SGV-A-124. ACUERDO SOBRE REQUERIMIENTOS MÍNIMOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI) [1] [2]

(Incluye las reforma de los acuerdos SGV-A-163 y SGV-A-165)

CONSIDERANDO

I) Una inadecuada administración del riesgo operativo en el área de tecnología de información de los sujetos fiscalizados por la Superintendencia General de Valores (SUGEVAL), puede repercutir negativamente en el patrimonio de los inversionistas, en la propia entidad fiscalizada y en el desarrollo del mercado de valores costarricense.

II) La gestión del riesgo operativo es responsabilidad de cada una de las entidades fiscalizadas. No obstante, le compete a la SUGEVAL garantizar la protección de los legítimos intereses y derechos de los inversionistas y del mercado de valores en general. En razón de lo anterior, resulta indispensable la determinación de ciertos requerimientos mínimos de tecnología de información que deban ser atendidos de manera uniforme para la gestión del riesgo en el área de tecnología de la información (TI).

III) El desarrollo de servicios financieros de consulta o transaccionales a través de Internet forma parte de las estrategias institucionales tendientes a facilitar a los inversionistas sus operaciones.

IV) Según el artículo 3, inciso e), del Reglamento General sobre Sociedades Administradoras de de Fondos de Inversión, para el otorgamiento de la autorización correspondiente es indispensable que las Sociedades Administradoras cuenten con "*Documentación de la estructura organizativa y el recurso humano y tecnológico que le permita a la sociedad brindar sus servicios de manera adecuada, de conformidad con los lineamientos establecidos por el Superintendente*".

V) De conformidad con el artículo 58, inciso a), de la Ley Reguladora del

[1] Superintendencia General de Valores. Despacho del Superintendente. A las nueve horas del veintidós de agosto del dos mil seis

[2] Nombre modificado por el Acuerdo del Superintendente SGV-A-163 del 23 de noviembre del 2009.

Mercado de Valores, los puestos de bolsa están obligados a "*Cumplir las disposiciones de esta ley y sus reglamentos y acatar los acuerdos de la Superintendencia*".

VI) Es indispensable que los Puestos de Bolsa cumplan con ciertos estándares mínimos de tecnología de la información (TI) que garanticen la integridad, seguridad, auditabilidad y disponibilidad de la información y de los servicios ofrecidos.

VII) De conformidad con lo dispuesto en el artículo 8 inciso j) de la Ley Reguladora del Mercado de Valores, le corresponde al Superintendente adoptar todas las acciones necesarias para el cumplimiento efectivo de las funciones de regulación, supervisión y fiscalización atribuidas legalmente a la Superintendencia.

VIII) El presente Acuerdo fue sometido a consulta de conformidad con el Artículo 361 de la Ley General de Administración Pública.

Por tanto acuerda:

SGV-A-124. *ACUERDO SOBRE REQUERIMIENTOS MÍNIMOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI)*

Artículo 1. Objetivo

[3]

Las Sociedades Administradoras de Fondos de Inversión, los Puestos de Bolsa y los Proveedores de Precios, en adelante las entidades, deben contar con sistemas de Tecnología de Información (TI) que garanticen la integridad, seguridad, auditabilidad y disponibilidad de la información y de los servicios ofrecidos, independientemente del medio de comunicación electrónico que se utilice, ya sea público o privado. El diseño y funcionamiento de los sistemas de TI son responsabilidad de las entidades y deben estructurarse de forma tal que cumplan, al menos, con los requerimientos que se detallan en este Acuerdo.

SECCIÓN I
ADMINISTRACIÓN DEL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN (TI)

Artículo 2. Planificación en Tecnología de Información (TI)

[3] Párrafo modificado por el Acuerdo del Superintendente SGV-A-163 del 23 de noviembre del 2009.

Las entidades deben realizar un proceso de planificación en TI de acuerdo con la planeación estratégica institucional, de manera que se definan y facilite la consecución de sus metas en el futuro. Para ello, deben contar con un plan en TI formalmente documentado y aprobado por la Gerencia General y ratificado por la Junta Directiva o Consejo de Administración.

Artículo 3. Personal en Tecnología de Información (TI)

Las entidades deben contar con manuales de puestos actualizados, en los cuales se describan las funciones y responsabilidades de sus funcionarios según los alcances del presente acuerdo. Asimismo, las entidades deben contar con el personal necesario y técnicamente capacitado para desempeñar adecuadamente sus funciones en el área de TI.

Artículo 4. Subcontratación de servicios en Tecnología de Información (TI)

Las entidades pueden subcontratar los servicios de TI. En tal caso, deben contar en todo momento con un contrato vigente de prestación de servicios, el cual debe especificar los deberes y responsabilidades del proveedor o proveedores. Según los tipos de servicios que se incluyan, el contrato debe estipular, como mínimo, aspectos relacionados con:

a) Propiedad intelectual de los programas fuente de los sistemas de información.
b) Actividades preventivas y correctivas.
c) Tiempo de respuesta.
d) Seguridad.
e) Monitoreo.
f) Respaldos de información.
g) Requerimientos en caso de contingencias.
h) Confidencialidad de la información.
i) Procedimientos de control interno y documentación a la que debe sujetarse el contratado.
j) Cláusulas por incumplimiento.
k) Sujeción a las funciones de supervisión y fiscalización de la SUGEVAL.

La subcontratación de servicios de TI por parte de las entidades no las exime de responsabilidad ante la SUGEVAL, la cual conservará sus atribuciones de supervisión y fiscalización sobre los servicios, independientemente de que éstos le

sean suministrados por terceros. En todo momento será responsabilidad de la entidad fiscalizada suministrar la información o permitir el acceso de la Superintendencia para sus labores de supervisión.

SECCIÓN II
SEGURIDAD FÍSICA Y LÓGICA

Artículo 5. Políticas y procedimientos de seguridad lógica

Las entidades deben administrar adecuadamente los recursos de TI, así como mantener una adecuada seguridad en los puntos de acceso a las redes públicas de datos. Para esto, las entidades deben contar, al menos, con políticas y procedimientos sobre:

a) Acceso a los sistemas de información, sistemas operativos y bases de datos.
b) Auditoría de las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos.
c) Controles de tráfico hacia adentro y fuera de la red institucional (*firewall* o pared de fuego).
d) Uso del correo electrónico, cuando se utilice como medio de comunicación oficial.
e) Prevención de contaminaciones de virus a la red de datos.

Con formato: Numeración y viñetas

Artículo 6. Políticas y procedimientos en seguridad física

Las entidades deben establecer políticas y procedimientos relacionados con la ubicación, construcción, acceso físico a los centros de cómputo y comunicaciones, así como procedimientos de control que proporcionen un ambiente físico conveniente para su funcionamiento y que protejan los recursos materiales y al personal de TI contra peligros naturales o fallas humanas.

SECCIÓN III
SISTEMAS DE INFORMACIÓN

Artículo 7. Requerimientos del sistema de información

Las entidades deben velar por la adecuada disponibilidad, capacidad y desempeño de los sistemas de información. El diseño e implementación de estos sistemas debe procurar que estos sean eficaces, seguros y que impidan la

modificación no autorizada. Para esto, las entidades deben establecer políticas y procedimientos para:

a) El mantenimiento de las aplicaciones.
b) La separación de los ambientes de desarrollo y producción.
c) La actualización y disponibilidad de los manuales de usuario y técnico de los sistemas.
d) El mantenimiento de bitácoras de control activas donde se registren rastros de auditoría.

Los sistemas de información deben permitir, por medio de bitácoras o información histórica, reconstruir toda información relacionada con las transacciones de los clientes y aquellos procesos sensitivos definidos por la entidad, desde su inicio hasta su finalización, incluyendo las modificaciones de las que pudo ser objeto. Se deben poder observar los diferentes estados de los movimientos, así como el registro de los usuarios y la fecha y hora en que intervinieron en cada uno de los estados.

Artículo 8. Políticas y procedimientos para la entrada, procesamiento y salida de datos

Las entidades deben contar con políticas y procedimientos relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, de manera que asegure que estos permanezcan íntegros, completos, precisos y válidos.

SECCIÓN IV
SOFTWARE Y BASES DE DATOS

Artículo 9. Administración de software

Las entidades deben definir políticas y procedimientos para la adecuada autorización, instalación, mantenimiento y administración del *software*.

Artículo 10. Administración de base de datos

Las entidades deben contar con políticas y procedimientos que consideren el diseño, integridad, disponibilidad, capacidad y desempeño de sus bases de

datos. Las políticas y procedimientos deben contener los procesos de instalación, administración, migración, mantenimiento y seguridad de las bases de datos.
En las bases de datos debe mantenerse, al menos, la información del año precedente. No obstante lo anterior, la información histórica debe almacenarse de conformidad con lo establecido en la legislación, reglamentación o normativa vigente.

SECCIÓN V
HARDWARE, REDES Y COMUNICACIONES

Artículo 11. Administración de *hardware*, redes y comunicaciones

Para administrar el *hardware*, las redes y las líneas de comunicación, las entidades deben, como mínimo, establecer políticas y procedimientos para la instalación, administración, mantenimiento, seguridad y monitoreo del *hardware,* y las líneas de comunicación. Estas políticas y procedimientos deben asegurar la disponibilidad, capacidad y desempeño de la plataforma de TI, de manera que soporte las aplicaciones de las entidades y reduzca la frecuencia e impacto de las fallas de desempeño y vulnerabilidades. En el caso de redes instaladas, ya sean eléctricas, de voz o de datos, éstas deben cumplir con los requerimientos mínimos vigentes de cableado estructurado.

Adicionalmente, las entidades deben establecer un estándar de carácter técnico para la configuración de su equipo central de procesamiento. Éste debe cumplir con los requerimientos de redundancia y tolerancia a fallas que garanticen la disponibilidad del servicio.

SECCIÓN VI
CONTINUIDAD DE LAS OPERACIONES

Artículo 12. Políticas y procedimientos para el respaldo y recuperación de información

Las entidades deben establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información que, como mínimo, consideren la periodicidad, custodia, bitácoras y verificación de los datos respaldados. Estas políticas y procedimientos deben permitir asegurar que las funciones y servicios de las entidades puedan seguir funcionando durante períodos de emergencia causados por desperfectos en los equipos, pérdida de información u otras situaciones similares.

Artículo 13. Plan de continuidad

Las entidades deben establecer y documentar un plan de continuidad del cual existan copias fuera de las instalaciones principales. En éste se deben detallar los riesgos posibles que afecten de forma parcial o total la operativa normal de los servicios de TI y las acciones, procedimientos y recursos con que estos riesgos serán gestionados. Este plan debe ser aprobado por la Gerencia General y ratificado por la Junta Directiva o Consejo de Administración; y debe ser actualizado, probado y documentado al menos una vez al año.

Las entidades pueden incorporar, como parte de estas políticas, aspectos relacionados con la infraestructura de suministro de energía.

Artículo 14. Sitio alterno

Las entidades deben definir alternativas de procesamiento alterno o un sitio alterno de procesamiento, con el fin de proveer las necesidades de recuperación inmediatas y garantizar la operativa normal del negocio, ante algún eventual desastre.

SECCIÓN VII
SERVICIOS FINANCIEROS Y DE INFORMACIÓN A TRAVÉS DE SITIOS WEB

Artículo 15. Servicios financieros por Internet

Las entidades que ofrezcan a sus clientes servicios financieros transaccionales a través de Internet, deben contar con documentación, políticas y procedimientos que consideren al menos:

a) Responsabilidades legales y condiciones operativas bajo las cuales se brinda el servicio financiero por Internet a los clientes.

b) Acceso a los servicios financieros por Internet, a fin de proteger la integridad y privacidad de la información.

c) La actualización de la información disponible en la página web. En el caso de información sobre rendimientos, estados financieros auditados y otra información utilizada por los inversionistas para la toma de decisiones, ésta

deberá ser actualizada en un plazo máximo de 5 días naturales desde el momento de su generación.

d) Estándares de seguridad (autenticación, controles de acceso, confidencialidad, integridad y no repudio).

Los servicios que se ofrecen por Internet deben contar con un certificado de sitio Web seguro otorgado por una entidad certificadora calificada. Dicha certificación debe actualizarse por lo menos cada dos años.

Artículo 16. Advertencias y leyendas

La página Web debe contar con advertencias y leyendas para que el inversionista conozca con claridad acerca del producto en el cual invierte o desea invertir, según la legislación, reglamentación o normativa aplicable.

SECCIÓN VIII
DISPOSICIONES FINALES

Artículo 17. Requisitos para la autorización

Para el cumplimiento del requisito indicado en el inciso e) del artículo 8 del Reglamento sobre Valoración de Instrumentos Financieros, se debe presentar una declaración jurada que considere al menos el contenido definido en el Anexo I de este Acuerdo".

Artículo 18. Derogatorias y modificaciones

Se derogan las siguientes disposiciones:

a. Artículos 3, 4 y 5 del Acuerdo SGV-A-42 Instrucciones sobre los recursos humanos, tecnológicos e informáticos y operacionales que deberán cumplir las Sociedades Administradoras de fondos de Inversión y en los Fondos de Inversión, Ref. 3360 del 13 de noviembre del 2000.

b. Artículos 3, 4 y 5 del Acuerdo SGV-A-103 Instrucciones para la Publicación de Información Referente a Fondos de Inversión a Través de Sitios Web, Ref. 1544 del 8 de abril del 2005.

Se modifica el título del Acuerdo SGV-A-42 Instrucciones sobre los recursos humanos, tecnológicos e informáticos y operacionales que deberán cumplir las Sociedades Administradoras de Fondos de Inversión y en los Fondos de Inversión, Ref. 3360 del 13 de noviembre del 2000, para que en adelante se lea: "Instrucciones sobre los recursos humanos y operacionales que deberán cumplir las Sociedades Administradoras de Fondos de Inversión y en los Fondos de Inversión".

Artículo 19. Vigencia

Rige a partir del 1ero de setiembre del 2006.

Transitorio I

Las Sociedades de Fondos de Inversión y los Puestos de Bolsa cuentan con 6 meses para cumplir lo dispuesto en este acuerdo, con excepción de lo indicado en el Transitorio II.

Transitorio II

El plan de continuidad señalado en el artículo 13 debe estar elaborado a más tardar seis meses después de la entrada en vigencia de este Acuerdo.

El sitio alterno señalado en el artículo 14 debe estar definido y habilitado a más tardar dieciocho meses después de la entrada en vigencia de este Acuerdo.

ANEXO I [4]

CONTENIDO MÍNIMO DE LA DECLARACIÓN JURADA DEL PROVEEDOR DE PRECIOS

El contenido mínimo de la declaración jurada del proveedor de precios que debe presentar con los requisitos de autorización según lo indicado en el artículo 8 del Reglamento sobre valoración de instrumentos financieros, es el siguiente:

NUMERO.....: Ante mí, ..., Notario Público de ....., comparece (n) el (los) señor (es) ..... (nombre, apellido y demás calidades del declarante)....., en su calidad de representante legal con facultades de apoderado generalísimo, de la empresa denominada ....., cédula jurídica número .....; quién apercibido por el suscrito notario de las penas con las que el Código Penal castiga en su artículo 311 el perjurio (esto último de acuerdo con la redacción particular del notario), declara bajo la fe de juramento solemne: "Que el proveedor de precios cumple con los requerimientos de tecnología de información (TI) que le permiten brindar los servicios de manera adecuada, de conformidad con las disposiciones emitidas por la Superintendencia General de Valores. Que asumo en la calidad indicada toda responsabilidad y las respectivas consecuencias civiles y penales sobre la veracidad de la información señalada. Es todo." El suscrito notario advirtió al (a los) compareciente (s) sobre el valor y trascendencia legal de sus declaraciones. Se expide un primer testimonio para efectos de trámites administrativos ante la Superintendencia General de Valores. El suscrito Notario, con vista del asiento....., visible al folio....., del tomo....., que al efecto lleva la Sección Mercantil del Registro Nacional, da fe de la existencia de la empresa.....y de la vigencia de la representación y poderes ostentados por el (los) declarante (s). Es todo. Leído lo anterior al (a los) compareciente (s), lo aprueba y firmamos a las ..... horas del ... (día) ..... de ..(mes). de ...(año en letras)..... Firmas.

[4] Anexo adicionado por el acuerdo del Superintendente SGV-A-165 del 8 de enero del 2010