

CERTIFICACIÓN

Los infrascritos, **Sr. Ervin Novas Bello, gerente del Banco Central de la República Dominicana** (en lo adelante “Banco Central”), **en representación del gobernador del Banco Central, miembro ex officio y presidente del Consejo Nacional del Mercado de Valores** (en lo adelante “Consejo”); y **Sra. Fabel María Sandoval Ventura, secretaria del Consejo**, **CERTIFICAN** que el texto a continuación constituye copia fiel transcrita de manera íntegra conforme al original de la **Cuarta Resolución, R-CNMV-2023-10-MV**, adoptada por el Consejo en la reunión celebrada en fecha **veintiuno (21) de marzo del año dos mil veintitrés (2023)**, la cual reposa en los archivos de esta Secretaría, a saber:

**“CUARTA RESOLUCIÓN DEL CONSEJO NACIONAL DEL MERCADO DE VALORES
DE FECHA VEINTIUNO (21) DE MARZO DEL AÑO DOS MIL VEINTITRÉS (2023).
R-CNMV-2023-10-MV**

REFERENCIA: Autorización para someter a consulta pública el proyecto de Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores.

RESULTA:

Que, mediante comunicación recibida en esta misma en fecha, el señor superintendente del Mercado de Valores (en lo adelante “superintendente”) elevó al conocimiento y ponderación del Consejo Nacional del Mercado de Valores (en lo adelante “Consejo”), la versión definitiva del proyecto de Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores (en lo adelante “proyecto de Reglamento”), con la finalidad de recibir autorización para iniciar proceso de consulta pública.

Que conforme a las facultades que le confieren la Ley núm. 249-17, del Mercado de Valores de la República Dominicana, que deroga y sustituye la Ley núm. 19-00, del ocho (8) de mayo del año dos mil (2000), promulgada el diecinueve (19) de diciembre de dos mil diecisiete (2017), y su modificación (en lo adelante “Ley núm. 249-17”), y el Reglamento Interno del Consejo, adoptado por este organismo colegiado mediante la Primera Resolución, R-CNMV-2018-06-MV, dictada el veintinueve (29) de noviembre del año dos mil dieciocho (2018) (en lo adelante “Reglamento Interno del Consejo”); el Consejo, sesionando válidamente previa convocatoria cursada con la correspondiente documentación soporte, junto con la tiene a bien exponer lo siguiente:

CONSIDERANDO:

1. Que de la lectura combinada de los artículos 6 y 7 de la Ley núm. 249-17 se desprende que la Superintendencia del Mercado de Valores (en lo adelante “Superintendencia”) constituye un organismo autónomo y descentralizado del Estado, con autonomía administrativa, financiera y técnica, cuyo objeto es promover un mercado de valores ordenado, eficiente y transparente, proteger a los inversionistas, velar por el cumplimiento de la referida ley y mitigar el riesgo sistémico.
2. Que, en atención a lo dispuesto por el artículo 10 de la Ley núm. 249-17, la Superintendencia está integrada por un órgano colegiado, el Consejo, y un funcionario ejecutivo, el superintendente.
3. Que la referida ley, en la parte capital de su artículo 13, establece que el Consejo es el órgano superior de la Superintendencia, con funciones esencialmente de naturaleza normativa, fiscalizadora y de control.
4. Que, aunado a lo anterior, el numeral 5 confiere al Consejo la atribución de “[d]ictar, a propuesta del Superintendente, los reglamentos de aplicación de esta ley.”
5. Que, de igual manera, el artículo 25 de la Ley núm. 249-17 reitera que “[e]l Consejo es el órgano competente para establecer los reglamentos relativos a las actividades del mercado de valores señaladas en esta ley.”
6. Que, por otro lado, el artículo 13, numeral 4, de la Ley núm. 249-17, señala que constituye una atribución del Consejo revisar de manera periódica el marco regulatorio del mercado de valores, adecuándolo a las tendencias y realidades del mercado y proponer, por iniciativa propia o a propuesta del superintendente, las modificaciones que sean necesarias.
7. Que el párrafo I de dicho artículo añade que “[e]n el ejercicio de la potestad reglamentaria, el Consejo y la Superintendencia observarán los principios de legalidad y las reglas de consulta pública, participación y transparencia contenidos en la Constitución de la República y las leyes vigentes”.
8. Que, sobre este particular, el artículo 37 del Reglamento Interno del Consejo establece que “[l]a preparación de los borradores y la colocación en consulta pública previa, es responsabilidad del Superintendente del Mercado de Valores”.

9. Que es de resaltar que el artículo 2 de la mencionada Ley núm. 249-17 revela que las disposiciones contenidas en dicho estatuto jurídico se aplican a todas las personas físicas y jurídicas que realicen actividades, operaciones y transacciones en el mercado de valores de la República Dominicana, con valores de oferta pública que se oferten o negocien en el territorio nacional.
10. Que conforme al artículo 3, numeral 33, de la Ley núm. 249-17, participante del mercado de valores “[e]s la persona física o jurídica, inscrita en el Registro del Mercado de Valores y regulada por la Superintendencia del Mercado de Valores”.
11. Que, a este respecto, el artículo 36 de la mencionada ley establece que “[l]a Superintendencia tendrá un Registro a disposición del público, que podrá ser electrónico, y en él se inscribirán las personas físicas y jurídicas que participen en el mercado de valores, así como la información pública respecto de los valores inscritos en el Registro y de los participantes del mercado de valores regulados por esta ley.”
12. Que a través de comunicación recibida en la Secretaría del Consejo el dieciocho (18) de enero del dos mil veintitrés (2023), el señor superintendente elevó ante este órgano colegiado una solicitud por medio de la que procuraba recibir una autorización para iniciar proceso de consulta pública del proyecto de Reglamento.
13. Que, según la precitada misiva, “[e]l objeto de dicho Proyecto es establecer los criterios y lineamientos generales que deben adoptar los participantes del mercado de valores para procurar la integridad, disponibilidad y confidencialidad de la información y el funcionamiento óptimo de los sistemas de información y de la infraestructura tecnológica. Asimismo, establecer la adopción e implementación de prácticas para la gestión de riesgos de la seguridad cibernética y de la información.”
14. Que, aunado lo anterior, el oficio cursado indicaba que los siguientes participantes habrían de quedar sometidos a las formalidades previstas en el proyecto de Reglamento, a saber:

“

- 1) Los intermediarios de valores;
- 2) Las sociedades administradoras de mecanismos centralizados de negociación;
- 3) Los depósitos centralizados de valores;
- 4) Las entidades de contrapartida central;
- 5) Las sociedades administradoras de fondos de inversión;
- 6) Las sociedades fiduciarias de fideicomiso de oferta pública;

- 7) Las sociedades titularizadoras; y,
- 8) Las sociedades proveedoras de precio.”

15. Que la comunicación del señor superintendente precisó que aquellos participantes del mercado que se encuentren sujetos al ámbito de aplicación del Reglamento de Seguridad Cibernética y de la Información emitido por la Junta Monetaria, deberán cumplir con dichas disposiciones, las cuales primarían ante cualquier contradicción con el proyecto de Reglamento.
16. Que, de las piezas que componen el expediente, se destaca un documento titulado Exposición de Motivos, el cual refiere que ante el desarrollo de la tecnología, y sus riesgos asociados, por la ola creciente de los ciberataques y la importancia que éste fenómeno ha tomado en el mercado de valores dominicano, resulta necesario establecer los criterios y lineamientos generales que deberán adoptar los participantes del mercado de valores -en materia de seguridad cibernética y de la información- para el control interno, uso de herramientas, funcionamiento óptimo de sistemas, infraestructura, seguridad, confidencialidad y administración de riesgos; a los fines de mitigar el riesgo sistémico y velar por la protección de los inversionistas.
17. Que en dicho documento se añade que, debido a la naturaleza cambiante de amenazas cibernéticas, las organizaciones corren riesgos de pérdida de propiedad intelectual y destrucción o alteración de datos, disminución de la confianza pública e interna de las partes interesadas e interrupción de la infraestructura crítica.
18. Que, asimismo, se indica que una falla operativa en el mercado de valores puede afectar negativamente la estabilidad financiera, razón por la que resulta fundamental que las entidades identifiquen cuáles son sus operaciones críticas y activos de información de apoyo, comprender su situación interna y sus dependencias externas, de forma que puedan dar oportuna respuesta a las amenazas cibernéticas que se pueden presentar.
19. Que en el legajo también reposa la comunicación marcada con el número 1580, de fecha seis (6) de febrero del dos mil veintitrés (2023), suscrita por la subgerente de Sistemas e Innovación Tecnológica del Banco Central de la República Dominicana, señora Fabiola Herrera, mediante la que remite al presidente del Consejo opinión técnica sobre el proyecto de Reglamento.
20. Que, a partir de las instrucciones de este órgano colegiado en la reunión de pleno de fecha siete (7) de febrero del dos mil veintitrés (2023), fue celebrada una mesa de trabajo con los equipos técnicos de esta Superintendencia, del Banco Central de la República Dominicana y miembros del Consejo en fecha veintitrés (23) de febrero del dos mil veintitrés (2023).

21. Que, fruto de lo anterior, a través de la comunicación de fecha siete (7) de marzo del dos mil veintitrés (2023), el señor superintendente remitió al Consejo un memorando de posición técnica que responde las observaciones y comentarios formulados por la Subgerencia de Sistemas e Innovación Tecnológica del Banco Central de la República Dominicana.
22. Que, como resultado de lo precedentemente planteado, mediante comunicación recibida en la Secretaría del Consejo en fecha ocho (8) de marzo del dos mil veintitrés (2023), el señor superintendente elevó a ponderación del Consejo una versión actualizada del proyecto de Reglamento para fines de recibir autorización de consulta pública, acompañado una matriz que compila las observaciones y comentarios formulados, junto con las correspondientes argumentaciones de réplicas.
23. Que, posteriormente, mediante comunicación número 3663, de fecha veinte (20) de marzo del dos mil veintitrés (2023), la Subgerencia de Sistemas e Innovación Tecnológica del Banco Central de la República Dominicana remitió al presidente del Consejo nueva opinión técnica con puntos adicionales a considerar en torno al proyecto de Reglamento.
24. Que, atendidos los aspectos sometidos a revisión, mediante comunicación de esta misma fecha, el señor superintendente elevó a decisión de este órgano colegiado una solicitud de autorización para iniciar el proceso de consulta pública del proyecto de Reglamento, cuya última versión recoge todas las consideraciones que fueron vertidas en el proceso de redacción y revisión técnica de la propuesta de norma reglamentaria.
25. Que la Ley núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, de fecha seis (6) de agosto de dos mil trece (2013) (en lo adelante “Ley núm. 107-13”), establece en su artículo 30 que “[l]os estándares mínimos y obligatorios de los procedimientos administrativos que procuran la adopción de reglamentos que poseen un alcance general, cuya finalidad es que la Administración Pública obtenga la información necesaria para su aprobación, además de canalizar el diálogo con los interesados y el público en general, “promoviendo el derecho fundamental a la participación ciudadana como sustento de la buena gobernanza democrática”.
26. Que, conforme la precitada Ley núm. 107-13, serán nulas de pleno derecho las normas administrativas, en las cuales la Administración competente incumpla los principios y criterios del procedimiento aplicable a la elaboración de reglamentos, planes o programas de alcance general, indicados en el artículo 31 de la misma, a saber: “[...] 2. **Decisión bien informada.** El

procedimiento de elaboración del proyecto ha de servir para obtener y procesar toda la información necesaria a fin de garantizar el acierto del texto reglamentario, plan o programa. A tal fin deberán recabarse los estudios, evaluaciones e informes de naturaleza legal, económica, medioambiental, técnica o científica que sean pertinentes. Las alegaciones realizadas por los ciudadanos serán igualmente tenidas en cuenta para hallar la mejor solución posible en el reglamento, plan o programa. 3. **Audiencia de los ciudadanos directamente afectados en sus derechos e intereses.** La audiencia de los ciudadanos, directamente o a través de las asociaciones que les representen, se ha de producir en todo caso antes de la aprobación definitiva del texto reglamentario, plan o programa cuando puedan verse afectados en sus derechos e intereses legítimos. Habrá de otorgarse un plazo razonable y suficiente, en razón de la materia y de las circunstancias concurrentes, para que esa audiencia resulte real y efectiva. La Administración habrá de contar igualmente con un plazo razonable y suficiente para procesar y analizar las alegaciones realizadas. 4. **Participación del público.** La participación del público en general, con independencia de que se vea o no afectado directamente por el proyecto de texto reglamentario, plan o programa, deberá garantizarse antes de la aprobación definitiva salvo texto legal en contrario. 5. **Colaboración entre órganos y entes públicos administraciones.** La Administración competente para la aprobación del reglamento, plan o programa habrá de facilitar y recabar la colaboración de los demás órganos y entes públicos, cuando resulte necesario o conveniente en razón de los efectos significativos que pueda producir, mediante las consultas o informes oportunos.”

27. Que, por su parte, el artículo 23 de la Ley General de Libre Acceso a la Información Pública, núm. 200-04, de fecha veintiocho (28) de julio del año dos mil cuatro (2004) (en lo adelante “Ley núm. 200-04”), establece la obligación de las entidades que cumplen funciones públicas o que administran recursos del Estado de “publicar a través de medios oficiales o privados de amplia difusión, incluyendo medios o mecanismos electrónicos y con suficiente antelación a la fecha de su expedición, los proyectos de regulaciones que pretendan adoptar mediante reglamento o actos de carácter general, relacionadas con requisitos o formalidades que rigen las relaciones entre los particulares y la administración o que se exigen a las personas para el ejercicio de sus derechos y actividades”.
28. Que, aunado a lo anterior, el artículo 24 de la referida Ley núm. 200-04, dispone que las entidades que cumplan funciones públicas o que administran recursos del Estado deberán prever en sus respectivos presupuestos las sumas necesarias para publicar en medios de comunicación colectiva, con amplia difusión nacional, los proyectos de reglamentos y actos de carácter general que son detallados en el artículo 23 de la Ley núm. 200-04.

29. Que el párrafo del precitado artículo expresa que la entidad o persona que cumpla funciones públicas o que administre recursos del Estado, que cuente con un portal de Internet o con una página en dicho medio de comunicación, “deberá prever la existencia de un lugar específico en ese medio para que los ciudadanos puedan obtener información sobre los proyectos de reglamentación, de regulación de servicios, de actos y comunicaciones de valor general, que determinen de alguna manera la forma de protección de los servicios y el acceso de las personas de la mencionada entidad. Dicha información deberá ser actual y explicativa de su contenido, con un lenguaje entendible al ciudadano común.”
30. Que conforme a las disposiciones contenidas en el artículo 45 del Reglamento de la Ley núm. 200-04, aprobado mediante el Decreto núm. 130-05, de fecha veinticinco (25) de febrero del año dos mil cinco (2005) (en lo adelante “Decreto núm. 130-05”), el Estado dominicano en su conjunto, con los organismos, instituciones y entidades descritas en la ley, deberán poner a disposición de la ciudadanía y difundir de oficio la información referida a: “[...] a. Proyectos de regulaciones que pretendan adoptar mediante reglamento o actos de carácter general, relacionadas con requisitos o formalidades que rigen las relaciones entre los particulares y la administración o que se exigen a las personas para el ejercicio de sus derechos y actividades. b. Proyectos de reglamentación, de regulación de servicios, de actos y comunicaciones de valor general, que determinen de alguna manera la forma de protección de los servicios y el acceso de las personas de la mencionada entidad”.
31. Que, paralelamente, el artículo 3, numeral 8, de la Ley núm. 167-21, de Mejora Regulatoria y Simplificación de Trámites del doce (12) de agosto del dos mil veintiuno (2021) (en lo adelante “Ley núm. 167-21”) establece que la consulta pública es “es un mecanismo de participación ciudadana que se utiliza para transparentar el proceso de producción y revisión de las regulaciones, permitiendo la recepción de comentarios por parte de los diferentes grupos interesados y del público en general.”
32. Que, paralelamente, el artículo 6 de la Ley núm. 167-21 instruye a los entes y órganos de la Administración Pública a la creación de sus agendas o planificación regulatoria; cuyo párrafo I, literal g, agrega que “[l]os entes y órganos de la Administración Pública deberán indicar el período en que se pretenden realizar las consultas públicas de las propuestas regulatorias, cuando corresponda.”
33. Que, en cumplimiento con el mandato legal, mediante la Quinta Resolución, R-CNMV-2022-17-MV, en fecha trece (13) de septiembre del año dos mil veintidós (2022), el Consejo aprobó la agenda regulatoria de la Superintendencia, correspondiente al período comprendido de septiembre

del dos mil veintidós (2022), a marzo del dos mil veintitrés (2023), en la cual se incluyó, entre otros proyectos, el proyecto de Reglamento que nos ocupa.

- 34.** Que, no obstante lo anterior, si bien los trabajos de investigación y redacción iniciaron en el periodo de seis (6) meses antes referido, no fue posible sancionar un borrador final del proyecto de Reglamento para consulta fines de consulta pública; razón por la que la iniciativa fue diferida al período comprendido de marzo a septiembre del dos mil veintitrés (2023), atendiendo a lo dispuesto por el artículo 6, párrafo III, del Decreto núm. 486-22, de fecha veinticuatro (24) de agosto del año dos mil veintidós (2022), que aprueba el Reglamento de Aplicación de la Ley núm. 167-21 de Mejora Regulatoria y Simplificación de Trámites (en lo adelante “Decreto núm. 486-22”).
- 35.** Que, en tan sentido, en esta misma fecha, por medio de la Segunda Resolución, R-CNMV-2023-08-MV, este órgano colegiado aprobó la agenda o planificación regulatoria de la Superintendencia, correspondiente al período comprendido de marzo a septiembre del dos mil veintitrés (2023), que incluye el proyecto de Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores.
- 36.** Que el artículo 30 del Decreto núm. 486-22 dispone que los entes y órganos de la Administración Pública promoverán la participación ciudadana en la gestión pública por medio de consultas públicas; a la vez que desglosa la finalidad de las consultas públicas, en tanto contribuyen a que: “1) La Administración pública obtenga información sobre problemas de política pública y su posible solución. 2) El proceso regulatorio se lleve a cabo bajo los principios de transparencia, participación, rendición de cuentas y motivación. 3) La regulación resultante pueda nutrirse de la participación de los actores afectados por el problema y por la regulación. 4) Se canalice el diálogo con otros entes y órganos públicos, con los interesados y el público en general, con ponderación de las políticas sectoriales y derechos implicados y promoviendo el derecho fundamental a la participación ciudadana como sustento de la buena gobernanza democrática. 5) Los actores conozcan y sean parte del proceso regulatorio, contribuyendo a la predictibilidad de la actuación regulatoria.”
- 37.** Que, por su parte, de la lectura combinada del artículo 23 de la Ley núm. 167-21, y del artículo 33 del Decreto núm. 486-22, se desprende que la consulta pública de las propuestas de regulaciones económicas y sociales significativas será de cuarenta y cinco (45) días hábiles.
- 38.** Que el artículo 7 de la Ley núm. 167-21 establece que “[s]e consideran regulaciones económicas y sociales significativas, aquellas que se enmarcan dentro de los siguientes criterios: 1) Crean

nuevas obligaciones para los administrados o hacen más estrictas las obligaciones existentes. 2) Crean o modifican trámites, exceptuando cuando la modificación simplifica o facilita el cumplimiento del particular. 3) Reducen o restringen derechos o prestaciones para los administrados. 4) Establecen definiciones, clasificaciones, restricciones, caracterizaciones o cualquier otro término de referencia, que afecten o puedan afectar los derechos, obligaciones, prestaciones o trámites de los administrados.”

39. Que, de conformidad con el artículo 32 del Decreto núm. 486-22, además de la indicación de la fecha de inicio de la consulta pública en la agenda o planificación regulatoria, la Superintendencia podrá realizar un aviso previo de la consulta pública en medios de comunicación de amplia difusión pública, por lo menos cinco (5) días hábiles de la fecha de inicio; en cuyo caso, este aviso incluiría el objetivo de la consulta, la fecha de inicio y cierre, formas y canales de realización de la consulta y período durante el cual se recibirán los comentarios.
40. Que finalmente, este órgano colegiado es de opinión que, en la era de la digitalización e interconexión de los servicios financieros, resulta prioritario establecer mecanismos de protección de la información y de fortalecimiento de la seguridad cibernética; estableciendo los criterios y lineamientos que, a tales fines, deben adoptar los participantes del mercado de valores.
41. Que, merced de lo expuesto, este organismo colegiado favorece que el proyecto de Reglamento sea sometido a consulta pública, a los fines de recabar la opinión de los participantes del mercado, sectores interesados y público en general.

VISTOS:

- a. La Constitución de la República Dominicana, votada y proclamada por la Asamblea Nacional en fecha trece (13) del mes de junio del año dos mil quince (2015), publicada el diez (10) de julio de dos mil quince (2015).
- b. La Ley núm. 249-17, del Mercado de Valores de la República Dominicana, que deroga y sustituye la Ley núm. 19-00, del ocho (8) de mayo del año dos mil (2000), de fecha diecinueve (19) de diciembre de dos mil diecisiete (2017), y su modificación.
- c. La Ley núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, de fecha seis (6) de agosto del año dos mil trece (2013).

- d.** La Ley núm. 200-04, General de Libre Acceso a la Información Pública, de fecha veintiocho (28) de julio del año dos mil cuatro (2004).
- e.** La Ley núm. 167-21, de Mejora Regulatoria y Simplificación de Trámites, de fecha doce (12) de agosto del dos mil veintiuno (2021).
- f.** El Reglamento de la Ley General de Libre Acceso a la Información Pública, aprobado mediante el Decreto núm. 130-05, de fecha veinticinco (25) de febrero del año dos mil cinco (2005).
- g.** El Decreto núm. 486-22, de fecha veinticuatro (24) de agosto del año dos mil veintidós (2022), que aprueba el Reglamento de Aplicación de la Ley núm. 167-21 de Mejora Regulatoria y Simplificación de Trámites.
- h.** El Reglamento Interno del Consejo Nacional del Mercado de Valores, dictado mediante la Primera Resolución, R-CNMV-2018-06-MV, de fecha veintinueve (29) de noviembre del año dos mil dieciocho (2018).
- i.** La Segunda Resolución de fecha primero (1ro) de noviembre del año dos mil dieciocho (2018), de la Junta Monetaria, que autoriza la publicación del Reglamento de Seguridad Cibernética y de la Información.
- j.** La Quinta Resolución, R-CNMV-2022-17-MV, del Consejo Nacional del Mercado de Valores, de fecha trece (13) de septiembre del año dos mil veintidós (2022), que aprueba la agenda regulatoria de la Superintendencia del Mercado de Valores correspondiente al período septiembre del dos mil veintidós (2022), a marzo del dos mil veintitrés (2023).
- k.** La Segunda Resolución, R-CNMV-2023-08-MV, del Consejo Nacional del Mercado de Valores, de fecha veintiuno (21) de marzo del año dos mil veintitrés (2023), que aprueba la agenda o planificación regulatoria de la Superintendencia del Mercado de Valores, correspondiente al período comprendido de marzo a septiembre del dos mil veintitrés (2023)
- l.** Comunicación de fecha dieciocho (18) de enero del año dos mil veintitrés (2023), suscrita por el señor superintendente del Mercado de Valores, y anexos que cita.
- m.** La comunicación marcada con el número 1580, de fecha seis (6) de febrero del dos mil veintitrés (2023), suscrita por la señora Fabiola Herrera, subgerente de Sistemas e Innovación Tecnológica del Banco Central.

- n. Comunicación de fecha siete (7) de marzo del año dos mil veintitrés (2023), suscrita por el señor superintendente del Mercado de Valores, y anexos que cita.
- o. Comunicación de fecha ocho (8) de marzo del año dos mil veintitrés (2023), suscrita por el señor superintendente del Mercado de Valores, y anexos que cita.
- a. La comunicación marcada con el número 3663, de fecha veinte (20) de marzo del dos mil veintitrés (2023, suscrita por la señora Fabiola Herrera, subgerente de Sistemas e Innovación Tecnológica del Banco Central.
- b. Comunicación de fecha veintiuno (21) de marzo del año dos mil veintitrés (2023), suscrita por el señor superintendente del Mercado de Valores, y anexos que cita.
- c. Los demás documentos que integran el expediente.

POR TANTO:

Después de haber estudiado y deliberado sobre la especie, el **Consejo Nacional del Mercado de Valores**, en el ejercicio de las facultades que le confiere la Ley núm. 249-17, por votación unánime de los miembros presentes en la sesión, conformándose la mayoría legalmente requerida, atendiendo a los motivos expuestos,

RESUELVE:

PRIMERO: AUTORIZAR al señor superintendente a efectuar la publicación de la presente en uno o más medios de comunicación impresos de amplia circulación nacional, así como en el portal institucional, para fines de consulta pública de los participantes del mercado de valores, sectores interesados y público en general; así como publicar el aviso de inicio de consulta pública del proyecto de Reglamento de Seguridad Cibernética y de la Información para el Mercado de Valores, cuyo texto que se transcribe a continuación, conforme el documento sometido por la Superintendencia, elaborado por la Dirección de Regulación e Innovación, a saber:

“PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES”

TÍTULO I DISPOSICIONES GENERALES

CAPÍTULO I Objeto y Alcance

Artículo 1. Objeto. Establecer los criterios y lineamientos generales que deben adoptar los participantes del mercado de valores para procurar la Integridad, disponibilidad y Confidencialidad de la Información y el funcionamiento óptimo de los sistemas de Información y de la Infraestructura Tecnológica. Asimismo, establecer la adopción e implementación de prácticas para la gestión de Riesgos de la Seguridad Cibernética y de la Información.

Artículo 2. Alcance. Las disposiciones del presente Reglamento aplican a:

- 1) Los intermediarios de valores;
- 2) Las sociedades administradoras de mecanismos centralizados de negociación;
- 3) Los depósitos centralizados de valores;
- 4) Las entidades de contrapartida central;
- 5) Las sociedades administradoras de fondos de inversión;
- 6) Las sociedades fiduciarias de fideicomisos de oferta pública;
- 7) Las sociedades titularizadoras;
- 8) Las sociedades proveedoras de precios; y,
- 9) Los emisores, en tanto a los requerimientos mínimos que determine la Superintendencia del Mercado de Valores mediante norma técnica u operativa.

Párrafo I. Este Reglamento comprende las disposiciones normativas relativas al régimen general para la administración integral de Riesgos Tecnológicos, de seguridad cibernética y de seguridad de la información, así como el establecimiento de disposiciones relativas al gobierno interno de los participantes del mercado de valores. Las disposiciones contenidas en este reglamento serán de carácter supletorio para los participantes del mercado de valores que, en virtud de su participación en el sistema de pagos y liquidación de valores y el correspondiente intercambio de Información Esencial, se encuentren dentro del ámbito de aplicación de la normativa especializada emitida por la Junta Monetaria relacionada con estos Riesgos.

Párrafo II. Los participantes del mercado de valores que no se encuentren sujetos al sistema de pagos y liquidación de valores, podrán remitir los requerimientos relativos a incidentes y Vulnerabilidades al Centro Sectorial de Respuesta a Incidentes de Ciberseguridad para el Sistema Financiero y de Pagos (SPRICS), de conformidad a lo establecido en el Reglamento de Seguridad Cibernética y de la Información emitido por la Junta Monetaria.

Párrafo III. Para los demás participantes del mercado de valores no expresamente citados en este artículo, la Superintendencia podrá dictar disposiciones mínimas de Seguridad Cibernética en tanto se conecten a los sistemas de la Superintendencia para remisión documental y de información frente a sus obligaciones de reportería.

CAPÍTULO II

Definiciones

Artículo 3. Definiciones. En adición a los términos definidos por la Ley núm. 249-17 del Mercado de Valores de la República Dominicana del diecinueve (19) de diciembre de dos mil diecisiete (2017), que deroga y sustituye la Ley núm. 19-00 del ocho (8) de mayo del año dos mil (2000) (en lo adelante, la “Ley”), para los fines del presente Reglamento, los términos y conceptos que se detallan a continuación tienen el significado siguiente:

- 1) **Acceso:** Capacidad y medios para comunicarse o interactuar con un sistema, utilizar recursos de dicho sistema para manejar y adquirir conocimiento de la Información que contiene o controlar sus componentes y funciones.
- 2) **Amenaza:** Circunstancia desfavorable que puede ocurrir y que, de suceder, tendría consecuencias negativas sobre la Seguridad Cibernética y de la Información.
- 3) **Bases de Datos:** Serie de datos organizados y relacionados entre sí, que son recolectados y explotados por los sistemas de Información del participante del mercado de valores y por los proveedores de servicios mediante el mantenimiento de una conexión electrónica o el intercambio de Información Esencial.
Siglas
- 4) **BSA:** Corresponde a las siglas en inglés a Software Alliance (Alianza de Software).
- 5) **CIS:** Corresponde a las siglas en inglés a *Center for Internet Security* (Centro de Seguridad de Internet).

- 6) **CMMI:** Corresponde a las siglas en inglés de *Capability Maturity Model Integration* (modelos que contienen las mejores prácticas que ayudan a las organizaciones a mejorar sus procesos).
- 7) **Confidencialidad:** Preservación de la Información de forma que la misma no sea divulgada, total o parcial, sin autorización de su titular.
- 8) **Control de Acceso:** Proceso de concesión o denegación de solicitudes específicas para obtener y utilizar Información y servicios de procesamiento de Información relacionados o entrar en instalaciones físicas específicas.
- 9) **COSO:** Corresponde las siglas en inglés al *Committee of Sponsoring Organizations of the Treadway* (Comité de Organizaciones Patrocinadoras de la Comisión Treadway).
- 10) **COBIT:** Corresponde a las siglas en inglés a *Control Objectives for Information and related Technology* (Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas).
- 11) **Dispositivos Móviles:** Dispositivos informáticos portátiles que: (i) son de tamaño pequeño, de modo que pueden ser transportados fácilmente por un solo individuo; (ii) están diseñados para funcionar sin conexión física; (iii) poseen almacenamiento de datos local, no extraíble; y, (iv) operan durante largos períodos con una fuente de alimentación autónoma. Los Dispositivos Móviles también pueden incluir capacidades de comunicación de voz, sensores electrónicos que permitan capturar y procesar Información o características integradas para sincronizar datos locales con ubicaciones remotas.
- 12) **Encriptación:** Proceso mediante el cual la Información o archivos son alterados en forma matemática, utilizando una llave, con el objetivo de evitar que una persona no autorizada pueda interpretarlos.
- 13) **Entidad Interconectada:** Persona jurídica habilitada mediante una relación contractual para mantener una conexión electrónica o intercambio de Información con un participante del mercado de valores.
- 14) **Firmware:** Conjunto de datos e instrucciones para el funcionamiento de un dispositivo de computación, almacenado como Software de solo lectura en dicho dispositivo, debiendo permanecer inalterado durante su ejecución.

- 15) **GDPR:** Corresponde a las siglas en inglés de *General Data Protection Regulation* (Regulación General de Protección de Datos) de la Unión Europea.
- 16) **Gestión de Parches:** Proceso que consiste en mantener actualizados los sistemas y aplicaciones o Software para corregir Vulnerabilidades o errores que pueden ser explotados por atacantes.
- 17) **Gestión de Riesgo Tecnológico:** Método para determinar, analizar, valorar y clasificar el Riesgo con el objeto de implementar mecanismos que permitan controlarlo.
- 18) **Hardware:** Conjunto de equipos físicos que componen una computadora.
- 19) **Hipervisor:** Tecnología que se compone por una capa de Software que permite utilizar, al mismo tiempo, diferentes sistemas operativos o máquinas virtuales en una misma computadora central.
- 20) **IAPP:** Corresponde a las siglas en inglés al *International Association of Privacy Professionals* (Asociación Internacional de Profesionales de la Privacidad).
- 21) **IEC:** Corresponde a las siglas en inglés al *International Electrotechnical Commission* (Comisión Electrotécnica Internacional).
- 22) **Incidente:** Evento que pone en peligro la Integridad, disponibilidad y Confidencialidad de la Infraestructura Tecnológica o la Información procesada, almacenada o transmitida por dicho sistema y que constituye una violación o Amenaza inminente de violación de políticas o Procedimientos de seguridad o políticas de uso aceptable.
- 23) **Incidentes Cibernéticos y de la Información:** Evento o serie de eventos inesperados o no deseados contra un sistema que tienen una probabilidad significativa de comprometer la Información del participante del mercado de valores, provocando su pérdida o uso indebido, la interrupción parcial o total de los sistemas o arriesgando su Integridad, disponibilidad y Confidencialidad.
- 24) **Información:** Cualquier forma de registro electrónico, óptico, magnético u otros medios similares, susceptible de ser procesada, distribuida y almacenada.
- 25) **Información Esencial:** Es aquella que facilita el desarrollo de las actividades fundamentales de la entidad y que sustentan la operatividad de la Infraestructura Tecnológica.

- 26) **Información Esencial de Tipo Maestro:** Conjunto de datos básicos cuyos registros sufren poca o ninguna variación en el tiempo.
- 27) **Información Esencial de Tipo Transaccional:** Conjunto de datos cuyos registros contienen Información sobre las transacciones realizadas en un sistema de Información.
- 28) **Infraestructura Tecnológica:** Aquellos equipos y sistemas con que cuenta el participante del mercado de valores para procesar la Información y las adecuaciones del espacio físico que los aloja.
- 29) **Integridad:** Propiedad que poseen los datos para asegurar que los mismos no han sido alterados de manera no autorizada o destruidos de manera inadecuada durante su creación, transmisión o almacenamiento.
- 30) **IP:** Corresponde a las siglas en inglés de *Internet Protocol* (Protocolo de Internet).
- 31) **ISO:** Corresponde a las siglas en inglés de *Internacional Organization for Standardization* (Organización Internacional de Normalización).
- 32) **ISF:** Corresponde a las siglas en inglés de *Information Security Forum* (Foro de la Seguridad de la Información).
- 33) **ITIL:** Corresponde a las siglas en inglés de *Information Technology Infrastructure Library* (Biblioteca de Infraestructura de Tecnologías de Información).
- 34) **Mecanismos de Control de Acceso:** Medidas de seguridad diseñadas para detectar, restringir y permitir el Acceso a un sistema de Información o a un entorno local físico.
- 35) **Marco de Trabajo:** Son los marcos de referencia de control, estándares internacionales u otros estudios que ayuden a monitorear y mejorar las actividades críticas en el ámbito de la Tecnología de la Información, aumentar el valor del negocio y reducir sus Riesgos. Tales como: BSA, CIS, CMMI, COBIT, COSO, GDPR, IAPP, ISF, ISO 9001, ISO 20000, ISO 27001, ISO 27002, ISO 31000, IEC, ITIL, NIST, OWASP, PMBOK, SWIFT, entre otros estándares reconocidos internacionalmente que puedan aplicar.
- 36) **Monitoreo Continuo:** Proceso implementado para mantener en estado de vigilancia, el funcionamiento de los controles de seguridad de los sistemas de Información y la Infraestructura Tecnológica de los que depende la operación del participante del mercado de valores.

- 37) **NIST:** Corresponde a las siglas en inglés de *National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología).
- 38) **OWASP:** Corresponde a las siglas en inglés de *Open Web Application Security Project* (Proyecto Abierto de Seguridad de Aplicaciones Web).
- 39) **PBX:** Corresponde a las siglas en inglés de *Private Branch Exchange* (Central Privada Automática).
- 40) **Plan de Contingencia:** Conjunto de Procedimientos alternativos a la operatividad normal del participante del mercado de valores, cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto operativo y financiero que pueda ocasionar cualquier evento inesperado.
- 41) **Plan de Continuidad de Negocio:** Conjunto formado por planes de actuación, emergencia, financiero, de comunicación y Plan de Contingencia, destinados a mitigar el impacto provocado por la concreción de determinado Riesgo sobre la Información y los procesos de negocio de un participante del mercado de valores.
- 42) **PMBOK:** Corresponde a las siglas en inglés de *Project Management Body of Knowledge* (Guía de los Fundamentos para la Dirección de Proyectos).
- 43) **Problema:** Es la causa desconocida de un Incidente.
- 44) **Procedimientos:** Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción por medio de los cuales se asegura el cumplimiento de una función operativa.
- 45) **Procesos Críticos:** Procesos indispensables para la continuidad del negocio y las operaciones del participante del mercado de valores, y cuya falta de identificación o aplicación deficiente puede generar un impacto financiero negativo.
- 46) **Riesgo:** Es la posibilidad de ocurrencia de eventos que impacten negativamente los objetivos del participante del mercado de valores y su situación financiera.
- 47) **Riesgos Tecnológicos:** Posibilidad de sufrir un impacto adverso relacionado con la afectación de la Integridad, disponibilidad y Confidencialidad de la Información o de la Infraestructura Tecnológica.

- 48) **Seguridad Cibernética y de la Información:** La protección de los sistemas de Información y de la Información en todos sus formatos, durante su almacenamiento, procesamiento o transmisión, contra el Acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados.
- 49) **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora
- 50) **SWIFT:** Corresponde a las siglas en inglés de *Society for Worldwide Interbank Financial Telecommunication* (Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales).
- 51) **Tecnología de Información:** Conjunto de herramientas y métodos empleados para llevar a cabo la administración de la Información.
- 52) **Vulnerabilidad:** Es una debilidad en el sistema de Información, sus Procedimientos de seguridad, implementación o controles internos que podrían permitir la materialización de una Amenaza.

TÍTULO II

RÉGIMEN GENERAL SOBRE SEGURIDAD CIBÉRNETICA Y DE LA INFORMACIÓN

CAPÍTULO I

Marco de Trabajo y Responsabilidades

Artículo 4. Marco de Trabajo. Los participantes del mercado de valores sujetos al presente Reglamento deben establecer acciones para el desarrollo, implementación y mantenimiento de un programa de Seguridad Cibernética y de la Información y, a la vez, optar por uno o varios Marcos de Trabajo conforme a sus requerimientos y necesidades que se encuentren acorde a los estándares reconocidos internacionalmente que puedan aplicar.

Párrafo I. El programa de Seguridad Cibernética y de la Información requerido en este Reglamento debe ser diseñado de acuerdo con la naturaleza, tamaño, complejidad y perfil de Riesgos del negocio de cada participante del mercado de valores.

Párrafo II. El programa de Seguridad Cibernética y de la Información comprende las estrategias, actividades, procesos y políticas que los participantes del mercado de valores deben documentar, desarrollar e implementar, a fin de cumplir las disposiciones y requerimientos establecidos en este

Reglamento. Dicho programa se debe basar en la identificación de los eventos que podrían tener un efecto adverso sobre la continuidad de las operaciones, así como el impacto financiero, humano y reputacional sobre el participante del mercado de valores.

Párrafo III. Los Emisores deben adoptar un marco de gobernanza de ciberseguridad especial sujeto a la no objeción de la Superintendencia, que incluya los criterios de información definidos en el artículo 5 (Criterios de Información) del presente Reglamento, las políticas, procesos y estructuras de Gestión de Riesgos definidas con controles pertinentes adaptados a la naturaleza de los Riesgos de ciberseguridad a los que se enfrenta la sociedad y a los recursos de que dispone. Las prácticas efectivas incluyen a modo de referencia:

- 1) Definir un marco de gobernanza para apoyar la toma de decisiones basadas en la política de Riesgos;
- 2) Garantizar el compromiso activo de la Alta Gerencia y, el compromiso a nivel del consejo de administración con las cuestiones de ciberseguridad;
- 3) Identificar marcos y estándares para abordar la ciberseguridad; d. Utilizar métricas y umbrales para informar los procesos de gobernanza; y,
- 4) Realizar evaluaciones internas de Riesgos de ciberseguridad.

Artículo 5. Criterios de Información. Los participantes del mercado de valores deben observar los siguientes criterios para el establecimiento de sus políticas y Procedimientos para el control y la gestión de Riesgos en materia de Seguridad Cibernética y de la Información:

- 1) **Autenticación o autenticación:** Es el acto de validar la identidad de un usuario para otorgarle Acceso a recursos tecnológicos.
- 2) **Auditabilidad o trazabilidad:** Es el proceso que facilita la reconstrucción, revisión y análisis de la secuencia de eventos que, a la vez, permite el registro y Monitoreo Continuo de los distintos recursos por parte de los usuarios que han sido previamente autorizados a manipular la Información.
- 3) **Confiabledad:** Los sistemas deben brindar la Información correcta, completa, oportuna y exacta que será utilizada en la operación del participante del mercado de valores, en la toma de decisiones, en la preparación de estados financieros y demás Información para su remisión a los órganos reguladores competentes.

- 4) **Confidencialidad:** Se debe brindar protección a la Información contra la divulgación no autorizada o inadecuada en virtud de las disposiciones legales y normativas aplicables.
- 5) **Disponibilidad:** Los recursos y la Información deben estar disponibles en el tiempo y la forma requerida por los usuarios o las autoridades públicas competentes en el ejercicio de sus facultades legales.
- 6) **Efectividad:** La Información y los Procedimientos para su manejo deben ser relevantes, pertinentes y eficientes en términos de tiempo, de forma que garanticen el proceso del negocio. De igual forma, deben presentarse en forma correcta, coherente, completa y que puedan utilizarse oportunamente.
- 7) **Eficiencia:** La gestión y manejo de la Información debe realizarse mediante una óptima utilización de los recursos.
- 8) **Integridad:** Propiedad que poseen los datos y que asegura que los mismos no han sido alterados de manera no autorizada o destruidos de forma inadecuada, durante su creación, transmisión o almacenamiento.

Artículo 6. Responsabilidades en materia de seguridad. A los efectos del presente Reglamento, es responsabilidad de los participantes del mercado de valores:

- 1) Establecer y mantener actualizado un sistema de gestión que proporcione un enfoque estándar, formal y continuo para la Seguridad Cibernética y de la Información y procesos del negocio;
- 2) Definir políticas y Procedimientos para la Seguridad Cibernética y de la Información conforme a las Mejores Prácticas. Dichas políticas y Procedimientos deben procurar que la ejecución de los criterios de control interno relativos a eficacia, eficiencia y cumplimiento se encuentren alineados a los objetivos y las actividades del participante del mercado de valores. Las políticas y Procedimientos en la materia deben ser aprobadas por el consejo de administración;
- 3) Asegurar la Integridad, Confidencialidad y disponibilidad de la Información almacenada en sus sistemas y de la Información en tránsito, almacenada y procesada;
- 4) Preservar la Información privilegiada, reservada y confidencial;

- 5) Gestionar la privacidad de los datos en la forma contemplada en las leyes, normativa vigente aplicable y los Marcos de Trabajo reconocidos internacionalmente sobre la materia. De igual forma, guiar y coordinar la implementación de políticas, Procedimientos y actividades para asegurar que se cumplan las directivas sobre privacidad de los datos;
- 6) Formular, mantener y ejecutar un plan de tratamiento de Riesgos de Seguridad Cibernética y de la Información alineado con los objetivos estratégicos y operativos del participante del mercado de valores. Dicho plan debe de identificar las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los Riesgos identificados en la materia;
- 7) Revisar y monitorear de forma regular, la efectividad y cumplimiento de las disposiciones contenidas en este Reglamento y sus políticas y Procedimientos de control. Además, deben incluir las excepciones y resultados de las autoevaluaciones y mantener evidencia del Monitoreo Continuo realizado;
- 8) Identificar brechas y Vulnerabilidades de manera periódica;
- 9) Definir y evaluar las responsabilidades y competencias de sus empleados y de los proveedores de servicios en lo concerniente a la Seguridad Cibernética y de la Información;
- 10) Capacitar a sus empleados sobre la forma de interconectar con la Superintendencia; y,
- 11) Establecer, implementar, mantener y monitorear los controles, procesos y Procedimientos de continuidad de negocio o de recuperación que aseguren un nivel aceptable de Seguridad Cibernética y de la Información ante desastres o situaciones adversas.

CAPÍTULO II

Administración Integral de Riesgos Tecnológicos, Seguridad Cibernética y de la Información

Artículo 7. Gestión de Riesgos Tecnológicos. Los participantes del mercado de valores deben monitorear diariamente los Riesgos que implica el uso actual y futuro de la Tecnología de la Información, desde su concepción, desarrollo e implementación. Al efecto, dicho monitoreo incluye los entornos y procesos internos, en función del análisis de las Amenazas, Vulnerabilidades, controles, impacto y política de Riesgos establecidos por su consejo de administración y el alcance de dichas evaluaciones.

Artículo 8. Metodología para la Gestión de Riesgos. La Gestión de Riesgos Tecnológicos debe llevarse a cabo a través de metodologías que contemplen un análisis del Riesgo inherente al participante del mercado de valores y que, de forma cuantitativa y cualitativa, recopile el surgimiento e identificación de nuevos Riesgos, Amenazas y Vulnerabilidades, así como la probabilidad de ocurrencia, posible impacto en la operatividad del negocio y los controles necesarios para su mitigación.

Párrafo. Las evaluaciones de Riesgo deben contemplar, como mínimo, la divulgación no autorizada de la Información, su corrupción accidental o deliberada, manipulación y la disponibilidad de los entornos en cualquier período.

Artículo 9. Gestión de Riesgos Tecnológicos de terceros. Los participantes del mercado de valores deben verificar que las disposiciones de este Reglamento son cumplidas por cualquier Entidad Interconectada mediante el mantenimiento de una conexión electrónica o por el intercambio de Información Esencial, a través de cualquier medio digital, en la medida en que dicha vinculación pueda comprometer la estabilidad del mercado de valores y la salvaguarda de la Información que manejan.

CAPÍTULO III

Gestión y Control de la Seguridad Cibernética y de la Información

Artículo 10. Políticas y Procedimientos de seguridad. En el marco del programa de Seguridad Cibernética y de la Información, los participantes del mercado de valores deben diseñar, implementar y mantener políticas que contemplen los Procedimientos para la gestión de la Seguridad Cibernética y de la Información bajo el Marco de Trabajo. Dichas políticas y Procedimientos deben aplicar criterios de control interno relativos a la protección de activos de la organización, datos, Información y servicios de Tecnología de la Información.

Párrafo I. Las políticas y Procedimientos citadas anteriormente deben ser aprobadas por el consejo de administración y posteriormente comunicadas a los empleados, proveedores de servicios, Entidades Interconectadas y a las demás partes externas relevantes.

Párrafo II. Los participantes del mercado de valores deben elaborar y aplicar las políticas y Procedimientos citados en este Reglamento. Asimismo, deben documentar todos los procesos implementados para la gestión de la Seguridad Cibernética y de la Información.

Artículo 11. Educación y creación de conciencia. Los empleados del participante del mercado de valores y, cuando sea pertinente, los proveedores de servicios, afiliados o usuarios, deben recibir entrenamiento apropiado y periódico sobre las políticas y Procedimientos de Seguridad Cibernética y

de la Información. Esto incluye los requerimientos de seguridad, las responsabilidades legales y los controles del negocio. De igual forma, deben recibir entrenamiento en el uso correcto de las facilidades de procesamiento de Información.

Artículo 12. Gestión del ciclo de vida de los activos de Tecnologías y de la Información. Los participantes del mercado de valores deben desarrollar un esquema de gestión de activos de Tecnologías y de la Información a través de su ciclo de vida que contemple, al menos, lo siguiente:

- 1) Adquisición de todos los activos de Tecnologías y de la Información conforme a lo dispuesto en el artículo 41 (Gestión de proveedores externos) de este Reglamento y sus políticas y prácticas de adquisición;
- 2) Desplegar los activos de Tecnologías y de la Información siguiendo el ciclo de vida de implementación, incluyendo la gestión de cambios y pruebas de aceptación dispuestos en este Reglamento;
- 3) Procedimientos para identificar y clasificar los activos de Tecnologías y de la Información críticos y sensibles;
- 4) Registro actualizado y exacto de los activos de Tecnologías y de la Información necesarios para proveer los servicios, incluyendo:
 - a) Identificación específica del activo de Tecnologías y de la Información;
 - b) Implicaciones de pérdida y prioridad de recuperación;
 - c) Locación;
 - d) Propietario o custodio designado;
 - e) Clasificación según su Confidencialidad y Riesgo asociado.
- 5) Procedimientos de control para la devolución y asignación de los activos de Tecnologías y de la Información a los usuarios, con aceptación y firma de responsabilidades, según corresponda;
- 6) Definir responsabilidades de los empleados, proveedores de servicios y otras partes externas sobre la protección física de cada activo;
- 7) Establecer un plan de mantenimiento preventivo para todo el Hardware, considerando las recomendaciones del proveedor del servicio, el Riesgo en caso de interrupción del servicio, falla o la necesidad del reemplazo del activo;

- 8) Definir Procedimientos para el manejo adecuado cuando el activo de Tecnologías y de la Información es eliminado o destruido;
- 9) Definir Procedimientos para la seguridad de los activos de Tecnologías y de la Información fuera de las instalaciones del participante del mercado de valores, teniendo en cuenta los diferentes Riesgos asociados;
- 10) Procedimientos para advertir a los usuarios las responsabilidades y Procedimientos de seguridad para proteger los activos de Tecnologías y de la Información desatendidos; y,
- 11) Revisar los activos de Tecnologías y de la Información que contengan medios de almacenamiento para asegurar que los datos sensibles y Software licenciado se hayan removido o se hayan sobrescrito con seguridad antes de su disposición, eliminación o reutilización.

Artículo 13. Aplicaciones de estaciones de trabajo. Los participantes del mercado de valores deben establecer procesos para la gestión adecuada de la Seguridad Cibernética y de la Información de las aplicaciones instaladas en las estaciones de trabajo, contemplando los aspectos siguientes:

- 1) Inventario de las aplicaciones de estaciones de trabajo: Las aplicaciones de estaciones de trabajo deberán estar registradas en un inventario o su equivalente;
- 2) Protección de los archivos con Información confidencial: Los archivos creados en aplicaciones de estaciones de trabajo, cuyo contenido sea Información Confidencial, deben ser protegidos mediante la validación de la entrada, aplicando Mecanismos de Control de Acceso;
- 3) Desarrollo de aplicaciones de estaciones de trabajo: Debe ser llevado a cabo según la metodología de desarrollo seguro, adoptada por la entidad.

Artículo 14. Aplicaciones del negocio. Los participantes del mercado de valores deben implementar controles de seguridad para las aplicaciones del negocio que contemplen, al menos, lo siguiente:

- 1) **Protección de las aplicaciones:** Deben utilizar funcionalidades de Seguridad Cibernética y de la Información alineadas a la infraestructura técnica de seguridad, que permitan el cumplimiento de los requerimientos de Confidencialidad e Integridad de la Información;
- 2) **Protección de las aplicaciones basadas en navegación:** Deben establecer controles específicos de Seguridad Cibernética y de la Información sobre las aplicaciones y servicios

transaccionales, tanto internos como externos, que apoyen los servicios hacia internet, basados en el navegador y en los servidores donde se ejecutan; y,

- 3) **Validación de la Información en las aplicaciones de negocio:** Deben incorporar los controles de Seguridad Cibernética y de la Información que protejan la Confidencialidad e Integridad de la Información al ser ingresada, procesada o extraída de la aplicación.

Artículo 15. Clasificación y etiquetado de la Información. Los participantes del mercado de valores deben desarrollar las políticas y Procedimientos que aseguren que la Información recibe la protección adecuada de acuerdo a su importancia en términos de valor, requisitos legales, criticidad y sensibilidad a la divulgación o modificación no autorizada. Por lo que, solo las personas autorizadas pueden acceder a la Información almacenada.

Párrafo. Los Procedimientos de gestión de documentos físicos y digitales deben incluir las etapas de creación, clasificación, almacenamiento, adquisición, modificación y destrucción de documentos, así como los mecanismos de control para la protección de la Información acorde a su nivel de sensibilidad, Confidencialidad y períodos de conservación.

Artículo 16. Privacidad de la Información. Los participantes del mercado de valores deben desarrollar políticas y Procedimientos de protección de datos personales y de privacidad de la información según las leyes y normativas vigentes y el Marco de Trabajo. Dichas políticas y Procedimientos deben establecer, como mínimo, lo siguiente:

- 1) Mecanismos para la identificación, gestión y destrucción de Información confidencial identificable de los clientes y de los empleados;
- 2) Evaluaciones de Riesgo sobre la privacidad de la Información personal gestionada por procesos y aplicaciones del negocio;
- 3) Documentación del uso dado a la Información;
- 4) Mecanismos para la obtención de la aprobación por parte de los titulares de la Información antes de recopilar, procesar, almacenar o divulgarla a terceros;
- 5) Cifrado de la Información y gestión eficiente de las llaves de cifrado;

- 6) Uso de técnicas de enmascaramiento de datos para ocultar partes de la Información al momento de ser almacenada o transmitida;
- 7) Protección de los metadatos relacionados con la privacidad (atributos de archivos o Información descriptiva que pudiera contener Información personal); y,
- 8) Protocolos de notificación al órgano interno aplicable y a los titulares de la Información cuando se produce una violación de la privacidad.

Artículo 17. Obligaciones contractuales. Los contratos suscritos entre los participantes del mercado de valores y sus empleados, proveedores de servicios, Entidades Interconectadas y demás partes externas a los cuales se les concede Acceso a la Información, deben establecer las responsabilidades generales de las partes, disposiciones sobre la Confidencialidad y no divulgación de la Información, protección de datos y especificaciones sobre Seguridad Cibernética y de la Información. De igual forma, las disposiciones sobre las citadas materias deben prolongarse luego de la finalización de la relación contractual por el período definido que se defina en el acuerdo en virtud de la naturaleza del Acceso a la Información concedido.

Párrafo. Asimismo, el participante del mercado de valores debe conservar el derecho de auditar los procesos y controles de dichos proveedores de servicios o Entidad Interconectada.

Artículo 18. Protección contra la fuga de Información. Los participantes del mercado de valores deben mantener políticas, Procedimientos y mecanismos de protección contra la fuga de Información (*Data Loss Prevention -DLP*) a los sistemas, Infraestructura Tecnológica y entornos locales que procesan, almacenan o transmiten Información sensible.

Artículo 19. Registros de usuarios. Los participantes del mercado de valores deben mantener políticas y Procedimientos formales de altas y bajas de usuarios con objeto de garantizar y cancelar el Acceso a todos los sistemas y servicios de Información.

Artículo 20. Gestión de identidades y Mecanismo de Control de Acceso. Los participantes del mercado de valores deben mantener las políticas y Procedimientos de gestión de identidades y de Mecanismos de Control de Acceso que apliquen a los empleados, proveedores de servicios y demás partes externas y personas autorizadas que tengan Acceso a los sistemas de Información e Infraestructura Tecnológica, incluyendo:

- 1) Procedimientos documentados para la administración y autenticación de identidades a nivel institucional, incluyendo la doble autenticación;

- 2) Procedimiento documentado de asignación de roles y privilegios por tipo de usuario y componente de la Infraestructura Tecnológica;
- 3) Procedimiento para establecer los Mecanismos de Control de Acceso de los usuarios a los distintos componentes de la Infraestructura Tecnológica basado en los principios del menor privilegio;
- 4) Establecimiento de directrices generales para la asignación y utilización de cuentas privilegiadas en los sistemas de Información y aplicaciones del negocio, que regulan la asignación y el uso aceptable de las referidas cuentas a los casos que estrictamente lo ameriten tras obtener la autorización escrita por parte del órgano interno aplicable; y,
- 5) Procedimientos para la gestión de las autorizaciones de Acceso de los usuarios.

Párrafo I. Los Mecanismos de Control de Acceso deben considerar, al menos, lo siguiente:

- a) Contraseña o tóken físico o digital, tarjeta inteligente, certificado digital o similar; y,
- b) Elementos biométricos, como huella dactilar, patrón de iris, reconocimiento de voz, estilo de escritura o similares.

Párrafo II. Los participantes del mercado de valores pueden establecer uno o más Mecanismos de Control de Acceso, según el grado de criticidad de los sistemas de Información y otros componentes de la Infraestructura Tecnológica a los que cada usuario debe acceder conforme a los roles asignados y en virtud de los resultados de las evaluaciones de Riesgos Tecnológicos o de la funcionalidad de los Mecanismos de Control de Acceso.

Artículo 21. Gestión de contraseñas. Los participantes del mercado de valores deben mantener políticas y Procedimientos para la gestión segura de contraseñas de los sistemas de Información y los componentes de la Infraestructura Tecnológica, los cuales deben considerar, al menos, lo siguiente:

- 1) Formato de contraseñas y reglas relativas a la longitud;
- 2) Cambio de contraseñas temporales en su primera conexión y de manera periódica; y,
- 3) Registro de contraseñas utilizadas e impedimento de su reutilización.

Párrafo. Los empleados de los participantes del mercado de valores deben suscribir compromiso donde reconozcan la responsabilidad de mantener confidenciales las contraseñas personales para el Acceso a los sistemas de Información y los componentes de la Infraestructura Tecnológica.

Artículo 22. Seguridad física y del entorno. Los participantes del mercado de valores deben implementar políticas, Procedimientos y mecanismos para la protección de la seguridad física y el entorno de las instalaciones del negocio, según el Marco de Trabajo y la naturaleza de su actividad.

Párrafo I. Dichas políticas, Procedimientos y mecanismos deben contemplar, al menos, lo siguiente:

- 1) Procedimientos para la protección física de entornos críticos del participante del mercado de valores que contemplen la gestión del personal autorizado, uso de identificación en lugares visibles, documentación de entrada y salida autorizada de activos de Tecnologías y de la Información y control de visitas al entorno;
- 2) Mecanismos de control de visitas, incluyendo el registro de entrada y salida, uso obligatorio de identificación, Acceso limitado y bajo supervisión a las áreas autorizadas y el retorno obligatorio de los mecanismos de Acceso físico entregados;
- 3) Mecanismos para la protección de la Infraestructura Tecnológica y equipos especializados contra el daño causado por alguna Amenaza ambiental; y,
- 4) Monitoreo y control de la temperatura y humedad de los entornos conforme a los requerimientos definidos por los fabricantes.

Párrafo II. Los mecanismos para la protección de la seguridad física y el entorno de las instalaciones del negocio deben asegurar:

- 1) El ocultamiento de la ubicación de los entornos críticos para prevenir el Acceso no autorizado y el mantenimiento de la Confidencialidad de la misma mediante el uso señalizaciones discretas y la exclusión de directorios telefónicos y de portales informativos;
- 2) El fortalecimiento de la seguridad perimetral mediante el uso de paredes sólidas, ventanas y puertas blindadas, mecanismos contra robos de equipos informáticos críticos y documentación sensible en formato físico;

- 3) La instalación de controles físicos tales como cerrojos digitales, dispositivos de Acceso biométrico, cámaras de vigilancia en puntos vulnerables, sistemas de detección de intrusos, así como el despliegue de guardianes de seguridad en los entornos que sea necesario;
- 4) Los mecanismos para la protección de los cables de alimentación energética que cubran aspectos como la segregación de los cables de comunicaciones, instalación oculta y distinta de las rutas públicas, puntos de inspección y terminación cerrados y fuentes alternas; y,
- 5) Los mecanismos para el aseguramiento de la disponibilidad energética, instalación de equipos contra fluctuación de cargas, uso de generadores eléctricos de emergencia, instalación de luces de emergencia y la ubicación de interruptores cerca de las puertas de emergencia para facilitar el apagado rápido en caso de que sea necesario.

Párrafo III. Los entornos críticos deben ser construidos utilizando materiales resistentes a incendios y libres de Amenazas intrínsecas, tales como materiales combustibles y químicos peligrosos. De igual forma, deben contar con sistemas de detección y mitigación de incendios conforme al Marco de Trabajo.

Párrafo IV. Los participantes del mercado de valores deben capacitar a sus empleados sobre los protocolos para emergencias causadas por desastres naturales, incendios o situaciones de fuerza mayor.

CAPÍTULO IV

Operaciones de los Sistemas de Información y Continuidad del Negocio

Artículo 23. Sistemas informáticos e Infraestructura Tecnológica. Los participantes del mercado de valores deben procurar que los sistemas informáticos y la Infraestructura Tecnológica puedan ser protegidos contra toda Amenaza. Por lo que, deben configurar adecuadamente los controles de Seguridad Cibernética y de la Información integrados por defecto, incluyendo:

- 1) Compatibilidad con otros sistemas de Información, redes e instalaciones de telecomunicaciones utilizados, a fin de asegurar el establecimiento de controles de seguridad integrados;
- 2) Administración centralizada de sistemas a través de centros de operaciones de red, sistemas y seguridad, o mecanismos equivalentes;

- 3) Gestión adecuada de las actualizaciones de seguridad, listas de Control de Acceso, firmas y reglas de *firewalls* (cortafuegos); y,
- 4) Diseño adecuado de la red, contemplando segregación de sistemas de Información mediante el uso de dominios de seguridad, aislamiento de tipos particulares de tráfico de red, la restricción de puntos de entrada a la red y la denegación de Acceso a dispositivos no registrados. Al efecto, deben establecer la incorporación de mecanismos de autenticación, el diseño de esquemas de *firewalls* (cortafuegos) para evitar su omisión y la priorización del tráfico de red para reducir la latencia en el uso de servicios críticos.

Artículo 24. Gestión de cambio. Los participantes del mercado de valores deben contar con una política de gestión de cambios, incluyendo cambios estándar y de mantenimiento de emergencia, en los sistemas de Información e Infraestructura Tecnológica. Dicha política debe considerar, al menos, lo siguiente:

- 1) Procedimientos documentados de gestión de cambios de forma controlada que contemplen las etapas de solicitud, análisis de impacto, autorización, pruebas y aceptación final, para asegurar la aplicación adecuada de los cambios, con el fin de no comprometer la seguridad de la Infraestructura Tecnológica;
- 2) Creación de un registro de control de versiones, especificando cambios realizados, empleados involucrados, persona que autoriza los cambios, fechas de solicitud, realización, aprobación y componentes afectados;
- 3) Evaluaciones periódicas a la Infraestructura Tecnológica para identificar cambios no autorizados;
- 4) Gestión de los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura; y,
- 5) Procedimiento de vuelta atrás (*Rollback*), incluyendo Procedimientos y responsabilidades para abortar y recuperar los cambios sin éxito y de acontecimientos imprevistos.

Párrafo I. La gestión del cambio incluye los siguientes componentes: Hardware, equipo de comunicaciones y Software sistemas y de aplicación, así como toda la documentación y los Procedimientos asociados con la Infraestructura Tecnológica.

Párrafo II. Los participantes del mercado de valores deben realizar una evaluación de Riesgo de los cambios propuestos que contemple un análisis del impacto en el negocio y en otros componentes de la Infraestructura Tecnológica.

Párrafo III. Los participantes del mercado de valores deben aplicar pruebas de seguridad en entornos apropiados para verificar que los cambios realizados no provocan Vulnerabilidades ni fallos de rendimiento que pudieran comprometer la seguridad de la Infraestructura Tecnológica y que los mismos no comprometan los controles de Seguridad Cibernética y de la Información.

Artículo 25. Separación de ambientes. Los participantes del mercado de valores deben contar con entornos aislados para ejecutar las fases de desarrollo, pruebas y puesta en producción de sistemas de Información, aplicaciones del negocio y comunicaciones para reducir Riesgos de Acceso no autorizados o cambios en el ambiente de producción.

Artículo 26. Instalación de Software. Los participantes del mercado de valores deben definir e implementar Procedimientos, reglas y mecanismos para controlar que la instalación y actualización de Software y aplicaciones en los sistemas operativos, sea realizada por el personal autorizado para tales fines.

Párrafo. La instalación y actualización de Software y aplicaciones en los sistemas operativos solo podrán ser implementados luego de realizar pruebas adecuadas en un ambiente separado de producción. Las pruebas realizadas deben contemplar los aspectos siguientes:

- 1) Ensayo de rendimiento;
- 2) Carga de trabajo;
- 3) Seguridad;
- 4) Disponibilidad operativa;
- 5) Efectos sobre otros sistemas; y,
- 6) Copia de respaldo y de recuperación.

Artículo 27. Respaldos. Los participantes del mercado de valores deben contar con una política de gestión de copias de respaldos de seguridad de sistemas, aplicaciones, datos y documentación. Dicha política debe contemplar:

- 1) Ejecución de respaldos de Información y de Software exactas y completas, las cuales deben probarse regularmente acorde con la política de respaldo;

- 2) Procedimientos documentados para el resguardo y recuperación de la Información, cubriendo los requerimientos del negocio, métodos, herramientas y frecuencia de realización;
- 3) Registros o equivalentes que detallen la Información resguardada, la fecha y la hora, así como la fecha de expiración, el tipo de medio utilizado y su ubicación física;
- 4) Esquemas de etiquetado de copias de seguridad de los datos para su correcta identificación;
- 5) Controles para la prevención de la escritura accidental.

Párrafo I. Los participantes del mercado de valores deben contar con entornos locales seguros de Acceso restringido, procurando el almacenamiento de las copias de resguardo en formato físico con el nivel apropiado de protección ambiental y conforme a los métodos indicados por los fabricantes.

Párrafo II. Los respaldos de seguridad de sistemas, aplicaciones, datos y documentación deben probarse regularmente para asegurar que pueden ser confiables para el uso cuando sean necesarios. La prueba debe contemplar la capacidad para restaurar los datos de respaldo en medios dedicados a ensayos.

Párrafo III. Los participantes del mercado de valores deben contar con almacenamiento apartado, a una suficiente distancia para la salvaguarda de cualquier daño de un desastre en el sitio principal.

Párrafo IV. Los participantes del mercado de valores, cuya Infraestructura Tecnológica sea administrada por un proveedor de servicios, deben asegurarse que los sistemas, aplicaciones, datos y documentación se encuentran adecuadamente respaldados, según los lineamientos citados en este Reglamento y acorde a sus políticas y procedimientos.

Párrafo V. El resguardo de la Información Esencial deberá ser conservado de conformidad con el grado de utilidad de la misma para los fines de restauración. Dicha Información deberá ser cifrada. El tiempo de retención para la Información Esencial de Tipo Transaccional será de, por lo menos, un (1) año. Para la Información Esencial de Tipo Maestro, la entidad deberá resguardar en todo momento la más actualizada de las versiones disponibles de dicha Información.

Párrafo VI. Para las copias de resguardo de pistas de auditoría, el tiempo de retención será de por lo menos ciento ochenta (180) días.

Artículo 28. Configuración de los servidores. La configuración de los servidores físicos y virtuales debe realizarse con el objeto de evitar cambios o Accesos no autorizados, previniendo la interrupción de los servicios como resultado de una sobrecarga del sistema u otros factores. Al efecto, dichas configuraciones deben cumplir con lo siguiente:

- 1) Marco de configuraciones de línea base o de ajustes predeterminados para servidores físicos y virtuales, incluyendo el Hipervisor, así como lo siguiente:
 - a) Estandarización de las configuraciones del Firmware; y,
 - b) Estandarización y mantenimiento de las imágenes de instalación y configuración de los sistemas operativos, incluyendo parámetros adecuados de seguridad.
- 2) Restricción de Accesos para evitar uso de utilidades y de consolas de configuración de sistemas de la Información sin previa autorización;
- 3) Restricción de Accesos a un número limitado de usuarios con cuentas privilegiadas, asimismo, el Acceso al Sistema Básico de Entrada y Salida (BIOS, por sus siglas en inglés) de cada servidor debe estar protegido mediante contraseña u otro Mecanismo de Control de Acceso; e,
- 4) Inhabilitación de cuentas locales generadas por defecto por los sistemas operativos instalados en los servidores físicos y virtuales para proteger estos sistemas de algún Acceso no autorizado.

Párrafo. Los participantes del mercado de valores deben documentar los procesos para la configuración de los servidores físicos y virtuales mediante políticas y Procedimientos internos.

Artículo 29. Protección de Bases de Datos. Los participantes del mercado de valores deben definir e implementar Procedimientos para asegurar la Integridad y consistencia de toda la Información almacenada en formato electrónico, tales como Bases de Datos, almacenes de datos (*data warehouses*) y archivos de datos.

Párrafo. Las Bases de Datos gestionadas con aplicaciones de estaciones de trabajo deben ser protegidas mediante la validación de la entrada, la aplicación de controles de Acceso y la restricción a empleados autorizados a las funcionalidades de alto privilegio.

Artículo 30. Continuidad del negocio. Los participantes del mercado de valores deben establecer y mantener un plan logístico para permitir que el negocio y la Tecnología de la Información puedan responder a algún Incidente o a las interrupciones significativas de servicio de sus Procesos Críticos y

se mantenga la disponibilidad y Seguridad Cibernética y de la Información a un nivel aceptable para dicha entidad durante una crisis, desastres naturales, incendios o situaciones de fuerza mayor.

Párrafo. El plan debe ser diseñado de acuerdo con la naturaleza, tamaño, complejidad y perfil de Riesgos del negocio para garantizar su capacidad de operación, minimizar las pérdidas y asegurar la Seguridad Cibernética y de la Información ante una situación de emergencia en que se interrumpa el curso normal del negocio. La metodología y esquema del plan debe establecer, al menos, lo siguiente:

- 1) **Política de continuidad de negocio:** Este debe contener, como mínimo, los siguientes aspectos:
 - a) Roles y responsabilidades;
 - b) Recursos requeridos;
 - c) Requerimientos de entrenamiento;
 - d) Periodicidad de pruebas; y,
 - e) Periodicidad de mantenimiento.

- 2) **Análisis de Riesgo:** Consiste en identificar y evaluar los Riesgos que puedan afectar la operación de los procesos clave. De igual forma, identifica los desastres, Amenazas cibernéticas, eventos o accidentes que tienen una probabilidad de ocurrencia dentro de diferentes escenarios.

- 3) **Análisis de impacto del negocio:** Consiste en identificar funciones y Procesos Críticos del negocio con importancia estratégica y su clasificación según la criticidad, prioridades, impacto que su interrupción impondría y el tiempo de recuperación. Dicho análisis debe incluir, al menos, lo siguiente:
 - a) Análisis de las pérdidas potenciales asociadas con la disrupción de los Procesos Críticos del negocio, mediante el desarrollo de una evaluación de impacto al negocio (BIA, por sus siglas en inglés);
 - b) Análisis de Vulnerabilidad para el perfilado del tipo de Amenazas que son relevantes al participante del mercado de valores y su nivel de ocurrencia;
 - c) Preselección de planes adecuados para el tratamiento de los Riesgos identificados;
 - d) Escalas de tiempo aceptables para la recuperación de sistemas, aplicaciones y servicios;
 - e) Tiempo de interrupción máxima aceptable de sistemas, aplicaciones y servicios del participante del mercado de valores; y,

- f) Nivel de servicio mínimo que el participante del mercado de valores está dispuesto a aceptar tras la recuperación.
- 4) **Plan de recuperación de desastre (DRP, por sus siglas en inglés):** Se deben establecer y documentar planes de recuperación ante desastres para las operaciones tecnológicas que soportan los Procesos Críticos del negocio y garantizar la disponibilidad de los mismos cuando sea necesario.
 - 5) **Plan de Incidentes Cibernéticos y de la Información:** Se deben definir Procedimientos y mecanismos para mitigar y corregir ataques cibernéticos o ciberataque dirigidos.
 - 6) **Gestión de crisis:** se debe establecer un proceso de gestión de crisis con el soporte de una unidad de apoyo que detalle las acciones que se deben tomar en caso de la ocurrencia de un Incidente de Seguridad Cibernética y de la Información que afecten significativamente las operaciones normales del negocio.
 - 7) **Plan de Contingencia:** Se deben definir múltiples Planes de Contingencia desarrollados y desplegados para cada entorno del negocio para asegurar la continuidad de las operaciones para cada tipo de emergencia a enfrentar.
 - 8) **Retorno a la normalidad:** Proceso documentado para la vuelta a la normalidad una vez el Incidente haya sido superado, manteniendo los controles de Seguridad Cibernética y de la Información.
 - 9) **Recursos alternos:** Se deben definir y documentar los recursos necesarios para soportar los Procedimientos de continuidad y recuperación, considerando personas, instalaciones, Infraestructura Tecnológica y controles de Seguridad Cibernética y de la Información.

Párrafo. Los planes deben ser aprobados por el consejo de administración y revisados regularmente por la alta gerencia con el objeto de asegurar la viabilidad, efectividad y eficacia operativa de los mismos.

Artículo 31. Pruebas del Plan de Continuidad de Negocio. Los participantes del mercado de valores deben ejecutar pruebas al Plan de Continuidad de Negocio en períodos no mayores a un (1) año para confirmar la eficacia, eficiencia del plan y validar el desempeño coherente de las medidas de continuidad de Seguridad Cibernética y de la Información y realizar los ajustes pertinentes. Debe existir un registro o constancia de la calidad y los resultados de las mismas.

Artículo 32. Registros y Monitoreo Continuo. Los participantes del mercado de valores deben contar con una política para mantener y revisar regularmente los registros de eventos de las actividades realizadas por los usuarios en los sistemas infraestructura, aplicaciones, páginas web y Bases de Datos. De igual forma, deben contar con una política de las excepciones, fallas, y eventos de Seguridad Cibernética y de la Información, con el fin de facilitar las investigaciones futuras y el Monitoreo Continuo de los Controles de Acceso. Los registros de eventos deben contemplar, al menos, lo siguiente:

- 1) Identificación del usuario;
- 2) Actividades del sistema;
- 3) Fechas, horas y detalles de los eventos clave;
- 4) Identificación o ubicación del dispositivo, si es posible, y el identificador del sistema o los intentos de Acceso a los datos y otros recursos;
- 5) Registros de intentos de Acceso al sistema;
- 6) Cambios en la configuración del sistema;
- 7) Uso de privilegios;
- 8) Uso de utilidades y aplicaciones del sistema;
- 9) Archivos accedidos y tipo de Acceso;
- 10) Direcciones IP, origen, destino y protocolos de red;
- 11) Activación y desactivación de los sistemas de protección;
- 12) Procedimientos para identificar eventos falsos menores y eventos significativos; y,
- 13) Otros registros de eventos que la entidad considere relevantes conforme a su matriz de Riesgos.

Párrafo I. Las informaciones referidas en este artículo deben ser conservadas a través de los medios electrónicos definidos por la entidad por un período que, en ningún caso, será inferior a cinco (5) años.

Párrafo II. Estos registros deben ser protegidos contra modificación no autorizada y analizados de manera regular.

Artículo 33. Gestión de Problemas e Incidentes. Los participantes del mercado de valores deben establecer las responsabilidades e implementar los Procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a todo Problema o Incidente de Seguridad Cibernética y de la Información, incluyendo:

- 1) Establecimiento de un marco de gestión de Problemas o Incidentes de Seguridad Cibernética y de la Información contemplando lo siguiente:

- a) Definición de roles y responsabilidades del equipo de gestión para garantizar una respuesta rápida, eficaz, y ordenada;
 - b) Definición de tipo de Información necesaria para la gestión Problemas o Incidentes;
 - c) Uso de herramientas necesarias para asistir en el proceso de gestión de Problemas o Incidentes; y,
 - d) Datos sobre Problemas o Incidentes a ser documentados, incluyendo la Información de contacto, entorno de negocios afectados, aspectos técnicos como diagramas de red, configuraciones de sistemas, conexiones a redes externas e Información de inteligencia de la Amenaza.
- 2) Establecimiento de un Procedimiento para la gestión de Problemas e Incidentes de Seguridad Cibernética y de la Información que cubra las fases de identificación, respuesta, recuperación y seguimiento conforme al Marco de Trabajo, así como el mecanismo para su identificación, registro, categorización y clasificación. El tiempo de retención de los registros no podrá ser menor a cinco (5) años;
- 3) Implementación de sistemas especializados que contemplen herramientas para:
- a) Gestión, análisis y correlación de eventos de seguridad;
 - b) Investigación;
 - c) Restauración de registros históricos; y,
 - d) Manejo de evidencias e investigaciones forenses.
- 4) Establecimiento y documentación de Procedimientos para el análisis y revisión de la Información sobre Problemas e Incidentes de seguridad para:
- a) Determinar patrones y tendencias;
 - b) Determinar los costos tangibles e intangibles asociados;
 - c) Evaluar las implicaciones operacionales;
 - d) Determinar la efectividad de los controles; y,
 - e) Realizar comparaciones de los Problemas e Incidentes internos con reportes externos similares.

Artículo 34. Gestión de parches. Los participantes del mercado de valores deben gestionar e instalar de parches seguridad para proteger los sistemas de Información y la infraestructura de tecnología de la Información, así como mantener el conocimiento actualizado de los parches

disponibles. La gestión e implementación de parches debe considerar los aspectos del artículo 24 (Gestión de cambio) del presente Reglamento.

Párrafo. Los participantes del mercado de valores deben contar con políticas y Procedimientos para la gestión e instalación de los parches seguridad.

Artículo 35. Monitoreo Continuo. Los participantes del mercado de valores deben contar con una política para gestionar, mantener y revisar regularmente el rendimiento, sobrecargas y las capacidades de los servicios, sistemas y la Infraestructura Tecnológica.

Artículo 36. Prevención y detección de intrusos. Los participantes del mercado de valores deben implementar soluciones tecnológicas o mecanismos de prevención y detección de intrusos, a fin de proteger los sistemas y la Infraestructura Tecnológica. Estos deben cubrir, como mínimo, los siguientes aspectos:

- 1) Infraestructura Tecnológica;
- 2) Definición de mecanismos de prevención de intrusos los cuales deben identificar:
 - a) Características y patrones de ataques conocidos;
 - b) Comportamiento inusual de los sistemas;
 - c) Acceso no autorizado a los sistemas de Información; y,
 - d) Configuraciones base que contemplen actualizaciones de las Bases de Datos para incorporar cualquier nueva Amenaza o forma de ataque, envío de alertas cuando surja una actividad sospechosa o inusual y la protección contra ataques dirigidos.
- 3) Elaboración de análisis de las posibles intrusiones para determinar el impacto de los mismos en la entidad, incluyendo lo siguiente:
 - a) Determinación de ocurrencia de ataque para descartar los falsos positivos;
 - b) Determinación de tipo de ataque y trazabilidad del mismo;
 - c) Identificación de vectores de ataque; y,
 - d) Cuantificación del posible impacto del ataque.

Artículo 37. Protección de Software malicioso. Los participantes del mercado de valores deben contar con políticas, Procedimientos y mecanismos para la detección, prevención, y recuperación para proteger de Software malicioso a los sistemas e Infraestructura Tecnológica, así como Procedimientos y capacitación continua y adecuada para concientizar a los usuarios sobre el Software malicioso.

Párrafo I. Al efecto, los participantes del mercado de valores deben instalar y desplegar sistemas para la protección contra Software malicioso en todos los dispositivos que formen parte de la Infraestructura Tecnológica de la entidad.

Párrafo II. De igual forma, los participantes del mercado de valores deben definir la configuración de una línea base para los sistemas de protección contra Software malicioso que contemple políticas para la protección en tiempo real, la programación de escaneos en escalas de tiempo definidas, la notificación de potenciales infecciones, la inhabilitación y cuarentena de archivos infectados, la remoción de cualquier Software malicioso y archivos infectados asociados al mismo.

Párrafo III. los participantes del mercado de valores deben realizar análisis y escaneos periódicos a los componentes de la Infraestructura Tecnológica.

CAPÍTULO V

Seguridad de las Comunicaciones

Artículo 38. Gestión de la red. Los participantes del mercado de valores deben implementar los controles para garantizar la seguridad y protección de la Información en los componentes de redes y la protección de los servicios conectados e Información en tránsito. Por lo cual, deben establecer:

- 1) **Configuración de dispositivos de la red:** Los dispositivos de red deben ser configurados para funcionar de acuerdo con su rol y con los controles de seguridad que eviten cambios no autorizados o incorrectos;
- 2) **Gestión de la red física:** Las redes deben ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales, los puntos de Acceso a la red deben estar protegidos por Mecanismos de Control de Acceso, tales como, la documentación de la arquitectura de red e Integridad.
- 3) **Conexiones de redes externas:** Las conexiones de redes externas a los sistemas y redes informáticas deben ser identificadas, verificadas, registradas y aprobadas individualmente por el personal designado o comité funcional de Seguridad Cibernética y de la Información, para lo cual deben establecer:
 - a) Procedimientos para la gestión de las conexiones con redes externas que contemplen la identificación individual de cada conexión externa a otros sistemas y redes, mecanismos de Acceso a dispositivos autorizados, documentación de conexiones externas y remoción de conexiones innecesarias;

- b) Mecanismos de protección que contemplen la restricción de las conexiones a los puntos de entrada definidos, verificación de la fuente de las conexiones externas y registro de las mismas, así como registro de potenciales violaciones a la política de seguridad interna; y,
- c) Aislamiento de dispositivos desconocidos o inseguros en un segmento de cuarentena para los fines de configuración y actualización de los mismos.

4) **Tráfico de datos a través de los *firewalls* (cortafuegos):**

- a) La configuración del filtrado de tráfico debe utilizar reglas predefinidas tomando en cuenta los principios del menor privilegio, por defecto, y revisada periódicamente;
- b) Los *firewalls* (cortafuegos) deben contar con reglas de protección y protocolos de comunicación propensos a abusos por ataques;
- c) Bloqueo de paquetes maliciosos;
- d) Bloqueo del tráfico entrante o saliente a direcciones comprometidas; y,
- e) Pruebas de funcionamiento y efectividad de reglas, previo a su aplicación.

5) **Acceso y mantenimiento remoto:**

- a) Establecer responsabilidades y Procedimientos para la gestión de los activos de Tecnologías y de Información remotos;
- b) Establecer Procedimientos para la gestión de Acceso remoto que contemplen las etapas de solicitud, autorización y registro;
- c) Identificar los usuarios que dispondrán de servicio de remoto;
- d) Implementar mecanismos de conexión segura con Encriptación de datos, autenticación e identificación para el Acceso remoto de los usuarios;
- e) Establecer Procedimientos para la gestión de mantenimiento remoto de sistemas críticos por terceros autorizados, contemplando la definición de objetivos y alcance del mantenimiento planificado, controles para el registro de Acceso individualizado por cada tercero, mecanismos de autorización de Acceso a los sistemas mediante credenciales únicas especializadas y su revocación tras la finalización del mantenimiento;
- f) Elaborar un análisis independiente de las labores de mantenimiento remoto;
- g) Supervisar los mantenimientos remotos durante su realización. Una vez terminadas las sesiones de mantenimiento, las sesiones de conexión deben finalizar automáticamente;
- h) Definir los controles para aplicaciones de gestión de mantenimiento remoto, contemplando aspectos de gestión de Acceso, análisis de origen y destino de conexiones,

así como el Monitoreo Continuo de las actividades realizadas en cada sesión y la inhabilitación de la conexión tras la conclusión del mantenimiento.

6) **Acceso a redes inalámbricas:** Elaboración de Procedimientos documentados para la gestión de redes inalámbricas, contemplando los siguientes aspectos:

- a) Ubicación segura y configuración de Acceso inalámbrico;
- b) Mecanismos de restricción de Acceso a usuarios no autorizados;
- c) Cifrado de conexiones entre dispositivos previamente registrados, utilizando algoritmos;
- d) Inventario de puntos de Acceso a la red;
- e) Mecanismos de detección de usuarios y dispositivos no autorizados;
- f) Uso de identificadores de servicios (SSID, por sus siglas en inglés) ocultos en redes privadas para evitar revelar Información importante de la red inalámbrica;
- g) Aplicación de múltiples capas de protección para la red, tales como, listas de Control de Acceso, autenticación de dispositivos y de usuarios;
- h) Uso de mecanismos para el filtrado de seguridad para prevenir el Acceso no autorizado a la red;
- i) Establecimiento de redes inalámbricas segregadas de la red principal para uso del personal externo tales como: visitantes, suplidores y empleados que deseen conectarse con sus dispositivos personales. Estas redes deben estar localizadas en segmentos exclusivos de la red, monitoreadas y protegidas por *firewalls* (cortafuegos);
- j) Redes de voz sobre IP (VoIP, por sus siglas en inglés); y,
- k) Controles de seguridad y monitoreo contemplando el registro de intentos de Acceso, restricción y filtrado del tráfico, así como mecanismos de redundancia.

7) **Telefonía y Conferencia:**

- a) Procedimientos documentados para la gestión y uso de servicios de telefonía y conferencia, así como la administración de su infraestructura subyacente;
- b) Controles generales de red, tales como, el despliegue de herramientas de monitoreo, instalación de componentes para el aseguramiento de resiliencia y redundancia de la red de telefonía, instalación de *firewalls* (cortafuegos) con capacidad de filtrado de tráfico de voz y bloqueo de terminales no autorizadas;
- c) Controles especializados para la infraestructura de telefonía, tales como, la separación del tráfico de voz, aplicación de configuraciones de seguridad a teléfonos, enrutadores,

centrales PBX, cifrado de dispositivos, conexiones, escaneo de Vulnerabilidades y el registro y Monitoreo Continuo de eventos;

- d) Protección de los sistemas de buzones de voz contra el Acceso no autorizado a través de mecanismos de autenticación;
- e) Documentación de cambios realizados a las configuraciones de los servicios de telefonía y conferencia, tales como, cambios de extensiones, restablecimiento de contraseñas de buzones y redireccionamiento de llamadas; y,
- f) Despliegue de sistemas de telecomunicaciones alternos para asegurar la continuidad de las operaciones del negocio del participante del mercado de valores dentro de un período razonable de tiempo de acuerdo al Plan de Contingencia.

Artículo 39. Dispositivos Móviles. Los participantes del mercado de valores deben establecer mecanismos de seguridad para proteger la Información intercambiada a través de los Dispositivos Móviles utilizados por los empleados, incluyendo:

- 1) Gestión y autorización de los Accesos desde entornos remotos;
- 2) Gestión centralizada de los Dispositivos Móviles;
- 3) Protección de la Información: Los Dispositivos Móviles deben ser protegidos contra la divulgación no autorizada de Información, pérdida o hurto, mediante Control de Acceso y cifrado;
- 4) Conectividad segura de los Dispositivos Móviles;
- 5) Dispositivos portátiles de almacenamiento: El uso de dispositivos portátiles de almacenamiento debe ser objeto de aprobación con Acceso restringido. El almacenamiento de Información en este tipo de dispositivos debe ser cifrada.

Artículo 40. Comunicaciones electrónicas. Los participantes del mercado de valores deben asegurar las comunicaciones electrónicas, mediante controles y políticas de Seguridad Cibernética y de la Información, incluyendo:

- 1) **Correos electrónicos:** Los sistemas de correos electrónicos de los participantes del mercado de valores deben estar protegidos por una combinación de procesos, concienciación y controles técnicos de Seguridad Cibernética y de la Información que contemplen lo siguiente:
 - a) Definición de política interna de correo electrónico, la cual debe contemplar Procedimientos para la configuración de buzones, escaneo de mensajes de correo para la detección y bloqueo de cualquier Amenaza de seguridad, uso de firma digital,

términos y condiciones de uso y Monitoreo Continuo de actividad, así como la revisión de capacidades y requerimientos para su continuo funcionamiento;

- b) Establecimiento de controles de seguridad para la prevención de la divulgación accidental de mensajes a través del cifrado, inhabilitación de funcionalidades de autoenvío, prohibición del uso de grandes listas de distribución y la presentación de advertencias a los usuarios previo al envío de correo a grandes grupos de destinatarios; y,
 - c) Establecimiento de controles de seguridad para el bloqueo de mensajes no deseados, mecanismos de no repudiación del origen y recepción de mensajes, así como de validación de direcciones IP.
- 2) **Mensajería instantánea:** Los servicios de mensajería instantánea deben ser protegidos mediante el establecimiento de un proceso de gestión que contemple las etapas de solicitud, autorización, implementación de los controles y la configuración de los elementos de Seguridad Cibernética y de la Información; y,
- 3) **Servicios de comunicación de voz:** Los servicios de comunicación de voz deben ser aprobados y protegidos por una combinación de controles tecnológicos, los cuales deben monitorearse regularmente y estar respaldados por restricciones en el Acceso.

Artículo 41. Gestión de proveedores externos. Los participantes del mercado de valores que contraigan obligaciones contractuales con proveedores externos de productos o servicios tecnológicos, deben asegurar la integración de los requerimientos de Seguridad Cibernética y de la Información, conforme a los aspectos siguientes:

- 1) Tercerización: Establecer un proceso para regir la selección y gestión de los proveedores externos, apoyado en contratos que especifiquen los requisitos de Seguridad Cibernética y de la Información; y,
- 2) Requisitos de seguridad a los proveedores externos: El cumplimiento de los requisitos de Seguridad Cibernética y de la Información debe revisarse de manera periódica durante la relación con los proveedores externos, contemplando el análisis y la gestión adecuada de los Riesgos.

Párrafo. En los casos que los servicios provistos consideren Información financiera u otro tipo de Información sensible, los participantes del mercado de valores deben solicitar a la entidad proveedora una evaluación enfocada en los Riesgos de Integridad, disponibilidad y Confidencialidad. Dicha evaluación debe ser realizada por un tercero independiente utilizando modelos de reportes de Riesgo y controles en la provisión de servicio (Tal como: SOC 2, etc., u otras que puedan aplicar conforme a la naturaleza del servicio contratado).

Artículo 42. Contratación de servicios de computación en la nube. Los participantes del mercado de valores deben documentar una política para el uso y contratación de servicios de computación en la nube, incluyendo el hospedaje de servicios web, que contemple el desarrollo de un análisis de los Riesgos de Seguridad Cibernética y de la Información de los servicios contratados, para determinar el uso de los mismos por parte de los empleados, la Integridad de la Información almacenada y sus mecanismos de protección. Esta política debe ser comunicada a todos los empleados que puedan hacer uso de los mismos.

CAPÍTULO VI

Desarrollo y Mantenimiento de los Sistemas de Información

Artículo 43. Desarrollo de sistemas subcontratados. Los participantes de mercado de valores que mantengan en su estructura orgánica un área de desarrollo de sistemas, deben establecer un proceso de gestión de desarrollo de sistemas que contemple:

- 1) Metodología de Desarrollo de Sistemas: Las actividades de desarrollo de sistemas deben llevarse a cabo de acuerdo con una metodología de desarrollo documentada y apegada al Marco de Trabajo;
- 2) Entorno de Desarrollo de Sistemas: Las actividades de desarrollo de sistemas se deben realizar en los entornos de desarrollo especializados, los cuales deben estar separados de los ambientes de producción y preproducción, y protegidos contra Accesos no autorizados. Los datos de entornos productivos no deben ser utilizada o almacenada en los entornos de desarrollo. Deben establecerse mecanismos para asegurar la privacidad y protección de los datos de carácter personal en los ambientes de preproducción (aseguramiento de la calidad) y producción;
- 3) Aseguramiento de la Calidad: El desarrollo de los sistemas debe realizarse siguiendo normas y pruebas de calidad que procuren que los controles y requisitos de Seguridad Cibernética y de la Información acordados sean implementados durante el ciclo de desarrollo del mismo.

Artículo 44. Entornos de desarrollo de sistemas. Los datos de entornos productivos no deben ser utilizados ni almacenados en los entornos de desarrollo. Deben establecerse mecanismos para asegurar

la privacidad y protección de los datos de carácter personal en los ambientes de preproducción (aseguramiento de la calidad) y producción.

Artículo 45. Interfaces programables de aplicaciones (API, por sus siglas en inglés). Los sistemas y aplicaciones que permitan la extensibilidad de funciones a través de interfaces de aplicaciones programables, deben contar con controles de Seguridad Cibernética y de la Información que regulen la interacción con otros sistemas y aplicaciones, tanto internos como de terceros. Del mismo modo, las aplicaciones desarrolladas que interactúen con estas interfaces de aplicaciones programables deben cumplir con los requerimientos de seguridad establecidos por los participantes del mercado de valores.

Artículo 46. Información a la Superintendencia. Los participantes del mercado de valores deben informar formalmente a la Superintendencia del Mercado de Valores (en lo adelante, la “Superintendencia”), a más tardar el día hábil siguiente, sobre la ocurrencia y las acciones tomadas para corregir los siguientes eventos:

- 1) La activación del Plan de Contingencia o estrategias de recuperación de las operaciones del negocio;
- 2) La interrupción en el funcionamiento normal de los sistemas operativos y Software aplicativos principales que afecten la prestación de servicios a los clientes;
- 3) La toma de decisión formal de realizar cambios en la plataforma central de operaciones y sistemas computarizados;
- 4) La ocurrencia de Incidentes de seguridad relacionados con la realización exitosa de ataques externos o penetración a los sistemas de la entidad a través de los servicios de red y comunicaciones, previamente reportados al SPRICS;
- 5) La toma de decisión formal de implementar o cambiar la plataforma tecnológica utilizada para proporcionar servicios financieros por medios electrónicos; y,
- 6) Cualquier evento que provoque cambios no programados en la Infraestructura Tecnológica de la Información.

CAPÍTULO VII

Gestión y Control de Vulnerabilidades

Artículo 47. Criptografía. Los participantes del mercado de valores deben establecer políticas y Procedimientos sobre la gestión y empleo de controles criptográficos para asegurar la Integridad, disponibilidad, Confidencialidad, autenticidad y no repudio de la Información, los cuales deben incluir:

- 1) La administración de las soluciones criptográficas, contemplando la selección de herramientas y soluciones de cifrado, la gestión de solicitudes, aprobaciones y gestión de actualizaciones de soluciones y algoritmos de cifrado;
- 2) Mantenimiento de un registro de soluciones criptográficas aprobadas, contemplando lo siguiente:
 - a) Especificación de la intención del uso de cifrado;
 - b) Información sobre los usuarios autorizados a utilizar las mismas;
 - c) Detalles de los entornos locales donde se aplica la solución; y,
 - d) Requerimientos de licenciamiento de la solución.
- 3) Análisis de Riesgos asociados al uso de soluciones criptográficas, incluyendo los algoritmos de Encriptación;
- 4) Uso, protección y duración de las claves criptográficas en todo su ciclo de vida;
- 5) Mecanismos para la distribución segura, almacenamiento, respaldo, recuperación, reemplazo y actualización de llaves criptográficas;
- 6) La forma de designación de los custodios de llaves criptográficas, incluyendo la sensibilización a usuarios sobre sus deberes y responsabilidades; y,
- 7) Forma de revocación de llaves criptográficas en caso de que alguna llave haya sido comprometida o por modificación del custodio de llave criptográfica.

Artículo 48. Gestión de las Vulnerabilidades. Los participantes del mercado de valores deben contar con políticas, Procedimientos y mecanismos para identificar y evaluar de forma continua las Vulnerabilidades en su infraestructura, aplicaciones, páginas web y Bases de Datos que permitan determinar el tipo de Amenaza, impacto potencial y mejor curso de acción para hacer frente a cada Vulnerabilidad.

Párrafo. Sobre las pruebas de penetración, las mismas deben llevarse a cabo por lo menos una vez al año, con el objetivo de identificar nuevas Vulnerabilidades utilizando técnicas avanzadas y garantizando que las Vulnerabilidades identificadas previamente han sido corregidas correctamente.

Artículo 49. Sincronización de reloj de sistemas e Infraestructura Tecnológica. Los sistemas de procesamiento de Información relevantes o de dominio de seguridad de los participantes del mercado de valores debe estar sincronizados para asegurar la exactitud de los registros de auditoría, los cuales podrán requerirse para investigaciones o como pruebas en acciones legales o disciplinarias. Al efecto, se deben establecer las políticas y Procedimientos internos.

Artículo 50. Registros y monitoreo de los usuarios administradores. Los participantes del mercado de valores deben contar con políticas, Procedimientos y mecanismos para proteger, revisar y registrar las actividades realizadas por los usuarios privilegiados de los sistemas e Infraestructura Tecnológica. Las revisiones deben realizarse por lo menos cinco (5) veces al año.

Artículo 51. Ciclo de vida del desarrollo de sistemas y aplicaciones. Los participantes del mercado de valores que mantengan en su estructura orgánica un área de desarrollo de sistemas, deben adoptar un ciclo de vida para el desarrollo seguro de sus sistemas y aplicaciones, tanto internas como tercerizadas, de acuerdo a las disposiciones siguientes:

- 1) **Especificaciones de los requerimientos:** Los requerimientos del negocio, incluidos los de Seguridad Cibernética y de la Información, deben ser contemplados durante la fase de especificación de requerimientos;
- 2) **Diseño de sistemas y aplicaciones:** Los requisitos de Seguridad Cibernética y de la Información para los sistemas que se encuentran en el ciclo de desarrollo deben ser considerados en el diseño de dichos sistemas y aplicaciones, a fin de minimizar las Vulnerabilidades;
- 3) **Dispositivos Personales:** El Acceso a la red a través de Dispositivos Móviles propiedad de los empleados, debe contar con la debida autorización y la implementación de controles técnicos que contemplen los requerimientos de Seguridad Cibernética y de la Información;
- 4) **Compilación de sistemas y aplicaciones:** Las actividades de compilación de los sistemas y aplicaciones, incluyendo la codificación y personalización de paquetes, deben llevarse a cabo de conformidad con el Marco de Trabajo de la industria, realizadas por el personal especializado en el desarrollo de sistemas y aplicaciones. Las actividades de compilación deben ser inspeccionadas para identificar modificaciones o cambios no autorizados;
- 5) **Prueba de sistemas y aplicaciones:** Los sistemas y aplicaciones en desarrollo deben ser probados en una zona dedicada de pruebas que simule el entorno de producción, con la debida

atención a los datos de carácter personal utilizada, antes de que el sistema o aplicación sea colocado en el ambiente de producción;

- 6) **Pruebas de seguridad:** Los sistemas y aplicaciones en desarrollo deben ser sometidos a pruebas de Seguridad Cibernética y de la Información en las fases requeridas dentro del ciclo de desarrollo, utilizando herramientas para la detección de Vulnerabilidades, pruebas de penetración y pruebas de Control de Acceso, previo a su colocación en los ambientes de producción;
- 7) **Proceso de instalación:** Los nuevos sistemas y aplicaciones se deben instalar en el entorno de producción, de acuerdo con un proceso documentado que contemple los requerimientos de Seguridad Cibernética y de la Información; y,
- 8) **Revisiones luego de las implementaciones:** Luego de la implementación, se deben realizar revisiones periódicas de acuerdo con procesos documentados, incluyendo la cobertura de la Seguridad Cibernética y de la Información.

TÍTULO III

DISPOSICIONES SOBRE EL GOBIERNO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN

CAPÍTULO I

Órganos de Gestión

Artículo 52. Gobierno de Seguridad Cibernética y de la Información. Los participantes del mercado de valores deben contar con un adecuado Gobierno de Seguridad Cibernética y de la Información, el cual se constituye como parte integral del programa de gobierno empresarial-corporativo que brinda dirección estratégica para garantizar que se logren los objetivos del negocio y determina que el Riesgo tecnológico se administre de forma apropiada y que los recursos se utilicen con responsabilidad.

Artículo 53. Responsabilidad del consejo de administración. El consejo de administración será responsable del cumplimiento de los principios y lineamientos básicos en materia de Seguridad Cibernética y de la Información. En tal virtud, el consejo debe cumplir con las responsabilidades que se detallan a continuación:

- 1) Establecer y velar por la existencia de un Gobierno de Seguridad Cibernética y de la Información;
- 2) Evaluar y aprobar un sistema de gestión de la Seguridad Cibernética y de la Información que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la Información, tecnología y procesos de negocios que estén alineados con los requerimientos de negocio y la gestión de seguridad del participante del mercado de valores;
- 3) Cumplir con el sistema de gestión de la Seguridad Cibernética y de la Información;
- 4) Aprobar el programa de Seguridad Cibernética y de la Información, incluyendo los objetivos, lineamientos y políticas en materia de tecnología, Seguridad Cibernética y de la Información y sus Riesgos, así como velar por su cumplimiento;
- 5) Proveer los recursos necesarios para lograr el cumplimiento de las políticas y lineamientos en materia de Seguridad Cibernética y de la Información y de las disposiciones contenidas en este Reglamento;
- 6) Evaluar y aprobar las decisiones relativas a tecnología de la Información y velar que se han adoptado en línea con las estrategias y objetivos del participante del mercado de valores, garantizando la supervisión de los procesos de manera efectiva y transparente, el cumplimiento de los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del consejo de administración;
- 7) Velar para que los Riesgos relacionados con Tecnología de la Información no excedan la tolerancia de Riesgo de la entidad;
- 8) Evaluar que las adecuadas y suficientes capacidades relacionadas con la seguridad de Tecnología de la Información estén disponibles para soportar eficazmente los objetivos del participante del mercado de valores;
- 9) Velar por el cumplimiento en la implementación de sistemas de Información propios, adquiridos o subcontratados, con la normativa vigente aplicable;
- 10) Adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o Acceso no autorizado;

- 11) Evaluar, aprobar y poner en funcionamiento el Plan de Continuidad de Negocios, Plan de Contingencia y programas de pruebas de estrés, como parte de su proceso de gestión integral de Riesgo;
- 12) Asegurar que exista un sistema adecuado de delegación de responsabilidades y segregación de funciones en la entidad; y,
- 13) Asignar y verificar el cumplimiento de las funciones y responsabilidades de Seguridad Cibernética y de la Información para los roles definidos en el área correspondiente.

Artículo 54. Comité funcional de Seguridad Cibernética y de la Información. Los participantes del mercado de valores deben establecer un comité funcional de Seguridad Cibernética y de la Información, cuyas responsabilidades se detallan a continuación:

- 1) Diseñar los lineamientos para la Seguridad Cibernética y de la Información y el mantenimiento del Programa de Seguridad Cibernética y de la Información, en consonancia con los objetivos estratégicos de la entidad, determinados por el consejo de administración;
- 2) Someter al consejo de administración para su aprobación, las políticas del programa de Seguridad Cibernética y de la Información;
- 3) Evaluar la efectividad del programa de Seguridad Cibernética y de la Información, en consonancia con los objetivos estratégicos de la entidad;
- 4) Aprobar las conexiones de redes externas a los sistemas y redes informáticas identificadas por el área a cargo de la Seguridad Cibernética y de la Información;
- 5) Ratificar las decisiones de tratamiento de Riesgo en coordinación con las áreas pertinentes de negocios, previamente presentados por el oficial de Seguridad Cibernética y de la Información; y,
- 6) Comunicar al consejo de administración los resultados de las valoraciones sobre los aspectos de Seguridad Cibernética y de la Información.

Párrafo I. El comité funcional de Seguridad Cibernética y de la Información estará integrado por un número impar, como mínimo, de tres (3) miembros con voz y voto:

- a) Un miembro del consejo de administración que no ocupe cargos ejecutivos en el participante del mercado de valores, quien lo presidirá;

- b) El ejecutivo principal del participante del mercado de valores; y,
- c) El oficial de seguridad cibernética y la Información, quien fungirá como secretario.

Párrafo II. Podrán asistir a las reuniones del comité en calidad de invitados con voz, pero sin voto, el personal u otros ejecutivos de la sociedad que los miembros del comité consideren necesarios para la presentación y sustentación de los temas que se deban tratar en la respectiva sesión, lo cual se hará constar en el acta levantada de la reunión.

Párrafo III. Los sujetos obligados deben remitir la integración del comité a la Superintendencia en un plazo de quince (15) días hábiles, contados a partir de su designación. De igual forma, cualquier modificación en la composición del comité debe ser comunicada a la Superintendencia, a más tardar, cinco (5) días hábiles luego del hecho.

Párrafo IV. La Superintendencia vía norma técnica u operativa establecerá las disposiciones relativas a los Comité funcional de Seguridad Cibernética y de la Información

CAPÍTULO II

Estructura Gerencial

Artículo 55. Estructura gerencial y funciones de control de Seguridad Cibernética y de la Información. Los participantes del mercado de valores deben contar con una estructura gerencial para el control de Seguridad Cibernética y de la Información, acordes a su naturaleza, tamaño, y complejidad. El programa establecido en el marco de las responsabilidades definidas en este Reglamento será dirigido por la unidad funcional de Seguridad Cibernética y de la Información, la cual estará a cargo del oficial de Seguridad Cibernética y la Información y reportará directamente al consejo de administración.

Artículo 56. Oficial de Seguridad Cibernética y de la Información. El oficial de Seguridad Cibernética y de la Información debe contar con la competencia y capacidad requerida para sus funciones. Según la estructura de cada participante del mercado de valores, el oficial de Seguridad Cibernética y la Información, debe tener suficiente autoridad e independencia para cumplir con sus responsabilidades.

Artículo 57. Responsabilidades del oficial de Seguridad Cibernética y de la Información. El oficial de Seguridad Cibernética y de la Información debe cumplir, al menos, con las responsabilidades siguientes:

- 1) Desarrollar, implementar y mantener actualizado el programa de Seguridad Cibernética y de la Información, el cual debe ser revisado y actualizado una vez al año;
- 2) Presentar informes periódicos o, al menos, un informe anual al consejo de administración sobre el contenido, aplicabilidad y actualización de las políticas establecidas en materia de Seguridad Cibernética y de la Información;
- 3) Implementar políticas, estándares y Procedimientos apropiados para apoyar el programa de Seguridad Cibernética y de la Información;
- 4) Asignar las responsabilidades de los miembros que conforman las áreas especializadas;
- 5) Gestionar las acciones para el tratamiento del Riesgo tecnológico en coordinación con las áreas pertinentes del negocio;
- 6) Cumplir con los límites de los niveles de Riesgos relevantes establecidos por el consejo de administración, relacionados con Amenazas o Incidentes de Seguridad Cibernética y de la Información;
- 7) Monitorear permanentemente el estado de estado de la Seguridad Cibernética y de la Información y rendir informes periódicos según la necesidad sobre los hallazgos y Riesgos identificados al comité funcional de Seguridad Cibernética y de la Información;
- 8) Cumplir con las atribuciones asignadas y decisiones tomadas por el consejo de administración; y,
- 9) Definir y evaluar las responsabilidades de los proveedores de servicios en lo concerniente a la Seguridad Cibernética y de la Información.

CAPÍTULO III

Monitoreo Interno

Artículo 58. Autoevaluación. Los participantes del mercado de valores deben autoevaluar su cumplimiento normativo en materia de Seguridad Cibernética y de la Información con periodicidad anual. Los resultados de dicha evaluación, así como los de la evaluación del nivel de exposición en esta materia deben presentarse anualmente al consejo de administración.

Párrafo. Las evaluaciones deben contemplar los eventos que involucren la divulgación no autorizada de Información, la corrupción accidental o deliberada, la manipulación de la Información y la disponibilidad de los entornos en cualquier período.

Artículo 59. Auditoría interna. Los participantes del mercado de valores deben establecer procesos de auditorías internas para garantizar la supervisión efectiva del programa de Seguridad Cibernética y de la Información y del estado de la Seguridad Cibernética y de la Información en sus sistemas de Información y de la Infraestructura Tecnológica. El resultado de las auditorías internas debe contener la documentación y notificación a las partes interesadas de sus conclusiones y recomendaciones.

Artículo 60. Evaluación de un tercero independiente. Los participantes del mercado de valores deben realizar evaluaciones independientes sobre el cumplimiento normativo en materia de Seguridad Cibernética y de la Información, con una periodicidad no mayor de tres (3) años.

Párrafo I. La evaluación inicial se llevará a cabo dentro de los tres (3) años contados a partir de la entrada en vigencia de este Reglamento.

Párrafo II. La entidad debe contar por lo menos con cinco (5) años de experiencia y con las calificaciones e independencia necesaria para realizar la evaluación.

Párrafo III. Los participantes del mercado de valores deben presentar las auditorías realizadas por auditores externos inscritos en el Registro al consejo de administración, cada vez que se realicen por parte del comité de auditoría.

TÍTULO IV DISPOSICIONES FINALES

Artículo 61. Normativa complementaria. El superintendente del Mercado de Valores, mediante normas técnicas u operativas, emitirá el contenido y otros requisitos aplicables para la elaboración, implementación y manejo del programa de Seguridad Cibernética y de la Información de los participantes del mercado de valores.

Párrafo. De igual manera, el superintendente del Mercado de Valores podrá establecer disposiciones especiales en materia de Seguridad de la Información para los emisores, auditores externos, calificadoras de riesgos y cualquier otro participante del mercado de valores no contemplado en el alcance de este Reglamento mediante normas técnicas u operativas.

Artículo 62. Obligatoriedad. Las disposiciones establecidas en este Reglamento son de cumplimiento obligatorio y, en caso de incumplimiento, se aplicarán las sanciones previstas en la Ley y el Reglamento del Procedimiento Administrativo Sancionador.

Artículo 63. Entrada en vigencia. Las disposiciones de este Reglamento entran en vigencia en el plazo de nueve (9) meses, contados a partir del día hábil siguiente a su publicación.

Artículo 64. Plazo de adecuación. Los participantes del mercado de valores deben adecuarse a las disposiciones del presente Reglamento previo a su entrada en vigencia.

Párrafo I. Para el fin anterior, los participantes del mercado de valores deben remitir a la Superintendencia un cronograma de adecuación gradual que, al menos, se ajuste a la siguiente distribución en su implementación:

Frecuencia	%
Trimestre 1	20%
Trimestre 2	40%
Trimestre 3	40%

Párrafo II. El cronograma de adecuación indicado en párrafo anterior debe remitirse a la Superintendencia dentro de treinta (30) días hábiles, contados a partir del día hábil siguiente a la publicación de este Reglamento.

Párrafo III. Los participantes del mercado de valores que por su nivel de sofisticación estén avanzados en el cumplimiento de los estándares de este Reglamento, deben notificarlo a la Superintendencia.” [Sic]

SEGUNDO: OTORGAR un plazo de cuarenta y cinco (45) días hábiles para recabar la opinión de los participantes del mercado de valores, sectores interesados y público en general, a partir de la publicación de la presente.

Párrafo: Las opiniones a las que se refiere el presente artículo podrán ser remitidas físicamente a la División de Normas de la Dirección de Regulación e Innovación de la Superintendencia del Mercado de Valores; o por vía electrónica, a través del correo normas@simv.gob.do.

TERCERO: INSTRUIR a la señora secretaria del Consejo expedir copia certificada de la presente resolución, conforme lo dispuesto por el artículo 16, párrafo, de la Ley núm. 249-17; para los fines correspondientes.”

Aprobada y firmada por los miembros del Consejo, señores: **ERVIN NOVAS BELLO**, gerente del Banco Central, en representación del gobernador del Banco Central, miembro ex officio y presidente del Consejo; **MARÍA JOSÉ MARTINEZ DAUHJRE**, viceministra de Crédito Público del Ministerio de Hacienda, en representación del ministro de Hacienda, miembro ex officio, **ERNESTO A. BOURNIGAL READ**, superintendente del Mercado de Valores, miembro ex officio, **WILLIAM V. WALL**, miembro independiente de designación directa, **MANUEL GARCÍA TRONCOSO**, miembro independiente de designación directa, y **ABRAHAM SELMAN HASBÚN**, miembro independiente de designación directa. No figura la firma del señor **MARCOS IGLESIAS SÁNCHEZ**, miembro independiente de designación directa, en razón de que no participó en la deliberación y votación de la presente resolución por las causas previstas en la normativa vigente aplicable.

La presente se expide para los fines correspondientes, en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, el día diez (10) de abril del año dos mil veintitrés (2023).

ERVIN NOVAS BELLO

Por el gobernador del Banco Central de la República Dominicana, miembro ex officio y presidente del Consejo Nacional del Mercado de Valores

FABEL MARÍA SANDOVAL

Secretaria del Consejo Nacional del Mercado de Valores