Superintendencia del Mercado de Valores
de la República Dominicana

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 oficio 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 **Segunda Resolución, R-CNMV-2024-08-MV,** adoptada por el Consejo en la reunión celebrada en fecha **dieciséis (16) de julio del año dos mil veinticuatro (2024)**, la cual reposa en los archivos de esta Secretaría, a saber:

"SEGUNDA RESOLUCIÓN DEL CONSEJO NACIONAL DEL MERCADO DE VALORES DE FECHA DIECISEIS (16) DE JULIO DEL DOS MIL VEINTICUATRO (2024).
R-CNMV-2024-08-MV

REFERENCIA: Aprobación del Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores.

RESULTA:

Que en fecha primero (1ro.) de julio del dos mil veinticuatro (2024), 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"), el proyecto de Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores (en lo adelante "proyecto de Reglamento").

Que el Consejo, en cumplimiento con las atribuciones 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 en atención a lo dispuesto por el Reglamento Interno del Consejo Nacional del Mercado de Valores, adoptado por este organismo colegiado mediante la Primera Resolución, R-CNMV-2018-06-MV, de fecha veintinueve (29) de noviembre de dos mil dieciocho (2018) (en lo adelante el "Reglamento Interno del Consejo"); reunido válidamente, previa convocatoria, junto con la correspondiente documentación soporte, tiene a bien exponer lo siguiente:

CONSIDERANDO:

1. Que conforme al artículo 6 de la Ley núm. 249-17, la Superintendencia es un organismo autónomo y descentralizado del Estado, investido con personalidad jurídica, patrimonio propio, autonomía administrativa, financiera y técnica.

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

2. Que según dispone el artículo 7 de la citada legislación, la Superintendencia tiene por objeto promover un mercado de valores ordenado, eficiente y transparente, proteger a los inversionistas, velar por el cumplimiento del referido estatuto legal y mitigar el riesgo sistémico, mediante la regulación y fiscalización de las personas físicas y jurídicas que operan en el mercado de valores.

3. Que, en atención a lo dispuesto por el artículo 10 de la Ley núm. 249-17, la Superintendencia del Mercado de Valores (en lo adelante "Superintendencia") está integrada por un órgano colegiado, el Consejo, y un funcionario ejecutivo, el superintendente.

4. 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.

5. Que, asimismo, el referido artículo 13, en sus numerales 4 y 5, confiere al Consejo la atribución de dictar los reglamentos de aplicación de la Ley núm. 249-17, así como de revisar de manera periódica el marco regulatorio del mercado de valores, adecuándolo a las tendencias y realidades del mercado, a la vez que le faculta para proponer, por iniciativa propia o a propuesta del superintendente, las modificaciones que sean necesarias.

6. Que, en ese orden, el artículo 25 Ley núm. 249-17 establece que "[e]l Consejo es el órgano competente para establecer los reglamentos relativos a las actividades del mercado de valores señaladas en esta ley. Corresponde a la Superintendencia el desarrollo de las normas técnicas u operativas derivadas de esta ley y de los reglamentos aplicables y normas necesarias, para el ejercicio de su potestad de auto organización interna."

7. Que, aunado a lo anterior, por virtud del artículo 17, numeral 14, de la aludida norma, el superintendente se encuentra investido de facultad para dictar las resoluciones, circulares e instructivos requeridos para el desarrollo de la Ley núm. 249-17 y sus reglamentos.

8. Que el artículo 25, párrafo I, de la Ley núm. 249-17 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".

9. Que el artículo 4 de la preindicada disposición legal establece que el mercado de valores se regirá con estricto apego a la Constitución de la República, a lo prescrito en dicha ley y en los reglamentos y resoluciones que dicte el Consejo y la Superintendencia, en el área de sus respectivas competencias;

FSS

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

siendo de aplicación supletoria, en los asuntos no previstos específicamente en las anteriores normas, las disposiciones generales del derecho administrativo, la legislación societaria, comercial, monetaria y financiera, de fideicomiso, el derecho común y los usos mercantiles, en el orden citado.

10. Que es de resaltarse que el artículo 2 de la Ley núm. 249-17 revela que las disposiciones contenidas en dicho estatuto 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.

11. Que, paralelamente, en el párrafo del artículo mencionado se establece que "[l]as personas físicas y jurídicas que realicen cualesquiera de las actividades o servicios previstos en esta ley, estarán sujetas a la regulación, supervisión y fiscalización de la Superintendencia del Mercado de Valores, en lo relativo al ejercicio de esas actividades o servicios mencionados."

12. Que entre las facultades que invisten al superintendente de conformidad con el artículo 17, numerales 2 y 11, se destacan:

> "2) Cumplir y hacer cumplir las disposiciones de esta ley y sus reglamentos, asegurando la correcta aplicación de sus principios, políticas y objetivos.
>
> 8) Supervisar, inspeccionar y fiscalizar las actividades y operaciones de los participantes del mercado de valores.
>
> 11) Requerir las informaciones que deberán suministrar las personas físicas y jurídicas inscritas en el Registro."

13. Que, por su parte, el artículo 36 de la Ley núm. 249-17 expresa 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."

14. Que, de acuerdo a lo que manifiesta el artículo 3, numeral 33, del señalado precepto legal, son participantes del mercado de valores las personas físicas o jurídicas inscritas en el Registro del Mercado de Valores y reguladas por la Superintendencia.

15. Que mediante comunicación recibida en la Secretaría del Consejo en fecha dieciséis (16) de abril del dos mil veinticuatro (2024), el señor superintendente elevó al conocimiento y aprobación definitiva del este órgano colegiado el proyecto de Reglamento, conjuntamente con un expediente justificativo.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

16. Que en dicha misiva se informa que el objeto del proyecto de Reglamento es establecer los criterios y lineamientos generales que deben adoptar los participantes del mercado para procurar la integridad, disponibilidad y confidencialidad de la información, así como el funcionamiento óptimo en los sistemas de información y de la infraestructura tecnológica. De igual manera, establecer la adopción e implementación de prácticas para la gestión de riesgos de la seguridad cibernética y de la información.

17. Que la indicada comunicación manifiesta que, en cumplimiento con el ordenamiento jurídico vigente aplicable, el proyecto de Reglamento fue sometido a consulta pública desde el veinticinco (25) de abril hasta el veintinueve (29) de junio del año dos mil veintitrés (2023), inclusive; recibiendo comentarios por distintos actores del sector privado.

18. Que, igualmente, de los documentos que acompañan la comunicación del señor superintendente se destaca que, fruto del referido proceso consultivo, fueron recibidos comentarios de: la Asociación Dominicana de Sociedades Administradoras de Fondos de Inversión, Inc. (ADOSAFI), la Asociación Dominicana de Puestos de Bolsa, Inc. (APB)., el Centro Financiero BHD, CEVALDOM Depósito Centralizado de Valores, S.A., Bolsa y Mercados de Valores S.A. (BVRD), la Asociación Cibao de Ahorros y Préstamos; y la Asociación La Nacional de Ahorros y Préstamos.

19. Que se destaca que el cuerpo técnico involucrado en el análisis de las observaciones y comentarios presentados por el mercado incluye funcionarios y colaboradores de las direcciones de Participantes, de Tecnología de la Información y la Comunicación; de Regulación e Innovación, de Oferta Pública; Jurídica y de Análisis de Riesgos y Estudios Económicos.

20. Que de las piezas que componen el expediente se resalta una matriz que recoge las observaciones y comentarios presentados, debidamente analizados y respondidos por el equipo técnico de la Superintendencia; celebrándose, de manera posterior, como parte del procedimiento administrativo y en atención a los principios de transparencia y participación, una mesa de trabajo -en modalidad virtual- con los sectores interesados el quince (15) de abril del dos mil veinticuatro (2024).

21. Que, asimismo, en los documentos presentados al Consejo se encuentra una relación de los datos relevantes en la que se explica el proyecto de Reglamento contempló las siguientes mejoras a partir del proceso de consulta, a saber:

"

- Se adecua redacción del Alcance.
- Se exceptúan a las Entidades de Intermediación Financiera del Alcance del Reglamento
- Se incluyen las definiciones de Ataque y Evento.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

- Se elimina la referencia a las prácticas efectiva del marco de gobernanza.
- Se adecuan los mecanismos de control de acceso.
- Se elimina el artículo de entornos de desarrollo de sistemas.
- Se modifica la periodicidad de la revisión de los Registros y monitoreo de los usuarios administradores.
- Se adecuan las responsabilidades del consejo de administración
- Se modifica la composición del comité funcional de Seguridad Cibernética.
- Se modifica la entrada en vigencia del reglamento y el plazo de adecuación." [sic]

22. Que, posteriormente, mediante comunicación recibida en la Secretaría del Consejo en fecha primero (1ro.) de julio del dos mil veinticuatro (2024), el señor superintendente reintrodujo al Consejo una versión actualizada del proyecto de Reglamento, merced de ajustes de redacción realizados por virtud de observaciones y comentarios presentados por el equipo técnico del Banco Central de la República Dominicana el catorce (14) de junio del dos mil veinticuatro (2024).

23. Que, de acuerdo a lo explicado en el documento denominado Exposición de Motivos, en el desarrollo del Reglamento se han considerado las mejores prácticas en materia de regulación del Mercado de Valores, especialmente los objetivos y los principios establecidos por la Organización Internacional de Comisiones de Valores (IOSCO, por sus siglas en inglés), con apego al marco legal de la República Dominicana.

24. Que se agrega que IOSCO contempla la necesidad de que los reguladores estén a la vanguardia respecto al desarrollo creciente de la tecnología y los avances en el área de comercio electrónico.

25. Que, conforme lo razonado en dicho documento, ante el desarrollo de la tecnología -y sus riesgos asociados por la ola creciente de los ciberataques- y la importancia que 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 respecto a estos, a los fines de mitigar el riesgo sistémico y velar por la protección de los inversionistas.

26. Que se explica que una falla operativa en el Mercado de Valores puede afectar negativamente a la estabilidad financiera, por tal razón, es fundamental que las entidades identifiquen cuáles son sus operaciones críticas y activos de información de apoyo, en orden de prioridad, comprender su situación interna y sus dependencias externas, es la clave para poder responder de manera eficaz a las posibles amenazas cibernéticas que se pueden presentar.

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

27. Que, considerando el riesgo sistémico que representa esta materia en el mercado de valores, el proyecto de Reglamento será de aplicación obligatoria para los siguientes participantes del mercado de valores:

a) Intermediarios de valores.
b) Sociedades administradoras de mecanismos centralizados de negociación.
c) Depósitos centralizados de valores.
d) Sociedades que administren los sistemas de compensación y liquidación.
e) Entidades de contrapartida central

28. Que, de igual modo, las sociedades administradoras de fondos de inversión, sociedades fiduciarias de fideicomisos de oferta pública, sociedades titularizadoras, sociedades proveedoras de precios, y promotores de inversión personas jurídicas, estarán sometidas de manera obligatoria al cumplimiento de en títulos específicos del proyecto de Reglamento, y podrán, de manera voluntaria, acogerse a las demás disposiciones.

29. Que, asimismo, la aplicación del proyecto de Reglamento se extenderá a las entidades que provean servicios mediante el mantenimiento de una conexión electrónica o 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.

30. Que, en atención a todo lo expuesto precedentemente, ponderados los informes y documentaciones rendidos por el área técnica de la Superintendencia, este organismo colegiado es de opinión que el proyecto de Reglamento puede ser acogido de manera favorable.

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), promulgada el 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).

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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. 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).

f. 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).

g. 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).

h. La comunicación recibida en la Secretaría del Consejo en fecha dieciséis (16) de abril del dos mil veinticuatro (2024), suscrita por el señor superintendente, y documentación adjunta.

i. La comunicación recibida en la Secretaría del Consejo en fecha primero (1ro.) de julio del dos mil veinticuatro (2024), suscrita por el señor superintendente, y anexos que cita.

j. Los demás documentos que integran el expediente.

POR TANTO:

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

RESUELVE:

PRIMERO: APROBAR la versión definitiva del proyecto del Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores; conforme el documento presentado por la Dirección de Regulación e Innovación, a través del señor superintendente, cuyo contenido es copiado textualmente a continuación:

"REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES"

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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; y,
8) Las sociedades proveedoras de precios.

Párrafo I. Este Reglamento comprende las disposiciones normativas relativas al régimen general para la administración integral de Riesgos Tecnológicos, de Seguridad Cibernética y 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, por lo que, esta última será el régimen de aplicación principal para dichas entidades.

Párrafo II. Los Participantes del Mercado de Valores que no se encuentren sujetos al sistema de pagos y liquidación de valores y a los cuales les sea otorgado el Acceso al Equipo de Respuesta a Incidentes de Seguridad Cibernética para el Sector Financiero (CSIRT, por sus siglas en inglés) por parte del Banco Central de la República Dominicana deben remitir los requerimientos relativos a Incidentes de conformidad a lo establecido en el Reglamento de Seguridad Cibernética y de la Información emitido por la Junta Monetaria.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

Párrafo III. El superintendente de la Superintendencia del Mercado de Valores (en lo adelante, el "superintendente") podrá desarrollar mediante norma técnica u operativa los requerimientos mínimos aplicables a los Emisores. Las Entidades de Intermediación Financiera reguladas y fiscalizadas por las Administración Monetaria y Financiera estarán sujetas únicamente a las disposiciones sobre la materia emitidas por su regulador sectorial.

Párrafo IV. El superintendente podrá dictar las disposiciones y lineamientos mínimos en materia de Seguridad Cibernética y de la Información a los fines de permitir la conexión de los Participantes del Mercado de Valores, incluyendo aquellos que no se encuentran sujetos al Alcance del presente Reglamento, a los sistemas de la Superintendencia del Mercado de Valores (en lo adelante, la "Superintendencia").

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") y sus reglamentos de aplicación, 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. Una Amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una Vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un Incidente de seguridad.

3) **Ataque**: Intento de obtener acceso no autorizado a los sistemas, sus recursos, servicios o Información, o de comprometer la Integridad de los mismos. Comprender cualquier tipo de actividad maliciosa que pretenda recopilar, degradar o destruir los recursos de los sistemas de Información, la Información contenida en éstos, interrumpir o provocar negación de sus servicios, o el daño a la Infraestructura Tecnológica que los soporta.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

4) **Bases de Datos:** Serie de datos organizados y relacionados entre sí, almacenados en los sistemas de Información del Participante del Mercado de Valores o de sus proveedores de servicios.

5) **BSA:** Corresponde a las siglas en inglés a Software Alliance (Alianza de Software).

6) **CIS:** Corresponde a las siglas en inglés a *Center for Internet Security* (Centro de Seguridad de Internet).

7) **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).

8) **Confidencialidad:** Preservación de la Información a fin de que la misma no sea divulgada en todo o en parte a personas físicas o jurídicas, o procesos, a menos que éstos hayan sido autorizados para acceder a dicha Información. Incluye los medios para proteger la privacidad personal y la Información Esencial.

9) **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.

10) **COSO:** Corresponde las siglas en inglés al *Committee of Sponsoring Organizations of the Treadway* (Comité de Organizaciones Patrocinadoras de la Comisión Treadway).

11) **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).

12) **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.

13) **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.

14) **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.

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

15) **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la entidad, originados por la misma causa, que ocurren durante el mismo período.

16) **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.

17) **GDPR:** Corresponde a las siglas en inglés de *General Data Protection Regulation* (Regulación General de Protección de Datos) de la Unión Europea.

18) **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.

19) **Gestión de Riesgo Tecnológico:** Método para determinar, analizar, valorar y clasificar el Riesgo con el objeto de implementar mecanismos que permitan gestionarlo.

20) **Hardware:** Conjunto de equipos físicos que componen una computadora.

21) **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.

22) **IAPP:** Corresponde a las siglas en inglés al *International Association of Privacy Professionals* (Asociación Internacional de Profesionales de la Privacidad).

23) **IEC:** Corresponde a las siglas en inglés al *International Electrotechnical Commission* (Comisión Electrotécnica Internacional).

24) **Incidente:** Evento que pone en peligro la Integridad, disponibilidad o Confidencialidad de la Infraestructura Tecnológica o la Información procesada, almacenada o transmitida por dicho sistema, o que constituye una violación o Amenaza inminente de violación de políticas o Procedimientos de seguridad o políticas de uso aceptable.

25) **Incidentes Significativo:** Incidente o conjunto de Incidentes relacionados que podrían resultar en la degradación o pérdida de funciones críticas de servicios financieros, resultando en un riesgo sistémico para el sector financiero o en pérdida de la confianza.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

26) **Información:** Conjunto de datos o cualquier forma de registro electrónico, óptico, magnético u otros medios, susceptible de ser procesada, distribuida y almacenada.

27) **Información Esencial:** Es aquella que facilita el desarrollo de las actividades fundamentales de la entidad y que sustentan la operatividad de la Infraestructura Tecnológica.

28) **Información Esencial de Tipo Maestro**: Conjunto de datos básicos cuyos registros sufren poca o ninguna variación en el tiempo.

29) **Información Esencial de Tipo Transaccional**: Conjunto de datos cuyos registros contienen Información sobre las transacciones realizadas en un sistema de Información.

30) **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.

31) **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.

32) **IP**: Corresponde a las siglas en inglés de *Internet Protocol* (Protocolo de Internet).

33) **ISO:** Corresponde a las siglas en inglés de *Internacional Organization for Standardization* (Organización Internacional de Normalización).

34) **ISF:** Corresponde a las siglas en inglés de *Information Security Forum* (Foro de la Seguridad de la Información).

35) **ITIL:** Corresponde a las siglas en inglés de *Information Technology Infrastructure Library* (Biblioteca de Infraestructura de Tecnologías de Información).

36) **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.

37) **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,

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

ITIL, NIST, OWASP, PMBOK, SWIFT, entre otros estándares reconocidos internacionalmente que puedan aplicar.

38) **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.

39) **NIST:** Corresponde a las siglas en inglés de *National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología).

40) **OWASP:** Corresponde a las siglas en inglés de *Open Web Application Security Project* (Proyecto Abierto de Seguridad de Aplicaciones Web).

41) **PBX:** Corresponde a las siglas en inglés de *Private Branch Exchange* (Central Privada Automática).

42) **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.

43) **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.

44) **PMBOK:** Corresponde a las siglas en inglés de *Project Management Body of Knowledge* (Guía de los Fundamentos para la Dirección de Proyectos).

45) **Problema**: Es la causa conocida o desconocida de un Incidente.

46) **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.

47) **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.

48) **Riesgo**: Es la posibilidad de ocurrencia de Eventos que impacten negativamente los objetivos del Participante del Mercado de Valores y su situación financiera.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

49) **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.

50) **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.

51) **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

52) **SWIFT**: Corresponde a las siglas en inglés de *Society for Worlwide Interbank Financial Telecommunication* (Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales).

53) **Tecnología de Información:** Conjunto de herramientas y métodos empleados para llevar a cabo la administración de la Información.

54) **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 al Marco de Trabajo seleccionado y ser cónsono con la naturaleza, tamaño, complejidad y perfil de Riesgos del negocio de cada Participante del Mercado de Valores.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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.

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 autentificación:** 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) **Confiabilidad:** 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 a los usuarios y para las autoridades públicas competentes en el ejercicio de sus facultades legales en el tiempo y la forma requerida;

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;

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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, que permita garantizar la Integridad, Confidencialidad y Disponibilidad de la Información, así como gestionar efectivamente los Riesgos, incluyendo los de Ciberseguridad, mediante la adecuada combinación de políticas, Procedimientos, controles, estructura organizacional y herramientas informáticas especializadas;

2) Definir políticas y Procedimientos para la Seguridad Cibernética y de la Información conforme a al Marco de Trabajo adoptado. 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 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 y adoptado por la entidad. 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 Riegos 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

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

y resultados de las autoevaluaciones y mantener evidencia del Monitoreo Continuo realizado, conforme a lo establecido en sus políticas;

8) Identificar Amenazas 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) Entrenar a los empleados que cuenten con Acceso 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/o 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

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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, en tanto sea pertinente en virtud de las funciones ejercidas o servicios contratados.

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 concientización. Los empleados del Participante del Mercado de Valores y, cuando sea pertinente, los proveedores de servicios, afiliados o usuarios, deben recibir entrenamiento y orientación 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 Tecnología de la Información. Los Participantes del Mercado de Valores deben desarrollar un esquema de gestión de activos de Tecnología de la Información a través de su ciclo de vida que contemple, al menos, lo siguiente:

1) Adquisición de todos los activos de Tecnología 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;

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

2) Desplegar los activos de Tecnología 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 Tecnología de la Información críticos y sensibles;

4) Registro actualizado y exacto de los activos de Tecnología de la Información necesarios para proveer los servicios, incluyendo:

    a) Identificación específica del activo de Tecnología de la Información;
    b) Prioridad de recuperación;
    c) Locación;
    d) Propietario o custodio designado;
    e) Clasificación según el Riesgo asociado o criticidad definida.

5) Procedimientos de control para la devolución y asignación de los activos de Tecnología 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 Tecnología de la Información es eliminado o destruido;

9) Definir Procedimientos para la seguridad de los activos de Tecnología 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 Tecnología de la Información desatendidos; y.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

11) Revisar los activos de Tecnología 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 deben 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 conforme al Marco de Trabajo adoptado para las aplicaciones del negocio. Dichos controles deben contemplar, 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 *web* 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.

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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 Información según las leyes y normativas vigentes y el Marco de Trabajo seleccionado. 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

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

las citadas materias deben prolongarse luego de la finalización de la relación contractual por el tiempo 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 revisar periódicamente 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, algunos de los siguientes:

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

a) Algo que el usuario sabe, por ejemplo, contraseña o PIN;
b) Algo que el usuario tiene, por ejemplo, token físico o digital, tarjeta inteligente o certificado digital;
c) Algo que el usuario es o hace, por ejemplo, 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 decidir establecer uno o más Mecanismos de Control de Acceso, según el análisis de Riesgo realizado por la entidad y 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, de conformidad a su análisis de Riesgo, 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 y reglas para su reutilización.

Párrafo. Los empleados de los Participantes del Mercado de Valores deben suscribir un compromiso donde reconozcan la responsabilidad de mantener confidenciales las contraseñas y credenciales 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 adoptado 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 Tecnología de la Información y control de visitas al entorno;

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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, por ejemplo, el uso señalizaciones discretas y la exclusión de directorios telefónicos y de portales informativos;

2) El fortalecimiento de la seguridad perimetral y mecanismos contra robos de equipos informáticos críticos y documentación sensible en formato físico, por ejemplo, el uso de paredes sólidas, ventanas y puertas blindadas;

3) La instalación de controles físicos, por ejemplo, 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, tales como, instalación de equipos contra fluctuación de cargas, uso de generadores eléctricos de emergencia, instalación de luces de emergencia o 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, incluyendo lugares que albergan los sistemas informáticos, tales como, los centros de datos, redes, equipos de telecomunicaciones, material físico sensible y otros activos importantes, deben ser protegidos contra accidentes, Ataques y el acceso físico no autorizado; contra los

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

cortes o fluctuaciones de energía, así como estar protegidos contra incendios, inundaciones y otras Amenazas naturales.

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 Amenazas. 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;

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, 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;

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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. Sobre las aplicaciones de alta relevancia de la entidad, 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, según corresponda, los aspectos siguientes:

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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, para sistemas que realicen copias en cinta;

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 y, en caso de las copias de resguardo en formato digital, en la nube o en un ambiento con diferentes niveles de Acceso y de localización.

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, con la suficiente distancia definida por la entidad, para la salvaguarda de cualquier daño de un desastre en el sitio principal.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

interrupción impondría y el tiempo de recuperación. Dicho análisis debe ponderar, 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 estimado;
c) Preselección de planes adecuados para el tratamiento de los Riesgos identificados;
d) Escalas de tiempo para la recuperación de sistemas, aplicaciones y servicios;
e) Tiempo de interrupción máxima 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 Significativos:** 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 Significativo 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.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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, es decir, derechos y permisos otorgados;
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 falsos positivos 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 tres (3) años.

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

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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 Significativo, 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 y aspectos técnicos.

2) Establecimiento de un Procedimiento para la gestión de Problemas e Incidentes Significativos 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 tres (3) años, procurando el almacenamiento en formato físico con el nivel apropiado de protección ambiental y conforme a los métodos indicados por los fabricantes o, en caso tratarse de almacenamiento en formato digital, en la nube o en un ambiento con diferentes niveles de Acceso y de localización;

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,

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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 parches de 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, conforme a lo determinado en la norma de carácter técnico emitido por el superintendente.

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 estimada del posible impacto del Ataque.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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 sus empleados sobre el Software malicioso. De igual manera, los Participantes del Mercado de Valores deberán informar y hacer recomendaciones a los usuarios a los fines de concientizarlos 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 mantener configuraciones adecuadas 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;

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

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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) Verificar el cumplimiento y registrar las labores de mantenimiento remoto;

FSS

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

g) Supervisar los mantenimientos remotos durante su realización. Una vez terminadas las sesiones de mantenimiento, la conexión debe 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;
d) Inventario de dispositivos de puntos de Acceso de redes inalámbricas;
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 como, por ejemplo, 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;

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

c) Controles especializados para la infraestructura de telefonía como, por ejemplo, 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 como, por ejemplo, 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 en el ejercicio de sus funciones laborales, 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, términos y condiciones de uso

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

debe ser realizada por un tercero independiente utilizando modelos de reportes de Riesgo y controles en la provisión de servicio (Por ejemplo: SOC 2, etc., u otras 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. 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 desarrollo, preproducción y producción, así como 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. 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.

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

Artículo 45. Información a la Superintendencia. Los Participantes del Mercado de Valores deben notificar mediante comunicación confidencial a 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 decisión de realizar cambios en la plataforma central de operaciones y sistemas computarizados que afecten o podrían afectar la operatividad de la entidad;
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, debidamente reportados previamente al CSIRT para aquellos que cuenten con acceso para realizar dichas notificaciones conforme al Párrafo II del artículo 2 de este Reglamento;
5) La decisión 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 46. 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.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

3) Análisis de Riesgos asociados al uso de soluciones criptográficas, incluyendo los algoritmos de Encriptación, cuando sean aplicados;

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 47. 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 la 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 con regularidad cada vez que sea necesario y en todo caso, por lo menos, una (1) vez al año con el objetivo de identificar nuevas Vulnerabilidades utilizando técnicas avanzadas y garantizando que las identificadas previamente han sido corregidas correctamente.

Artículo 48. 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 49. 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, semestralmente o en un período inferior definido por la entidad en función de los hallazgos detectados en evaluaciones anteriores y de la necesidad del negocio.

Artículo 50. 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

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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) **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;

4) **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;

5) **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;

6) **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,

7) **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.

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

TÍTULO III
DISPOSICIONES SOBRE EL GOBIERNO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN

CAPÍTULO I
Órganos de Gestión

Artículo 51. Gobierno de Seguridad Cibernética y de la Información. Los Participantes del Mercado de Valores deben contar con un 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.

Párrafo. Los Participantes del Mercado de Valores deben contar con una estructura organizacional y funcional de control de Seguridad Cibernética y de la Información acordes a su naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica, la cual estará conformada por:

a) El comité funcional de Seguridad Cibernética y de la Información especializado o cuyas funciones sean asumidas por el comité de Riesgos de la entidad;
b) La estructura gerencial quien dirigirá el Programa de Seguridad Cibernética y de la Información, en el marco de las responsabilidades definidas en este Reglamento.

Artículo 52. 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 la estrategia y enfoque estándar, formal y continuo a la gestión de seguridad para la Información y procesos de negocios que estén alineados con los requerimientos de negocio y la gestión de seguridad del Participante del Mercado de Valores;

3) Aprobar el programa de Seguridad Cibernética y de la Información, incluyendo los objetivos, lineamientos y políticas en dicha materia y sus Riesgos, así como velar por su cumplimiento;

4) 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;

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

5) Velar para que los Riesgos relacionados con la Seguridad Cibernética y de la Información no excedan la tolerancia de Riesgo de la entidad;

6) Dar seguimiento al cumplimiento de la implementación de sistemas de Información propios, adquiridos o subcontratados, con la normativa vigente aplicable;

7) Adoptar las políticas que contemplen las estrategias 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;

8) Aprobar y dar seguimiento al Plan de Continuidad de Negocios, Plan de Contingencia y programas de pruebas de estrés, como parte de su proceso de gestión integral de Riesgo;

9) Asegurar que exista un sistema adecuado de delegación de responsabilidades y segregación de funciones en la entidad.

Artículo 53. 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, evaluados y aprobados 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) 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;

6) Ratificar las decisiones de tratamiento de Riesgo en coordinación con las áreas pertinentes de negocios,

FSV

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

previamente presentados por el oficial de Seguridad Cibernética y de la Información; y,

7) 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;
c) Un miembro de la Alta Gerencia designado por el consejo de administración cuyas funciones guarden relevancia en la materia.

Párrafo II. El oficial de Seguridad Cibernética y la Información fungirá como secretario del comité funcional de Seguridad Cibernética y de la Información y participará con voz, pero sin voto.

Párrafo III. En las reuniones del comité deberán asistir en calidad de invitados permanentes el Ejecutivo Principal en materia de tecnología y el gerente de Riesgos. De igual forma, podrán asistir a las reuniones del comité en calidad de invitados con voz, pero sin voto, el personal u otros ejecutivos de la entidad 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 IV. Las entidades 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 V. Las labores del comité funcional de Seguridad Cibernética y de la Información podrán ser asumidas por el comité de Riesgos de los Participantes del Mercado de Valores (el cual no alterará su composición en este caso) que, por su naturaleza, complejidad, perfil de Riesgo e importancia sistémica así lo requieran. En estas entidades, el proceso de gestión integral de Riesgos debe tomar en consideración el programa de Seguridad Cibernética y de la Información en lo que respecta a los Riesgos asociados a dicha materia. Cuando el comité de Riesgos sesione en calidad de comité funcional de Seguridad Cibernética y de la Información deben participar, con voz y sin voto, el oficial de Seguridad Cibernética y la Información y el Ejecutivo Principal en materia de tecnología.

FSS

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

Párrafo VI. La Superintendencia vía norma técnica u operativa establecerá las disposiciones relativas al comité funcional de Seguridad Cibernética y de la Información

CAPÍTULO II
Estructura Gerencial

Artículo 54. 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 Ejecutivo Principal y al consejo de administración.

Artículo 55. 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 56. 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;

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

6) Cumplir con los límites de los niveles de Riesgos relevantes establecidos por el consejo de administración, relacionados con Amenazas o Incidentes Significativos;

7) Monitorear permanentemente el 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 57. 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 materia de Seguridad Cibernética y de la Información 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 58. 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 59. 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.

FSR

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

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 del Mercado de Valores al consejo de administración posterior a la evaluación por parte del comité de auditoría.

TÍTULO IV
DISPOSICIONES FINALES

Artículo 60. Normativa complementaria. El superintendente, 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.

Artículo 61. 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 62. Entrada en vigencia. Las disposiciones de este Reglamento entran en vigencia en el plazo de seis (6) meses, contados a partir del día hábil siguiente a su publicación.

Artículo 63. Plazo de adecuación. Los Participantes del Mercado de Valores deben adecuarse a las disposiciones del presente Reglamento en el plazo máximo de doce (12) meses contados a partir de 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:

FSV

Frecuencia	%
Trimestre 1	**%**
Trimestre 2	**%**
Trimestre 3	**%**
Trimestre 4	**%**

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5

Párrafo II. El cronograma de adecuación indicado en párrafo anterior debe remitirse a la Superintendencia dentro de noventa (90) días hábiles, contados a partir del día hábil siguiente a la publicación de este Reglamento.

Párrafo III. Los Participantes del Mercado de Valores deberán remitir un informe trimestral a la Superintendencia sobre su nivel de avance o ejecución de la adecuación reglamentaria conforme al cronograma notificado. No obstante, los Participantes del Mercado de Valores que, por su nivel de sofisticación y estrategias de mitigación de Riesgos, estén avanzados en el cumplimiento de los estándares de este Reglamento, deben notificarlo a la Superintendencia."

SEGUNDO: INSTRUIR al señor superintendente publicar la presente resolución en uno o más diarios de amplia circulación nacional, así como en el portal institucional, a los efectos del principio de publicidad contenido en el artículo 138 de la Constitución de la República Dominicana, en atención a lo dispuesto por los artículos 3, numeral 7, y 31, numeral 8, de la Ley núm. 107-13, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo; el artículo 3 de la Ley núm. 200-04, Ley General de Libre Acceso a la Información Pública, y su reglamento de aplicación.

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 oficio y presidente del Consejo; **MARÍA JOSÉ MARTINEZ DAUHAJRE**, viceministra de Crédito Público del Ministerio de Hacienda, en representación del ministro de Hacienda, miembro ex oficio, **ERNESTO BOURNIGAL READ**, superintendente del Mercado de Valores, miembro ex oficio, **ABRAHAM SELMAN HASBÚN**, miembro independiente, **MIGUEL NÚÑEZ HERRERA**, miembro independiente, y **JAVIER LARA REINHOLD**, miembro independiente.

La presente se expide para los fines correspondientes, en la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, el día veintidós (22) de julio del año dos mil veinticuatro (2024).

ERVIN NOVAS BELLO
Por el gobernador del Banco Central de la República Dominicana, miembro ex oficio y presidente del Consejo Nacional del Mercado de Valores

FABEL SANDOVAL VENTURA
Secretaria del Consejo Nacional del Mercado de Valores

Av. César Nicolás Penson No. 66, Santo Domingo, República Dominicana
Teléfono: 809.221.4433 • http:www.simv.gob.do / info@simv.gob.do / RNC: 4-01-51572-5