

e) La solicitud de cambio debe estar documentada en un formulario estándar, prestando particular atención a lo siguiente:

1) Las especificaciones de los cambios deben estar descritas adecuadamente.

2) El formulario de cambio debe ser firmado por el usuario solicitante.

3) El formulario de cambio debe ser revisado y aprobado.

4) El trabajo debe ser asignado a una analista, programador y el feje de grupo de programación debe ejercer su supervisión.

f) Se deben realizar procedimientos de prueba que garanticen los resultados deseados previos a realizar el traslado de cambios al ambiente de producción.

g) La unidad de auditoria interna debe seleccionar y analizar periódicamente una muestra de los cambios realizados a los programas, haciendo seguimiento incluso al formulario de mantenimiento, para determinar si los cambios fueron autorizados, verificar que el formulario tenga las aprobaciones debidas y comparar la fecha en el formulario con la fecha acordada para su actualización en producción.

h) Si un grupo independiente (Servicios Externos) actualiza los cambios a los programas en producción, la unidad de auditoria debe determinar si existen los procedimientos para asegurar que se cuenta con el formulario de solicitud de cambio y validar que no existan códigos maliciosos que puedan afectar a la institución en el cambio realizado antes de la actualización.

Arto. 14. Cambios de emergencia.- En situaciones donde se requiera llevar a cabo cambios de emergencia para resolver problemas del sistema y para posibilitar la continuidad de un procesamiento crítico, deben existir procedimientos para asegurar que se puedan realizar los arreglos de emergencia sin comprometer la integridad del sistema.

La ocurrencia de estos eventos deberá ser registrada y supervisada con minuciosidad.

Es responsabilidad de auditoria Interna monitorear que los cambios de emergencia ser realizan adecuadamente.

CAPÍTULO V
ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Arto. 15. Derechos de propiedad intelectual.-Las instituciones deben contar con las políticas y procedimientos documentados para asegurar que su plataforma tecnológica no sea usada para el resguardo, copia, distribución o uso de cualquier programa de aplicación, software de oficina, contenido multimedia o cualquier otro material en forma digital cuyos derechos no hayan sido adquiridos por la institución y cuyo uso no esté autorizado.

Arto. 16. Administración de software,- Las instituciones deben definir políticas y procedimientos para la adecuada instalación, mantenimiento y administración de software debidamente autorizado. Para esto la entidad debe considerar al menos:

a) Establecer prohibiciones y controles sobre la instalación de software no autorizado por la institución o que no corresponda al perfil del usuario.

b) Actualizar todo software con las últimas mejoras de seguridad publicadas por el proveedor, de la versión que este utilizando y que todavía cuenta con soporte por parte del proveedor. Se exceptúan de lo anterior las actualizaciones que puedan afectar o impactar negativamente los sistemas informáticos en producción de la institución.

c) En el caso de aplicaciones de negocio, mantener actualizada su documentación técnica y de usuario de acuerdo a los últimos cambios efectuados.

d) Mantener actualizado un inventario de los contratos con las empresas de servicios de desarrollo de software y de las licencias de software adquiridas con sus documentos soporte.

e) Procedimientos de control de versiones.

Arto. 17. Administración de base de datos.- La institución debe administrar adecuadamente sus bases de datos, para esto deberá considerar al menos:

a) Definir la arquitectura de información para organizar y aprovechar de la mejor forma los sistemas de información.

b) Establecer política y procedimientos actualizados relacionados con la instalación, administración, migración, mantenimiento, respaldo y seguridad de las bases de datos.

c) Definir mecanismos para controlar la integridad, disponibilidad, capacidad y el desempeño de las bases de datos.

d) Establecer procedimientos de activación, gestión y revisión de bitácoras, pistas de auditoría, etc.

e) Definir períodos de almacenamiento y eliminación de información, acordes con los requerimientos internos, legales y regulatorios.

f) Mantener actualizada la información técnica del diseño y funcionamiento de las bases de datos.

Arto. 18. Administración de hardware y comunicaciones.- La entidad debe administrar adecuadamente el hardware, las redes y las líneas de comunicación de misión crítica, considerando al menos lo siguiente:

a) Realizar estudios de capacidad y desempeño y del hardware y las líneas de comunicación, que permitan determinar en forma oportuna, necesidades de ampliación de capacidades o actualizaciones de equipo.

b) Establecer procedimientos de monitores y reporte del uso eficiente y efectivo de equipos.

c) Establecer mecanismos para procura que todas las redes instaladas, ya sean eléctricas, de voz de datos, cumplan con los requerimientos mínimos vigentes de cableado estructurado.

d) Asegurar la existencia de la documentación y el etiquetado de los equipos y cableado.

f) Asegurar que as condiciones climáticas y ambientales de las instalaciones de procesamiento y comunicaciones sean apropiadas para el buen funcionamiento de las mismas.

g) Mantener actualizados los contratos de proveedores, diagramas de red y comunicaciones, diagramas de distribución física, inventarios, configuración técnica y cualquier otra información requerida.

h) Los procedimientos de baja de equipos deben considerar que los medios de almacenamiento que contengan material sensitivo, deban ser físicamente destruidos o sobrescritos en forma segura en vez de utilizar las funciones de borrado estándar.

Arto. 19. Administración de las operaciones.-La institución debe garantizar que toda tarea o proceso interno de TI sea debidamente documentado, esto con el objetivo de lograr un entorno operativo que tenga un nivel adecuado de madurez.

La documentación a realizarse puede incluir entre otros a los procesos relacionados con:

a) El desarrollo, mantenimiento e implementación de TI.

b) La adquisición de hardware y de software.

c) Administración de operaciones de TI.

d) Operaciones día a día.

e) Operaciones centralizadas por lote y procesos de cierre contable.

f) Operaciones de soporte técnico o mesa de ayuda.

g) Operaciones de resolución de problemas.

h) Seguridad.

i) Administración de recursos humanos.

j) Procedimientos para monitorear el uso eficiente y efectivo de los recursos.

k) Administración general.

Dichos procesos deben evaluarse y actualizarse en un periodo no mayor a dos (2) años, para garantizar su calidad y ajuste a la realidad de la institución.

Es responsabilidad de la auditoria interna vigilar por que las funciones estén documentadas y sean ejercidas de acuerdo a su definición para producir los resultados deseados.

Arto. 20. Administración y monitoreo de los niveles de servicio.- Las instituciones deberán establecer estrategias y procedimientos de trabajo orientados a garantizar que los usuarios internos y clientes de la institución reciban los niveles mínimos requeridos de disponibilidad y tiempos de repuesta sobre los servicios proporcionados con tecnología de la información. Dicha disposición aplica a servicios brindados internamente o los que sean prestados por terceros.

CAPÍTULO VI
ADMINISTRACIÓN DE SERVICIOS PRESTADOS POR TERCEROS

Arto. 21. Servicios descentralizados.- Las instituciones que requieran descentralizar total o parcialmente los procesos de tecnología de la información, excluyendo los servicios de desarrollo de software, fuera de sus propias instalaciones o supervisión directa, deberá informar al Superintendente dicha situación con al menos treinta (30) días hábiles de anticipación al inicio de operaciones en el sitio remoto; esta información debe incluir al menos:

a) Las razones de este requerimiento.

b) El detalle de los procesos o actividades que serán descentralizadas.

c) Copia del acuerdo, contrato o cualquier documento donde se establezca la relación con la entidad encarada de brindar el servicio.

d) La descripción del entorno de procesamiento, del sitio remoto, los encargados de su operación y las responsabilidades de control.

La institución debe ajustar todas las actividades de procesamiento descentralizadas, conforme la norma que regula la materia sobre la contratación de proveedores de servicios.

Arto. 22. Subcontratación de servicios.- Cuando ciertas funciones o procesos puedan ser objeto de una subcontrataciones o tercerización, la institución deberá proceder conforme la norma que regula la materia sobre la contratación de proveedores de servicios.

Arto. 23. Adquisición de software a terceros.- Cuando una institución adquiera o tenga planes de adquirir aplicaciones informáticas para soportar procesos de negocio, deberá tomar en consideración al menos lo siguiente:

a) La definición de requerimientos iniciales y su comparación con las bondades del producto: El producto a seleccionar debe cumplir de la mejor forma posible las necesidades definidas.

b) Solicitar referencias de clientes: Se deben verificar las referencias suministradas por el vendedor para validar las aseveraciones sobre el funcionamiento del producto y la realización del trabajo efectuado por el vendedor.

c) Analizar la viabilidad y estabilidad financiera del vendedor: El vendedor que suministre o que dé soporte al producto debe tener buena reputación y por lo tanto, debe poder proveer evidencia d su estabilidad financiera. Los vendedores y productos nuevos presentan un riesgo substancialmente más alto par la organización.

d) Garantizar la disponibilidad de documentación completa y confiable: El vendedor debe estar dispuesto y debe poder suministrar la documentación técnica y de usuarios del sistema para su revisión antes de la adquisición. El nivel de detalle y de precisión que se encuentre en la documentación puede ser un indicador del detalle y de la precisión utilizada dentro del diseño y de la programación del sistema mismo.

e) Garantizar la existencia de soporte del vendedor: El vendedor debe tener disponible una línea completa de productos de apoyo para el paquete de software. Esto puede incluir una línea de ayuda permanente, entrenamiento/formación local durante su implementación, actualizaciones del producto, notificación automática de nuevas inversiones y mantenimiento local cuando se solicite.

f) Garantizar la disponibilidad del código fuente: El código fuente debe ser recibido del vendedor al inicio, o debe haber previsiones para la adquisición del código fuente incluyendo sus actualizaciones, en el caso de que el vendedor abandone el negocio.

g) Verificar el número de años de experiencia en el producto ofrecido: Más años indican estabilidad y familiaridad con el negocio que el producto respalda.

h) Obtención de una lista de actualizaciones recientes: Una lista corta de actualizaciones pudiera sugerir una falta de actualización continua del producto.

i) Obtener una lista de clientes usando el producto: La lista podría indicar la aceptación del producto en el mercado.

j) Pruebas de aceptación del producto: Se debe poder realizar pruebas al producto antes de adquirir compromisos de compra para verificar si realmente satisface los requerimientos establecidos.

CAPÍTULO VII
ADMINISTRACIÓN DE LA SEGURIDAD

Arto. 24. Responsabilidad en materia de seguridad.- A los efectos de la presente norma y sin perjuicio de las demás disposiciones aplicables, es responsabilidad de cada institución en materia de seguridad de la información lo siguiente:

a) Asegurar la integridad de de la información almacenada en sus sistemas de cómputo.

b) Preservar la confidencialidad de los datos sensitivos.

c) Asegurar el cumplimiento con la confianza depositada y de la obligación en relación con cualquier

información relativa a una persona identificada o identificable (es decir, sujeto de datos) en conformidad con su política de privacidad o leyes y regulaciones de privacidad aplicables.

d) Asegurar la disponibilidad continúa de sus sistemas de información.

e) Asegurar el cumplimiento a las leyes, regulaciones y normas aplicables.

Arto. 25. Políticas y procedimientos de seguridad.- La institución deberá establecer y mantener políticas y procedimientos de seguridad de la información, cuya estructura y contenido incluya, como mínimo:

A) Estructura o esquema:

1) Propósito: que defina el porqué fueron creados estos documentos y el beneficio esperados de los mismos.

2) Ámbito: debe definir su aplicabilidad.

3) Responsabilidad: el documento debe definir quien se hará responsable por la implementación apropiada de los lineamientos que contenga.

B) Políticas de seguridad:

a) Políticas sobre la clasificación y protección de activos de información: que considere los niveles de clasificación y la protección requerida de acuerdo a cada nivel, los controles de etiquetado de la información, controles sobre el almacenamiento y transmisión de información confidencial y controles sobre la destrucción segura de la información confidencial.

b) Políticas sobre la seguridad del acceso a los sistemas de información: que defina cómo serán identificados y autenticados todos los usuarios, los requerimientos estándares de control de acceso, y los eventos a auditarse en los sistemas.

c) Políticas sobre el adecuado de los equipos de computo: que defina quien puede hacer uso de los mismos y cómo pueden ser utilizados.

d) Políticas sobre el uso de Internet: que defina quienes pueden tener acceso y cómo debe ser el uso apropiado a este recurso.

e) Políticas sobre el uso de correo electrónico: que defina quienes pueden tener acceso y cómo debe ser el uso apropiado a este recurso.

Arto. 26. Educación y creación de conciencia en temas de seguridad: Todos los empleados de la institución, y cuando sea relevante los usuarios de terceras partes, deben recibir un entrenamiento apropiado y actualizaciones periódicas sobre la importancia de la seguridad en las políticas y procedimientos de la organización. Esto incluye requerimientos de seguridad, responsabilidades legales y controles del negocio, así como también entrenamiento en el uso correcto de las facilidades de procesamiento de información.

Los diferentes mecanismos disponibles para elevar la conciencia de la seguridad incluyen, pero no se limitan a los siguientes:

a) Las políticas y procedimientos escritos de seguridad y sus actualizaciones.

b) Declaraciones firmadas por los empleados comprometiéndose a acatar la política y los procedimientos de seguridad documentados.

c) declaraciones de no revelación de información firmadas por el empleado.

d) Uso de diferentes medios para promulgar la seguridad (por ejemplo, boletín de noticias de la compañía, página Web, vídeos, ect.)

e) Incidentes simulados de seguridad para mejorar los procedimientos de seguridad.

f) Recompensar a los empleados que reporten casos sospechosos.

g) Auditorias periódicas.

Arto. 27. Seguridad lógica.- La instituciones deberán de finar una política de limitación y control de acceso a programas, base de datos, servicios de redes y sistemas operativos. Entre otros aspectos, debe contemplarse lo siguiente:

a) Controles de identificación y autentificación de usuarios.

b) Procedimientos formales para la concesión, administración y revocación de derechos, perfiles y usuarios.

c) Monitoreo del uso de los recursos y registros de eventos.

d) Políticas de prohibición de uso de Usuarios Genéricos y control de no repudio de responsabilidades.

e) Controles especiales sobre el uso adecuado de cuentas de usuario con altos privilegios en los sistemas de información y tecnologías relacionadas.

f) Controles para garantizar la permanente efectividad de medios de autenticación y contraseñas.

g) Protección de puertos y servicios de red.

h) Controles sobre el uso de programas utilitarios que pudieran obviar controles establecidos en los sistemas de información.

i) Desconexión bloqueo de estaciones de trabajo por tiempo de inactividad.

Arto. 28. Seguridad de personal.- Las instituciones deberán definir procedimientos para reducir los riesgos asociados al error humano, robo, fraude o mal uso de activo, vinculados al riesgo de TI. Al establecer restos procedimientos, deberá tomarse en consideración, entre otros aspectos:

a) Definir adecuados roles y responsabilidades sobre la información y su procesamiento.

b) Definir procedimientos adecuados de contratación de personal, especialmente para el manejo de procesos críticos de TI.

c) Establecer la firma de acuerdo de confidencialidad por los empleados y personal externo al que se brinde acceso a las instalaciones de procesamiento o sistemas de información.

d) Definición de otros términos y condiciones de empleo.

e) Establecer políticas de rotación de funciones y vacaciones.

f) Control cruzado y compartido de operaciones sensitivas.

g) Capacitación constante al personal en materia de seguridad.

Arto. 29. Seguridad física y ambiental.- Las instalaciones de procesamiento de información critica o sensible de la empresa, deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones. La protección provista debe ser proporcional a los riesgos identificados; entre los objetivos de control a considerar se encuentran:

a) La identificación y control deceso sobre áreas restringidas.

b) Implementar políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a documentos, medios de almacenamiento e instalaciones de procesamiento de información.

c) Los visitantes de áreas de acceso restringido deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Solo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

d) Los equipos de cómputo deben ser ubicados o protegidos de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.

e) Los equipos de cómputo deben estar protegidos con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos.

Arto. 30. Usuarios remotos y computación móvil.- El uso de equipos de cómputos para procesar información fuera del ámbito de la organización, debe ser autorizado por el nivel gerencial, sin importa quien es el propietario del mismo.

El nivel de seguridad para estos equipos debe ser equivalente a la suministrada dentro del ámbito de la organización, teniendo en cuentas los riesgos asociados a la forma de trabajo. Esta disposición incluye todo tipo de computadoras personales, organizadores, teléfonos móviles, u otro tipo de dispositivo que pueda ser transportado y utilizado para este propósito fuera de la institución.

Arto. 31. Protección contra software malicioso.- Se deben implementar controles de detección y prevención para la protección contra software malicioso como; virus informáticos, caballos de Troya, gusanos de red y otras amenazas semejantes.

Arto. 32 amenazas y seguridad por el uso de Internet.- Las instituciones deben identificar los riesgos a los que se encuentran expuestos por el uso de Internet e implementar controles de seguridad apropiados para el uso de este recurso. Los controles a implementar deben considerar al menos las siguientes amenazas:

Ataques pasivos o de búsqueda de información, por ejemplo:

Análisis de redes.

Fisgoneo (Eavesdropping)

Análisis de Tráfico de red

b) Ataques activos o un ataque para lograr acceso total a los sistemas, o lo suficiente parar llevar a cabe amenazas particulares, por ejemplo:

Ataques de fuerza bruta.

Enmascaramiento

Reenvío de Paquetes (Packet replay)

Modificación de mensajes.

Acceso no autorizado a trasvés de Internet o servicios basados en la Web

Negación de servicio

Ataques de penetración mediante llamada telefónica

Bombardeo y Spamming del Correo Electrónico

Spoofing o suplantación de correo electrónico

Arto. 33. Clasificación de seguridad.- La instituciones deberán realizar un inventario periódico de activos físicos y activos de información, que tenga por objetivo proveer la base para una posterior clasificación de seguridad de acuerdo a una política de clasificación dictada por la junta directiva o la instancia competente. Esta clasificación debe indicar el nivel de criticidad o sensibilidad y seguridad requerida por la institución.

CAPÍTULO VIII
ADMINISTRACIÓN DE PROBLEMAS, PLANEACIÓN DE CONTINGENCIA Y ESTRATEGIAS DE RECUPERACIÓN

Arto. 34. Administración de problemas.- Debido al carácter complejo de la tecnología, deben existir mecanismos para administrar incidentes, problemas, errores o cualquier condición anormal en las operaciones de TI, estos mecanismos deben permitir la identificación, análisis, solución y documentación de errores, según se detalla a continuación:

a) Los errores que deben ser ingresados en el registro incluyen, entre otros:

Errores de programa,
Errores de sistema,

Errores de operación,

Errores de red,

Errores de telecomunicación,

Errores de hardware.

b) La documentación sobre estos eventos que debe conservarse debe considerar al menos, lo siguiente:

Fecha de error,

Descripción de la resolución del error,

Código de error,

Descripción del error,

Fuente del error,

Iniciales de la persona responsable de mantener el registro,

Iniciales de la persona responsable del cierre del ingreso al registro,

Departamento o centro responsable de la resolución de errores,

Código de situación de la resolución del problema (por ejemplo, problema abierto, problema cerrado en espera de una fecha específica futura o el problema no tiene solución en el ambiente actual),

Narrativa de la situación de resolución del error.

c) Para fines de control:

La capacidad de agregar al registro de errores no debe estar restringida.

La capacidad para actualizar el registro de errores debe estar restringida a las personas autorizadas.

La capacidad para cerrar una entrada de registro de errores asignada a una persona diferente de la que es responsable de mantener o de iniciar la entrada la registro de errores.

Arto. 35. Procedimientos de respaldo y restauración.- Las instituciones deben establecer procedimientos de respaldos de información regulares y periódicamente validos para asegura que se reasuma el procesamiento normal de la información en caso de una interrupción de corto plazo y/o si hay necesidad de procesar o de reiniciar un proceso.

Dentro de los controles a considerar en dichos procedimientos están los siguientes:

La documentación y aprobación del procedimiento.

La realización de análisis sobre los requerimientos de respaldo sobre configuraciones, bases de datos,

códigos fuentes, archivos de oficina, ect.

El establecimiento de periodicidad de respaldo de cuerdo al los requerimientos de negocio y sus planes de contingencia.

El resguardo de medios de almacenamiento y sus procedimientos de restauración por tiempos predefinidos de acuerdo a requerimientos internos legales y regulatorios.

La realización de pruebas a los dispositivos de almacenamiento para verificar la existencia de la información respaldada.

El establecimiento de procedimientos de respaldo con frecuencia razonable en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

La implementación y prueba de procedimientos de recuperación y restauración de los respaldos en casos de contingencia.

Arto. 36. Participación de tecnología de la información en la continuidad de negocio.- Como parte de la planeación de continuidad de negocio, las instituciones cuyo procesamiento de datos de sus procesos críticos, esté implementada sobre sistemas de información, deberán considerar la participación de tecnología de la información en sus planes de contingencia y recuperación de desastres.

Estas instituciones deben tener la capacidad de continuar y reestablecer a la normalidad el procesamiento de los sistemas de información, en caso de que las instalaciones primarias de procesamiento de información no estén disponibles por un período significativo de tiempo.

Se debe efectuar un proceso de planeación de contingencia de tecnología de la información, que contemple las siguientes etapas.
a) La conformación de un comité multidisciplinario encargado del proceso: es importante la participación de los responsables de las áreas críticas de negocio.

b) La creación de una política de planeación de contingencia: que identifique los requerimientos para el plan de contingencia, que sea aprobada por junta directiva o la autoridad competente, y que sea publicada al personal.

c) El análisis de riesgo y de impacto de negocio: en el cual se identifiquen los recursos críticos de TI, se identifiquen el impacto de caídas de los sistemas y los tiempos de caída permisibles y se definan el desarrollo de prioridades de recuperación.

d) Identificar controles preventivos: se deben implementar y dar mantenimiento a los controles preventivos.

e) Desarrollar estrategias de recuperación: se deben identificar las estrategias de recuperación e integrarlas a la arquitectura de sistemas.

f) Desarrollar un plan de contingencia de TI: donde se encuentre documentada la estrategia de recuperación del procesamiento de los sistemas de información

g) Desarrollar un plan de pruebas, programa de entrenamiento, divulgación y concientización de los planes: se deben definir objetivos de prueba, criterios de éxito de las pruebas, documentar las lecciones aprendidas e incorporarlas a los planes y capacitar al personal para lograr la ejecución exitosa

de los mismos. La documentación de las pruebas y sus resultados deben ser debidamente documentados y esta disponibles cuando se requieran. Deben realizarse pruebas con una frecuencia no mayor a un (1) año.

h) Implementar mantenimientos al plan: se debe revisar y actualizar el plan, debe existir coordinación con áreas internas y organizaciones externas que sea necesario, se deben establecer controles sobre la distribución del plan y se deben incorporar controles de cambios.

Las estrategias de recuperación deben permitir la restitución de los sistemas, aplicativos críticos y actividades de procesamiento de información, en el sitio principal de procesamiento o en un sitio alterno bajo condiciones de operación adecuadas.

Los planes desarrollados por la institución deben considerar el mejor balance para la institución entre el costo de la contingencia y el costo de recuperación de los servicios.

Arto. 37. Uso de seguros.- Las instituciones deben contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones que permita mitigar al menos riesgos provocados por incendio, accidentes, fenómenos naturales, huelga, motines y robo.

CAPÍTULO IX
ADMINISTRACIÓN INTEGRAL DEL RIESGO TECNOLÓGICO

Arto. 38. Evaluación del Riesgo Tecnológico.- Las instituciones deben implementar procedimientos internos que permitan autoevaluarse de acuerdo con esta norma, los resultados de dicha evaluación y la evaluación del nivel de exposición de riesgo tecnológico debe presentarse al menos una vez al año a la junta directiva de la institución.

Arto. 39. Metodología de administración integral de riesgo tecnológico.- Sin perjuicio de lo establecido en la normativa que regula la materia sobre administración integral de riesgos, con relación al riesgo operativo y riesgo tecnológico, las instituciones a quienes corresponda el cumplimiento de dicha normativa, deberán aprobar formalmente y documentar una metodología de administración de riesgo tecnológico que considere los análisis de riesgo de forma cuantitativa y cualitativa.

Arto. 40 Análisis cuantitativo de riesgo.- El análisis cuantitativo debe considerar la realización de las siguientes actividades:

a) La conformación de una base de datos histórica de eventos de pérdida o frotación de ganancia producto la materialización de riesgos tecnólogos.

b) La determinación de la frecuencia de ocurrencia de dichos eventos.

c) La determinación de su impacto o severidad.

d) La estimación y aprovisionamiento del valor en riesgo en base a información histórica razonable.

Arto. 41. Análisis cualitativo de riesgo.- La metodología de análisis cualitativo del riesgo tecnológico debe considerar lo siguiente:

a) La categorización de los riesgos.

b) La determinación de los riesgos inherentes a cada proceso que involucre el uso de tecnología de la información, describiendo su composición en amenazas y/o vulnerabilidades, su probabilidad de

ocurrencia e impacto.

c) La identificación de controles que mitiguen los riesgos identificados, su clasificación (Por ejemplo: detectivos, disuasivos, preventivos, y/o correctivos), su nivel de efectividad y cumplimiento.
d) La determinación del riesgo residual resultante de la aplicación de los controles a los riesgos inherentes.

e) La determinación de niveles aceptables de riesgo.

f) La identificación y seguimiento a planes de mejora cuando se requiera.

g) La realización de matrices y/o mapas de riesgo o severidad.

Arto. 42. Información al Superintendente.- La institución deberá informar formalmente al Superintendente durante las primeras cuarenta y ocho (48) horas de ocurridos, al menos los siguientes eventos:

a) Incidentes de seguridad: intentos de ataques y penetraciones significativas que hayan siso detectados, así como todos los incidentes de penetración a los sistemas; inoperatividad del sistema central o de producción, etc. Dicha información debe describir las acciones tomadas en el caso;

b) La activación de planes de contingencia de TI y/o estrategias de recuperación así como la estrategia a seguir.

c) La discontinuidad de servicios significativos para sus clientes, como consecuencia de una caída no planificado de los sistemas computarizados, que dure más de un día de labores.

d) La toma de decisión formal de realizar cambios en la plataforma central de operaciones y sistemas computarizados;

e) La toma de decisión formal de implementar o cambiar la plataforma tecnológica utilizada para proporciona servicios financieros por medios electrónicos; y

f) Otros eventos que en su carácter de institución regulada se considere necesario notificar.

CAPÍTULO X
OTRAS DISPOSICIONES

Arto. 43. Transitorio.- Las instituciones deberán cumplir con las disposiciones contenidas en los siguientes Capítulos de la presente norma, a más tardar, en los plazos establecidos a continuación:

Arto. 44. Derogación.- Deróguese la Norma sobre Gestión de Riesgos Tecnológico contenida en Resolución CD-SIBOIF-437-1-AGOS 14-2006 del 14 de agosto de 2006, publicada en La Gaceta, Diario Oficial No. 183 del 21 de septiembre de 2006; y la Norma sobre Ampliación del Plazo para la Aplicación de las Disposiciones Contenidas en la Norma sobre Administración Integral de Riesgos, contenida en Resolución CD-SIBOIF-483-1-JUN132007 del 13 de junio de 2007, publicada en La Gaceta, Diario Oficial No. 151 del 09 de agosto de 2007.

Arto 45. Vigencia.- La presente norma entrará en vigencia a partir de su notificación, sin perjuicio de su posterior publicación en La Gaceta, Diario Oficial. (f) Antenor Rosales B. (f) V. Urcuyo V. (f) Gabriel Pasos Lacayo (f) Roberto Solórzano Ch. (f) A. Cuadra G. (f) U. Cerna B.

URIEL CERNA BARQUERO, Secretario Consejo Directivo SIBOIF.