

REPÚBLICA DE PANAMÁ
SUPERINTENDENCIA DEL MERCADO DE VALORES

Acuerdo 5-2018
(De 21 de agosto de 2018)

“Que establece los Lineamientos Generales para la Gestión del
Riesgo de Tecnología de la Información”.

(Modificado por el Acuerdo No. 1-2026 de 28 de mayo de 2026)

TEXTO ÚNICO

LA JUNTA DIRECTIVA
En uso de sus facultades legales y

CONSIDERANDO

Que a través de la Ley 67 de 1 de septiembre de 2011, se crea la Superintendencia del Mercado de Valores (en adelante la “Superintendencia”) como organismo autónomo del Estado, con personería jurídica, patrimonio propio e independencia administrativa, presupuestaria y financiera, con competencia privativa para regular y supervisar a los emisores, sociedades de inversión, intermediarios y demás participantes del mercado de valores en la República de Panamá.

Que en virtud de lo establecido en el artículo 121 de la Ley 67 de 2011, la Asamblea Nacional expidió el Texto Único que comprende el Decreto Ley 1 de 1999 y sus leyes reformativas y el Título II de la Ley 67 de 2011, reformado por la Ley 12 de 3 de abril de 2012 y la Ley 56 de 2 de octubre de 2012 (en adelante la “Ley del Mercado de Valores”).

Que de conformidad con lo establecido en el artículo 3 de la Ley del Mercado de Valores, la Superintendencia tendrá como objetivo general la regulación, la supervisión y la fiscalización de las actividades del mercado de valores que se desarrollen en la República de Panamá o desde ella, propiciando la seguridad jurídica de todos los participantes del mercado y garantizando la transparencia, con especial protección de los derechos de los inversionistas.

Que el artículo 10, de la Ley del Mercado de Valores faculta a la Junta directiva para adoptar, reformar y revocar acuerdos que desarrollen las disposiciones de la Ley del Mercado de Valores.

Que en sesiones de trabajo de la Superintendencia del Mercado de Valores se ha puesto de manifiesto la necesidad de promover que las entidades con Licencia expedida por la Superintendencia cuenten con un sistema para la Gestión de Riesgos Tecnológicos que les permitan identificar, medir, limitar, controlar y reportar los riesgos que enfrentan, con el fin de administrar el posible impacto negativo de dichos riesgos.

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 mercado de valores.

Que el presente Acuerdo ha sido sometido al procedimiento de Consulta Pública contenido en el Título XIV de la Ley del Mercado de Valores, específicamente en los artículos 323 y siguientes, cuyo plazo fue del 21 de junio de 2018 al 26 de julio de 2018, según consta en el expediente de acceso público que reposa en las oficinas de la Superintendencia.

Que en virtud de lo anterior, la Junta Directiva de la Superintendencia del Mercado de Valores, en uso de sus facultades legales;

ACUERDA

ARTÍCULO PRIMERO: ADOPTAR los lineamientos generales para la Gestión Adecuada del Riesgo Tecnológico para las entidades con Licencia de Casas de Valores,

Asesor de Inversión, Administradoras de Inversiones, Proveedores de Servicios Administrativos del Mercado de Valores, Entidades Administradoras de Inversión de Fondos de Pensiones y Jubilaciones, Administradoras de Inversiones de Fondos de Cesantía, y las Organizaciones Autorreguladas, en adelante entidades con Licencia.

Capítulo I. Aspectos Generales.

Artículo 1. Ámbito de Aplicación.

Las disposiciones del presente acuerdo serán aplicables a las entidades con Licencia expedidas por la Superintendencia del Mercado de Valores, con el objetivo de establecer los criterios mínimos para la Evaluación y Administración del Riesgo Tecnológico, Seguridad y Transmisión de la Información, así como el uso y aplicación de los controles de las herramientas tecnológicas, previendo la estabilidad y eficiencia de las actividades desarrolladas en el mercado de valores en y desde la República de Panamá.

¹Artículo 2. Definiciones.

Para los propósitos del presente Acuerdo, los siguientes términos se entenderán de la siguiente manera:

- a) **Contingencia:** Situación potencial derivada de la posible materialización de un evento de riesgo relacionado con los sistemas, infraestructura, servicios o información tecnológica, cuya ocurrencia, aunque incierta, puede afectar la continuidad, disponibilidad, integridad o confidencialidad de las operaciones de la entidad, y que requiere la definición de medidas de respuesta, recuperación y mitigación dentro del marco de la Gestión Integral de Riesgos. La contingencia no elimina el riesgo, pero permite reaccionar de forma rápida y eficazmente para reducir su impacto.
- b) **Gobierno de la Tecnología de la Información:** Conjunto de procesos, responsabilidades, políticas, procedimientos, relaciones y controles que apoyan las metas del negocio, optimizan las inversiones y administran los riesgos y oportunidades asociados a la tecnología de la información, facilitando el logro de los objetivos y planes establecidos por las entidades con Licencia.
- c) **Incidente:** Cualquier evento tecnológico o no, externo o interno, que no forma parte de la operación normal de un servicio y que causa o pueda causar, una interrupción o una reducción de la calidad del mismo.
- d) **Información:** Cualquier forma de registro electrónico, digital, óptico, magnético o en otros medios similares, susceptible de ser reproducida, procesada, distribuida o almacenada e impresa.
- e) **Plan de continuidad de negocios:** Conjunto documentado de políticas, procedimientos, controles y recursos establecidos por la entidad con licencia para asegurar la continuidad, recuperación y oportuna reanudación de sus funciones, procesos y servicios críticos ante la ocurrencia de interrupciones que puedan afectar sus operaciones normales, con el fin de limitar las pérdidas, proteger los activos e información, preservar la confianza del mercado y garantizar el cumplimiento de sus obligaciones regulatorias y contractuales.
Este plan debe definir de manera precisa cómo la entidad va a reaccionar y a operar durante y después de un incidente que afecte sus operaciones.
- f) **Plan de recuperación de desastres:** Es un plan creado por una entidad que contiene instrucciones detalladas acerca de cómo responder a incidentes no planificados como desastres naturales, cortes de electricidad, ataques cibernéticos y cualquier otro evento disruptivo. El plan incluye estrategias o procedimientos para minimizar los efectos de un desastre y permitir que una entidad continúe operando o reanude

¹ Modificado por el ARTÍCULO SEGUNDO del Acuerdo No. 1-2016 de 28 de mayo de 2026.

rápidamente las operaciones importantes. El plan de recuperación de desastres busca restablecer los sistemas y servicios de la tecnología de la información lo antes posible después de un evento crítico, reduciendo al mínimo el impacto en la organización.

- g) **Procedimiento:** Método o sistema estructurado donde es detallada la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.
- h) **Riesgo de tecnología de la información:** Toda posible ocurrencia de daños, interrupción, alteración o fallas derivadas del uso de la Tecnología de la Información que soporta los procesos críticos de la entidad y que conlleve a una pérdida económica, material o de negocio.
- i) **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas, que buscan la confidencialidad, integridad y disponibilidad de la información en sí y de los demás recursos informáticos de la entidad.
- j) **Tecnología de la Información o TI:** Conjunto de instrumentos tecnológicos que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro, acceso y presentación de información.

Capítulo II.

Sobre la Gobernanza de la Tecnología de la Información.

Artículo 3. De la Tecnología de la Información (TI).

Las entidades con licencia podrán contar con una persona encargada o tercerizar los servicios para la adecuada administración de la Tecnología de la Información y sus riesgos asociados.

Aquellas entidades con Licencia que pertenezcan a un grupo financiero o económico y mantienen un área especializada de tecnología de la información encargada de la administración, dicho requerimiento será cubierto a través de esta figura, sin la necesidad de modificar su estructura organizacional vigente.

Artículo 4. Criterios de Control de Tecnología de la Información (TI)

Las políticas, planes estratégicos y procedimientos adoptados por la Junta Directiva de la entidad para la adecuada Gestión de la Tecnología de la Información (TI), serán revisados y evaluados como mínimo cada tres (3) años, enfocándose en los siguientes criterios de control y gestión, sin limitar:

- a) **Confiabilidad:** Los sistemas tecnológicos y demás herramientas tecnológicas empleadas deben brindar información cierta, correcta, fiable, veraz, completa, oportuna y exacta, la cual será utilizada en las actividades, operaciones y en la toma de decisiones de la entidad, preparación de los informes financieros, incluyendo los estados financieros, así como aquella información gerencial y su remisión a la Superintendencia.
- b) **Confidencialidad:** Los sistemas y herramientas tecnológicas empleadas deben brindar el debido resguardo al acceso a la información sensible o clasificada bajo reserva, previendo cualquier tipo de riesgo de divulgación y uso no autorizado.
- c) **Cumplimiento:** Los sistemas y herramientas tecnológicas empleadas para el buen desempeño del negocio deben cumplir, como mínimo, con las leyes y reglamentos emitidos por la Superintendencia, sus criterios de evaluación, así como las políticas internas adoptadas por la misma entidad.
- d) **Disponibilidad:** Los recursos tecnológicos, y la información obtenida de parte de los sistemas tecnológicos, deben estar disponibles en tiempo y forma, una vez que sean requeridos por los usuarios autorizados, debiendo contar con la característica de poder ser auditables.

- e) **Efectividad:** La información y los procesos deben ser relevantes y pertinentes para el proceso y buena marcha del negocio, además de presentarse en forma correcta, coherente, completa y que pueda utilizarse oportunamente.
- f) **Eficiencia:** El proceso de la información debe realizarse mediante una óptima utilización de los recursos.
- g) **Integridad:** La información debe de ser precisa, validable, y tener suficiencia, de acuerdo a las expectativas del negocio y sus actividades autorizadas.
- h) **Seguridad:** los sistemas y las herramientas tecnológicas empleadas por la entidad debe cumplir con el criterio de confidencialidad, integridad y disponibilidad de la información, independientemente del formato en que se tengan o el soporte de la misma, garantizando que la información no pueda ser alterada ante incidentes o intentos maliciosos desde su creación sin la autorización correspondiente.

Artículo 5. Responsabilidades de las Entidades con Licencia.

La Junta Directiva de las entidades, deberá adoptar las políticas, planes estratégicos y procedimientos, así como la asignación de recursos necesarios para la adecuada gestión de la Tecnología de la Información, debiendo como mínimo:

- a. Aprobar los objetivos, lineamientos y políticas generales para administrar, de manera adecuada y prudente, la seguridad y los riesgos de tecnología de la información.
- b. Aprobar el o los manuales necesarios para la buena gestión de los riesgos de tecnología de la información.
- c. Aprobar los planes estratégicos y de contingencia relacionados con la tecnología de la información.
- d. Aprobar las prioridades de inversión de la tecnología de la información, de conformidad con los objetivos del negocio.
- e. Incorporar y fortalecer el contenido de las políticas adoptadas, considerando las directrices emitidas por esta Superintendencia, y las mejores prácticas internacionales.

Artículo 6. Requisitos Mínimos de Infraestructura y Seguridad Física.

Como parte de los requisitos mínimos de Infraestructura y Seguridad Física, toda entidad con licencia debe contemplar lo siguiente:

- 1. Contar con los equipos de comunicación necesarios para el adecuado procesamiento de datos, así como con el soporte técnico para el mantenimiento de dichos equipos.
- 2. Los Ejecutivos Claves y demás miembros de la Alta Gerencia de las entidades con licencia deberán contar con los equipos tecnológicos en espacios seguros para el buen desempeño de sus funciones y responsabilidades, con las medidas necesarias para el resguardo de la información sensible de la entidad.
- 3. Los equipos de respaldo tecnológico deberán cumplir con las condiciones físicas, climáticas y ambientales apropiadas para el buen funcionamiento de las comunicaciones y procesamiento de la información.
- 4. Los equipos de información, así como sus respaldos y demás equipos de procesamiento de datos, deberán contar con las condiciones físicas apropiadas contra la ocurrencia de desastres naturales.

Artículo 7. Administración de Hardware y Comunicaciones.

Para la adecuada gestión y administración de hardware, redes y líneas de comunicación, la entidad tendrá las siguientes responsabilidades:

- 1. Contar con la capacidad tecnológica y administrativa para garantizar sus operaciones, acorde a su tamaño, naturaleza y complejidad de las operaciones y productos que ofrece.

2. Realizar el análisis sobre la capacidad y desempeño del hardware y las líneas de comunicación, que permitan determinar en forma oportuna, necesidades de ampliación de capacidades o actualizaciones de equipos.
3. Establecer y mantener políticas, procedimientos de monitoreo y reporte del uso eficiente y efectivo de equipos.
4. Establecer mecanismos para procurar que todas las redes instaladas, ya sean eléctricas, de voz o de datos, cumplan con los requerimientos mínimos vigentes de cableado estructurado.
5. Asegurar la existencia de la documentación, el etiquetado de los equipos y cableado.
6. Establecer y mantener planes de mantenimiento preventivo de acuerdo a lo recomendado por los proveedores.
7. Mantener actualizados los contratos de proveedores, diagramas de red y comunicaciones, diagramas de distribución física, inventarios, configuración técnica y cualquier otra información requerida.
8. Ejecutar los procedimientos de descarte de los equipos, los cuales deben considerar que los medios de almacenamiento, que contengan material sensible, deban ser físicamente destruidos o sobrescritos en forma segura.

Capítulo III.

Gestión de Riesgo de Tecnología de la Información (TI).

Artículo 8. Gestión de la seguridad de la información.

Los sistemas y demás herramientas tecnológicas empleadas deben garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, abusos, divulgación o modificación no autorizados, daño o pérdida, u otros factores disfuncionales de la misma.

El o los manuales, políticas y procedimientos adoptados para la Administración del Riesgo Tecnológico y Aseguramiento de la Información, deberán establecer las siguientes funciones:

1. Documentar, implementar y actualizar una política de seguridad de la información y los procedimientos correspondientes, así como asignar los recursos necesarios para lograr los niveles adecuados de seguridad requeridos.
2. Mantener una vigilancia constante sobre todo el marco de seguridad, definiendo y ejecutando acciones periódicas para su actualización.
3. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.
4. Informar y capacitar al personal sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de la Tecnología de la Información.
5. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con proveedores o terceros en el manejo de la información y/o documentación, así como protocolos para la terminación de contratos.
6. Establecer un marco metodológico que incluya la clasificación de los recursos de Tecnología de la Información, según su criticidad, la identificación y evaluación de riesgos.
7. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
8. Atención y seguimiento a los incidentes de seguridad de la información.
9. Establecer medidas de protección en los sistemas contra posibles amenazas o vulnerabilidades existentes.

10. Establecer procedimientos para la definición de perfiles lógicos de usuarios, roles y niveles de privilegio; para la identificación y autenticación, así como el acceso a la información, tanto para los usuarios como para recursos implementados.
11. Adoptar e Implementar planes de contingencia, planes de continuidad del negocio y planes de recuperación de desastre para mantener el nivel de seguridad durante las actividades de recuperación.

²Artículo 9. Plan de continuidad de negocios y recuperación de desastres.

Las entidades con licencia deberán contar con un plan de continuidad de negocios para la Tecnología de la Información y de recuperación de desastres debidamente aprobado por el Comité de Administración de Riesgos y ratificado por la Junta Directiva, en razón del tamaño, necesidades y estructura organizativa de la entidad con licencia, que tendrá como objetivo principal brindar respuestas efectivas que garanticen la continuidad en las actividades de servicios y del negocio ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en sus operaciones.

Este plan deberá ser probado al menos una vez al año y deberá contemplar como mínimo lo siguiente:

1. Objetivo del Plan.
2. Procesamiento alternativo, incluyendo el debido respaldo de la información y los sistemas, incluyendo sitio alterno, de acuerdo al tamaño, actividades autorizadas o naturaleza del negocio.
3. Identificación de los recursos críticos de la Tecnología de la Información.
4. Identificación del impacto por la interrupción de los servicios críticos.
5. Pruebas de resistencia diseñadas para mitigar el impacto de una interrupción mayor de las funciones y de los procesos claves del negocio (tiempos permisibles de interrupción de los servicios).
6. Respuesta a los inversionistas, clientes, usuarios, proveedores y demás grupos de interés.
7. Identificación, descripción de responsabilidades y funciones del personal clave que ejecutará el plan.
8. Capacidad de la recuperación de los servicios críticos de TI.
9. Programación y ejecución anual de pruebas identificadas en el Plan de Contingencia, así como su actualización conforme a los resultados obtenidos en dichas pruebas.

Los resultados obtenidos de las pruebas ejecutadas deberán ser notificados al Ejecutivo Principal y a la Junta Directiva de la entidad.

Artículo 10. Grupos Financieros o Económicos. Aquellas entidades con Licencia que pertenezcan a un grupo financiero o grupo económico, el plan de continuidad de negocios y recuperación de desastres adoptado a nivel de grupo será suficiente para los fines del pleno cumplimiento de lo establecido en el presente acuerdo.

Artículo 11. Tercerización.

Con la finalidad de garantizar que los recursos y servicios proporcionados por terceros sean administrados con responsabilidades definidas y estén sometidas a un monitoreo de su eficiencia y efectividad por parte de la entidad, los proveedores de servicio o facilidades tecnológicas deberán contar como mínimo con lo siguiente:

1. Certificación sobre la experiencia y competencia técnica comprobada del proveedor para implementar los servicios requeridos.
2. Solidez financiera del proveedor. El proveedor deberá presentar Estados Financieros o cualquier otra información pertinente.
3. Reputación comercial, litigios pendientes del proveedor o quejas.
4. Implementación de controles internos.
5. Planes de contingencia, incluyendo planes de recuperación tecnológica, cuando aplique.

² Modificado por el ARTÍCULO TERCERO del Acuerdo No. 1-206 de 28 de mayo de 2026.

6. Ubicación geográfica del proveedor.
7. Contratos con el proveedor de servicios, debidamente formalizados en donde se establezcan claramente el objeto y alcance de los servicios, los productos o resultados esperados, plazos de entrega, derechos y obligaciones de las partes.
8. Requerimientos contractuales en donde se definan la propiedad de la información y de las aplicaciones y la responsabilidad del proveedor de servicios de la Tecnología de la Información en caso de ser vulnerables sus sistemas.
9. Requerimientos contractuales en donde se definan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y la entrega de una documentación técnica, con la finalidad de minimizar la dependencia con el proveedor de servicios de la Tecnología de la Información y los eventos de riesgo que esto origine.
10. Las entidades con licencia serán responsables de validar y garantizar que los servicios contratados, como el proveedor, se ajusten a los requerimientos establecidos en el presente acuerdo.

Las entidades deberán mantener en sus instalaciones la infraestructura informática que sea utilizada para el procesamiento de la información. Sin embargo, aquellas que requieran descentralizar total o parcialmente los respaldos (resguardos), procesos tecnológicos de información, excluyendo los servicios de desarrollo de software, fuera de sus propias instalaciones o supervisión directa, deberá informar a esta Superintendencia dicha situación con al menos treinta (30) días calendarios de anticipación al inicio de operaciones, a fin de poder llevar a cabo la inspección correspondiente en sitio.

En el caso que las entidades mantengan la infraestructura informática fuera de la República de Panamá, deberá informar a esta Superintendencia y proporcionar de manera escrita, toda la información detallada referente a la infraestructura informática, seguridad lógica y física.

Capítulo IV. Disposiciones Finales.

Artículo 12. Sanciones.

El incumplimiento de lo dispuesto en las disposiciones del presente Acuerdo se sancionará de conformidad con las sanciones consagradas en la Ley del Mercado de Valores.

ARTÍCULO SEGUNDO: (VIGENCIA). El presente Acuerdo entrará a regir a partir del 01 de julio de 2019.

FUNDAMENTO LEGAL: Texto Único de la Ley del Mercado de Valores.

Dado en la ciudad de Panamá, a los veintiún (21) días del mes de agosto de dos mil dieciocho (2018).

PUBLÍQUESE Y CÚMPLASE

EL PRESIDENTE

EL SECRETARIO AD-HOC

JOSÉ RAMÓN GARCÍA DE PAREDES

LAMBERTO MANTOVANI

