PROYECTO DE INSTRUCTIVO DEL PROYECTO DE REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES

OBSERVACIONES

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
Comentario general	**ADOSAFI**	Actualmente existe un Reglamento y un instructivo sobre Ciberseguridad de la Junta Monetaria para los participantes del Sistema de Pagos de la República Dominicana (SIPARD).	Considerar que este proyecto no sea contradictorio con la normativa de ciberseguridad de la Junta Monetaria	
Comentario general	**ADOSAFI**	Atentamente solicitamos incluir un plazo razonable de adecuación e implementación, considerando la capacidad de los diversos participantes y las condiciones requeridas sugerimos 36 meses.		
Comentario General	**Centro Financiero BHD**	Actualmente existe un Reglamento y un instructivo sobre Ciberseguridad de la Junta Monetaria para los participantes del Sistema de Pagos de la República Dominicana (SIPARD). Esta normativa actualmente alcanza a varios participantes del mercado de valores de nuestro grupo financiero: BHD Puesto de Bolsa, BHD Fondos y Banco BHD. Sugerimos remover a los Emisores regulados por otros entes supervisores (ej. los Bancos). Recordemos que los bancos están alcanzados por la normativa de ciberseguridad de la Junta Monetaria.	Considerar que este proyecto no se solape con la normativa de ciberseguridad de la Junta Monetaria. En todo caso, considerar establecer prelación según el regulador de cada participante	
Comentario General	**Centro Financiero BHD**	Considerar que algunos participantes pertenecen a grupos financieros y reciben asesoría y apoyo en la gestión de riesgos o tercerizan en una entidad de su grupo.		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		Sugerimos indicar expresamente que los participantes pueden delegar esta gestión y que la entidad podrá considerar cumplidos los requerimientos de este instructivo si el que le provee este servicio cuenta con lo exigido por la normativa, sin necesidad de crear nuevas políticas propias.		
Artículo 2	**Asociación Cibao de Ahorros y Prestamos (ACAP)**	Se sugiere incluir un texto con la exclusión textual de los emisores que participan en el SIPARD, por encontrarse regulados bajo el marco del Reglamento de Seguridad Cibernética y de la Información y su instructivo de aplicación, emitidos por la Junta Monetaria y el BC, respectivamente.		
Artículo 3	**SCRiesgo, Sociedad Calificadora de Riesgo, S.R.L.**	SCRiesgo, Sociedad Calificadora de Riesgo, S.R.L. ("SCR República Dominicana") apoya el desarrollo de marcos regulatorios y de supervisión aplicables a las Sociedades Calificadoras de Riesgo ("Calificadoras") que sean consistentes con las mejores prácticas internacionales, y el rol limitado, aunque importante, que cumplen las Calificadoras en los mercados financieros. Sin embargo, nos preocupa la inclusión de las Calificadoras en el artículo 3 del Capítulo II del Proyecto de Instructivo, el cual establece requerimientos mínimos sobre seguridad cibernética y seguridad de la información diseñados con un foco específico en emisores y auditores externos, los cuales tienen un rol en el mercado sustancialmente diferente al de las Calificadoras.	La aplicación de este artículo del Proyecto de Instructivo busca introducir una serie de obligaciones adicionales aplicable a Calificadoras no previstas en el Reglamento de Seguridad Cibernética y de la Información, ni en el Reglamento de Sociedades Calificadoras de Riesgo, genera incertidumbre regulatoria, potenciales conflictos de ley y contradicción con algunos principios como el principio de legalidad, la jerarquía de las normas y la seguridad jurídica.[2]	

[2] Ver Art. 40.15 y Art. 138 de la Constitución dominicana, así como Art. 30 y 31 de la Ley No. 107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo.

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		Consideramos que la aplicación de este artículo podría tener un efecto negativo en el mercado como resultado de la incertidumbre regulatoria y potencial conflictos de ley que podrían generarse como consecuencia de la aplicación de diferentes normativas sobre la misma materia a los mismos sujetos obligados y las posibles inconsistencias que puedan surgir, según lo que se detalla a continuación. I. Consideraciones En primer lugar, es importante notar que, de conformidad con lo dispuesto en el artículo 2 del Proyecto de Instructivo, el mismo es aplicable a "los Participantes del Mercado de Valores sujetos al cumplimiento del Reglamento sobre la Seguridad Cibernética", actualmente pendiente de ser publicado tras la conclusión de un proceso de consulta pública. Sin embargo, de conformidad con el Articulo párrafo III del artículo 4 de dicho Reglamento sobre la Seguridad Cibernética, el mismo es aplicable únicamente a emisores y no a las Calificadoras. Es importante notar que la Calificadoras se encuentran reguladas de manera específica por Reglamento de Sociedades Calificadoras de Riesgo (R-CNMV-2022-03-MV), que constituye el principal marco regulatorio que rige a las Calificadoras y sus actividades en la República Dominicana. El Reglamento de Sociedades Calificadoras contiene disposiciones específicas relativas al gestión de seguridad cibernética y de la información,		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		resultando las Calificadoras obligadas a cumplir con dichas disposiciones.[1] I. Observaciones No obstante, lo descrito anteriormente, notamos que el artículo 3 del Proyecto de Instructivo inadvertidamente incorpora una serie de obligaciones que extiende también a Calificadoras. Adicionalmente anotamos que la disposición particular del Reglamento sobre la Seguridad Cibernética (párrafo III del artículo 4) de la cual deriva dicho artículo 3 del Proyecto de Instructivo es de aplicación exclusiva a emisores y no a Calificadoras. Como describimos anteriormente, nos preocupa que la referencia a la Calificadoras en el Proyecto de Reglamento pueda tener un efecto negativo en el mercado como resultado de la incertidumbre regulatoria y potencial conflictos de ley. No obstante, nuestros comentarios al Proyecto de Instructivo, destacamos que para SCR República Dominicana la gestión de seguridad cibernética y de la información es un aspecto importante de sus operaciones. En ese sentido,		

[1] Artículo 24. Gestión de riesgos de la Sociedad Calificadora de Riesgo. La Sociedad Calificadora de Riesgo debe implementar un sistema de gestión de seguridad de la Información que permita garantizar la integridad, confidencialidad y disponibilidad de la información, así como gestionar efectivamente sus riesgos, incluyendo 1os de ciberseguridad, mediante la adecuada combinación de políticas, procedimientos, controles, estructura organizacional y herramientas
informáticas especializadas.
Párrafo. Las Sociedades Calificadoras de Riesgo deben establecer las medidas necesarias para mitigar los riesgos por pérdida, fraude o uso indebido de la información entregada en desarrollo de la actividad de calificación.
Artículo 25. Seguridad cibernética y de la información. Las Sociedades Calificadoras de Riesgo deben contar con una estructura organizacional que le permita implementar y mantener el sistema de gestión de la seguridad Cibernética y de la Información, diseñado de acuerdo con la naturaleza tamaño, complejidad y perfil de riesgos del negocio.
Párrafo. Las Sociedades Calificadoras de Riesgo deben implementar, de acuerdo con su tamaño, una serie de controles como parte de la gestión de la seguridad cibernética y de la información, tales como: el control de acceso; la seguridad física y ambiental; la gestión de activos: la adquisición, desarrollo y mantenimiento de sistemas informáticos; los procedimientos de respaldo, la gestión de Incidentes de Seguridad de información, la privacidad de la información, entre otros que se requieran mediante norma técnica y operativa que emita el Superintendente.

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		ha desarrollado un sistema diseñado acorde con su naturaleza, tamaño, complejidad y perfil de riesgos del negocio, según lo dispuesto por el artículo 25 y otros relevantes del Reglamento de Sociedades Calificadoras de Riesgo. Por lo anterior, solicitamos atentamente a la SIMV considerar no incluir a las Calificadoras en el artículo 3 del Capítulo III del Proyecto de Instructivo de Seguridad Cibernética y de la Información, debido a que (1) el Reglamento de Sociedades Calificadoras de Riesgo contiene disposiciones específicas sobre el tema, y (2) el alcance del Reglamento sobre Seguridad Cibernética no incluye a las Calificadoras y ha sido diseñados principalmente para emisores que tienen un perfil de riesgo y rol en los mercados financieros muy diferente al de las Sociedades Calificadoras de Riesgo. Por último, quisiéramos mencionar que el Proyecto de Instructivo pareciera contener un error de tipeo al incluir la obligación de las Calificadoras de establecer un marco de gobernanza de ciberseguridad según los criterios definidos en el párrafo III del artículo 4 (Criterios de Información) del Reglamento de Seguridad Cibernética. Sin embargo, observamos que el párrafo III del artículo 4 no contiene los Criterios de Información, sino que establece las características del marco de gobernanza aplicable a emisores, mientras que es el artículo 5 del Reglamento el que establece los Criterios de Información.		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
Artículo 3	**ADOSAFI**	**Requerimientos mínimos.** Los emisores, auditores externos y sociedades calificadoras de riesgos deben adoptar un marco de gobernanza de ciberseguridad especial sujeto a la no objeción de la Superintendencia del Mercado de Valores (en lo adelante, la ¨Superintendencia¨). Dicho marco debe incluir los criterios de información definidos en el ~~párrafo III del artículo 4~~ artículo 5 (Criterios de Información) del Reglamento, las políticas, procesos y estructuras de Gestión de Riesgos definidas con controles pertinentes adaptados a la naturaleza de los Riesgos de ciberseguridad a los que se enfrenta la sociedad y a los recursos de que dispone. Las prácticas efectivas incluyen a modo de referencia: 1) Definir un marco de gobernanza para apoyar la toma de decisiones basadas en la política de Riesgos; 2) Garantizar el compromiso activo de la Alta Gerencia y del consejo de administración sobre los aspectos de Seguridad Cibernética y de la Información; 3) Identificar marcos y estándares para abordar la Seguridad Cibernética y de la Información; 4) Utilizar métricas y umbrales para informar los procesos de gobernanza; y, Realizar evaluaciones internas de Riesgos de ciberseguridad.	Recomendamos que se refiera al artículo 5 del Proyecto de Reglamento que es el que, de hecho, refiere a los Criterios de Información. Sugerimos incluir esta disposición, a los fines de estar homologada con el Proyecto de Reglamento sobre Seguridad Cibernética y de la Información, R-CNMV2023-10-MV. Párrafo III, Artículo 4 del Proyecto de Reglamento sobre Seguridad Cibernética y de la Información, RCNMV-2023-10-MV.	
Artículo 4	**CEVALDOM, S.A.**	Se recomienda especificar que el artículo se refiere a la Política de Gestión de Seguridad de la Información, pues de lo contrario podría interpretarse que el esquema establecido aplica a todas las políticas que el participante desarrolle a nivel interno para la gestión de sus actividades. Por otro lado, nos remitidos a nuestros comentarios al artículo 6, numeral 2	Aportar claridad y precisión al texto, evitando errores o diversidad criterios al momento de interpretar el mismo.	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		del Proyecto de Reglamento en lo concerniente a las diferencias entre políticas y procedimientos y la responsabilidad de su aprobación por parte de los distintos órganos de gobierno.		
Artículo 5	**ADOSAFI**	**Contenido.** Los Participantes del Mercado de Valores deben elaborar políticas y procedimientos para la gestión de la Seguridad Cibernética y de la Información que se incorporarán en el Programa de Seguridad Cibernética y de la Información, las cuales se deben encontrar alineadas con su estrategia, reglamentos y leyes, e incluirán de manera enunciativa pero no limitativa, lo siguiente: (…)	Se recomienda que se especifique que este contenido es el que se espera del Programa de Seguridad Cibernética y de la Información, establecido en el artículo 4 del Proyecto de Reglamento. Así evitar confusiones sobre los documentos que habría que producir. Se debe definir el término "usuario" el cual es usado en el proyecto de Reglamento y en este proyecto de Instructivo y velar porque sean utilizados en el mismo contexto para evitar confusión.	
Artículo 5	**CEVALDOM, S.A.**	En lo que se refiere al contenido del documento enumerado, a continuación, nuestros comentarios: 1) Qué se espera sea el contenido del numeral 1, el cual se lee Seguridad Cibernética y de la Información. ¿Se busca que el concepto sea definido en la política? 2) En el numeral 6, se sugiere eliminar "que no se encuentren comprometidos", ya que el alcance de una política de respaldo es más amplio. 3) Se sugiere eliminar el numeral 7 ya que el mismo se repite con el numeral 5 literal c. 4) En el numeral 12 sugerimos ajustar para que se lea Privacidad y seguridad de los datos personales, de forma que se encuentre cónsono con la terminología establecida en la Ley 172-13. 5) En el numeral 16, Se recomienda eliminar "de telecomunicaciones", pues el alcance debería ser para todos los equipos y sistemas y con esto estarían limitando el alcance. Por lo que	Claridad del requerimiento	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		sugerimos que el mismo se quede hasta aplicaciones. 6) En el numeral 19 no queda claro a qué se refieren con hitos. Sugerimos que el numeral solo se refiera a la gestión de incidentes		
Artículo 5, Párrafo	**CEVALDOM, S.A.**	Al listado de personas mencionadas en el texto, se sugiere agregar "según aplique", pues no todos los proveedores, usuarios y contratistas necesitan conocer todas las políticas y procedimientos documentados	Mejor claridad en la información requerida Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	
Artículo 5, Párrafo	**ADOSAFI**	**Párrafo.** Los Participantes del Mercado de Valores deben ~~contar~~ obtener al momento de contratación de ~~con declaraciones firmadas por los~~ cualquier empleado~~s~~, o de contratistas~~,~~ y proveedores de servicios relacionados a los sistemas de Información y de la Infraestructura Tecnológica, declaraciones juradas ~~afiliados, usuarios y otras personas que se disponga~~ en las cuales estos se comprometan a acatar la política y los ~~P~~rocedimientos de seguridad documentados en el Programa de Seguridad Cibernética y de la Información del Participante.	Se recomienda limitar expresamente a quienes se le requerirá firmar declaración jurada y la temporalidad de la misma.	
Artículo 6 numeral 3	**CEVALDOM, S.A.**	Se recomienda mayor claridad con relación a la información requerida con ejecución de ejercicios simulados de campaña para mejorar el procedimiento de seguridad, ya que el mismo no es específico. Asimismo, a los fines de delimitar el alcance de la obligación aclarar si los referidos ejercicios simulados deben ser dirigidos a los empleados, pues por la lectura del párrafo inicial parecería que dichos ejercicios además deben ser realizados con los usuarios y proveedores. La concientización a proveedores y usuarios debería limitarse a	Mejorar la claridad de la información requerida. Principio de Seguridad jurídica, de previsibilidad y certeza normativa Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		campañas educativas para ampliar el conocimiento de estas personas sobre los riesgos de seguridad.		
Artículo 7	**ADOSAFI**	Se sugiere aclarar cuales firmas digitales se encuentran en el alcance de este documento. Se recomienda considerar los lineamientos sugeridos por Indotel y se solicita aclaración sobre los controles requeridos.	Claridad para los participantes y armonización con otras normas y leyes vigentes en el pís.	
Artículo 7	**Centro Financiero BHD**	Se sugiere aclarar cuales firmas digitales se encuentran en el alcance de este documento. Se recomienda considerar los lineamientos sugeridos por Indotel, se solicita aclaración sobre los controles requeridos.	Resolución núm. 071-19 del INDOTEL mediante la cual dictó la norma complementaria por la que se establece la equivalencia regulatoria del sistema dominicano de infraestructura de claves públicas y de confianza con los marcos regulatorios internacionales de servicios de confianza	
Artículo 7 numeral 1	**CEVALDOM, S.A.**	Tenemos a bien solicitarse a qué se refieren con el término “adquisición de documentos” dentro del ciclo de vida de la gestión de documentos	Claridad del requerimiento	
Artículo 7, numeral 3)	**ADOSAFI**	3) Establecer los mecanismos correspondientes (encabezados, pies de página, firmas digitales, sellos físicos o digitales, entre otros) y las etiquetas que identifiquen la clasificación de cada uno de los **Activos de Información**; y,	Se recomienda insertar una sección de definiciones donde se incluya el término “Activo de Información”. Se pudiera tomar la definición que se provee en el Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria, Resolución JM 181101-02: “Bien tangible o intangible, que almacena, procesa y/o transmite información”.	
Artículo 8	**Centro Financiero BHD**	Se solicita aclaración sobre el nivel validación requerido previo la creación de usuarios. Se solicita aclaración sobre el nivel validación requerido previo la creación de usuarios.	Comentario de nuestros equipos de ciberseguridad y cumplimiento	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		Se propone considerar la siguiente redacción de este artículo para eliminar redundancias y aclarar los controles solicitados: Gestión de identidades y Mecanismo de Control de Acceso. Las Políticas y Procedimientos de gestión de identidades y de Mecanismos de Control de Acceso que apliquen los Participantes del Mercado de Valores a los empleados, personal contratado y terceros que tengan Acceso a los sistemas de Información e Infraestructura Tecnológica, deberán considerar la Política de Seguridad Cibernética y de la Información, el esquema de Clasificación de la Información, la debida clasificación de los activos de la información y su riesgo, así como factores adicionales requeridos por los fabricantes de la Infraestructura Tecnológica, así como sus niveles de interconexión e interoperabilidad con los sistemas de seguridad física. Las entidades sujeto de este reglamento deberán incluir: 1) Política documentada para la administración y autenticación de identidades, considerando lo siguiente: a) Procedimientos de validación de identidades y creación de cuentas de usuario contemplando: i) Asignación de privilegios de Acceso para cada usuario de manera individual, contando con previa autorización;		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		ii) Aplicación de los principios del menor privilegio para la asignación de roles predefinidos a los usuarios; iii) Nomenclaturas y mecanismos que imposibiliten el uso o reasignación de nombres usuarios previamente utilizados; iv) Revisión periódica a fin de asegurar que los privilegios asignados continúan siendo los apropiados para el desempeño adecuado de las funciones del usuario, incluyendo, pero no limitado a, cambios de funciones departamentales o desvinculación con el Participante del Mercado de Valores, entre otros; v) Revocación del Acceso a todo empleado y parte externa como consecuencia de la desvinculación de su empleo, terminación del contrato o acuerdo, o cambios internos de área o funciones. b) Procedimientos de identificación, autenticación, inicio de sesión y administración de usuarios. c) Procedimiento documentado para el Control de Acceso para los usuarios a los distintos componentes de la Infraestructura Tecnológica del Participante del Mercado de Valores basado en los principios del menor privilegio, el cual debe implementarse en: i) Sistemas de Información y aplicaciones del negocio; ii) Redes de datos y equipos de red; iii) Base de Datos; iv) Dispositivos de computación personal para uso institucional; y,		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		v) Cualquier otro componente de la Infraestructura Tecnológica que sea determinado por la entidad. d) Procedimiento estableciendo directrices generales para la asignación y utilización de cuentas privilegiadas en los sistemas de Información y aplicaciones del negocio que regularán 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, en las cuales se estipule: i) Autorización para usuarios con Acceso privilegiado global en los casos que sea estrictamente necesario; y, ii) Una revisión previa de los privilegios por parte del personal responsable, con el fin de confirmar que los mismos están aplicados correctamente; iii) Un registro de las identidades reales de cada uno de los usuarios, así como los identificadores de acceso y el nivel asignado de privilegio; iv) Una notificación al usuario sobre los términos y condiciones del uso de las cuentas privilegiadas; v) En caso de los usuarios cuyos roles asignados ameriten realizar funciones especiales como autorizaciones y otros tipos de transacciones financieras, se debe implementar mecanismos de doble factor de autenticación para la realización de estas funciones; y, vi) Los procedimientos de revisión periódica de los privilegios asignados.		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
Artículo 8	**ADOSAFI**	**Gestión de identidades y Mecanismo de Control de Acceso.** Las políticas y Procedimientos de gestión de identidades y de Mecanismos de Control de Acceso que apliquen los Participantes del Mercado de Valores a los empleados, personal contratado y terceros que tengan Acceso a los sistemas de Información e Infraestructura Tecnológica, **conforme al Marco de Trabajo elegido por el participante del mercado de valores,** deben incluir: (…)	Sugerimos insertar para homogeneizar con el Reglamento**.**	
Artículo 9	**Centro Financiero BHD**	Los asuntos tratados en este artículo son más relacionados a tecnología que a ciberseguridad, considerar el alcance del instructivo. Considerar definir interconexión.		
Artículo 9	**ADOSAFI**	Evaluar eliminar todo el artículo.	Los asuntos tratados en este artículo son más relacionados a tecnología que a ciberseguridad, considerar el alcance del instructivo.	
Artículo 9 numeral 2, literal b	**CEVALDOM, S.A.**	Tenemos a bien solicitar se aclare el requerimiento de cierre de aplicación, sistemas, bases de datos o ambientes, ya que no es claro si se refiere a la desactivación o desinstalación de sistemas de información que no estén en eso.	Claridad del requerimiento	
Artículo 10	**ADOSAFI**	En el numeral 1: "Mecanismos de prevención y detección de intrusos en los sistemas críticos y redes de Información para la detección de actividades y comportamientos inusuales, inaceptables e inesperados en los sistemas de la Información, aplicaciones del negocio y demás componentes de la Infraestructura Tecnológica; (…)"	Claridad y no necesidad de actualización de la documentación respecto a las respuestas pues no sólo es complejo tener dicha capacidad de actualización continua, sino que no resulta eficiente ni muy útil hacerlo para los fines que se persiguen.	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		En cuanto al numeral 2c: El procedimiento de detección y prevención de accesos no autorizados no puede incluir la documentación de respuestas a los diferentes tipos de ataques ya que supone la actualización continua de dicho documento por la naturaleza diversa de los mismos. Los esquemas de IPS e IDS son esquemas de seguridad bajo la vertical de Proteger, vale la pena hacer la diferenciación de las actividades en la vertical de Responder y Recuperar.		
Artículo 10	**Centro Financiero BHD**	En cuanto al numeral 2c: El procedimiento de detección y prevención de accesos no autorizados no puede incluir la documentación de respuestas a los diferentes tipos de ataques ya que supone la actualización continua de dicho documento por la naturaleza diversa de los mismos. Los esquemas de IPS e IDS son esquemas de seguridad bajo la vertical de Proteger, vale la pena hacer la diferenciación de las actividades en la vertical de Responder y Recuperar.		
Art. 11 numeral 5, literal b	**CEVALDOM, S.A.**	Sugerimos revisar la redacción a fin de aportar claridad al texto. Esto a los fines de aclarar si la revisión es para detectar si la propia solución contra código malicioso se encuentra infectada o si es para comprobar la efectividad de la misma para prevenir que los activos de la información de la entidad no estén infectados.	Claridad del requerimiento	
Art. 11	**ADOSAFI**	**Protección de Software malicioso.** Los Participantes del Mercado de Valores deben ~~considerar directrices~~ **contar con políticas y procedimientos para la detección, prevención y** para la protección ~~de~~ **contra**	Descripción más detallada de lo que se espera del participante.	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		Software malicioso, dentro de las cuales se encuentran, de manera enunciativa pero no limitativa, las siguientes: (…) ~~c) Gestión de Incidentes relacionados con Software malicioso en múltiples niveles (alto, medio, bajo) y su posterior divulgación a los empleados y terceros.~~	Los incidentes de seguridad son considerados confidenciales y no son divulgados a empleados y proveedores por tanto sugerimos eliminar este acápite. Ejemplos de estos pudieran considerarse como material de concientización, si aplica.	
Art. 11	**Centro Financiero BHD**	En cuanto al numeral 5c: Los incidentes de seguridad son considerados confidenciales y no son divulgados a empleados y proveedores por tanto sugerimos eliminar este acápite. Ejemplos de estos pudieran considerarse como material de concientización, si aplica. La gestión de software malicioso tiene mayores alcances, ¿qué sucede con iniciativas de microsegmentación, separación de ambientes, autenticación con MFA en plataformas de infraestructura, respaldos, recuperación de información, respaldos fuera de línea, gestión de estos?		
Art. 11 numeral 6 (Perla)	**CEVALDOM, S.A.**	Se recomienda delimitar el alcance, ya que cualquier dispositivo es muy amplio y las herramientas de protección contra malware solo son compatibles con ciertos sistemas operativos	Principio de Seguridad jurídica, de previsibilidad y certeza normativa Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	
Art. 11 numeral 8	**CEVALDOM, S.A.**	Se recomienda cambiar 'dispositivos de computación personal" por 'dispositivos finales', ya que estos últimos abarcan tanto los dispositivos personales como los asignados por la empresa.	Claridad del requerimiento	
Art. 12	**Centro Financiero BHD**	En cuanto al numeral 1 b: La segmentación de redes es parte vital de la naturaleza de las redes		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		y se encuentra considerada en el acápite a de este artículo, consideramos oportuno desestimarlo.		
Art. 12 numeral 2, literal a	**CEVALDOM, S.A.**	Se sugiere quitar " con direcciones MAC desconocidas", ya que existen diferentes maneras de bloquear el acceso y no solo por MAC ADDRESS.	Claridad del requerimiento	
Art. 12 numeral 2, literal b, numeral V	**CEVALDOM, S.A.**	Se sugiere agregar la palabra, "según aplique".	Mejorar la claridad de la información requerida. Principio de Seguridad jurídica, de previsibilidad y certeza normativa Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	
Art. 12, numeral 1, inciso b)	**ADOSAFI**	Gestión de la red. En adición a lo establecido en el artículo 38 (Gestión de la Red) del Reglamento, la configuración de dispositivos de la red y la gestión de red física del Participante del Mercado de Valores debe considerar lo siguiente: 1) Configuración de dispositivos de la red: los controles que se deben considerar de manera enunciativa, pero no limitativa, son: a) Dispositivos de red configurados de acuerdo con las prácticas estándar y conocidas de administración de la seguridad de dichos dispositivos y los principios de arquitectura de Seguridad Cibernética y de la Información; ~~b) Procedimiento para la segmentación entre redes con distintos niveles de seguridad;~~	Entendemos que la segmentación de redes es parte vital de la naturaleza de las redes y se encuentra considerada en el acápite a de este artículo, consideramos oportuno desestimarlo.	
Art. 13	**ADOSAFI**	~~**Comunicaciones electrónicas.** Las comunicaciones electrónicas incluyen los servicios de comunicación de voz, cuyos procedimientos deben contemplar:~~	Favor considerar que la mayoría (sino todos) proveedores actuales disponibles de telefonía en el país no cumplen con el cifrado de tráfico de voz.	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		~~1) Solicitud, aprobación y revocación de acceso al servicio;~~ ~~2) Términos y condiciones de uso de los servicios;~~ ~~3) Mecanismos de registro y autenticación de los usuarios,~~ ~~4) Configuraciones de seguridad conforme al Marco de Trabajo elegido por el participante del mercado de valores; y,~~ ~~Definición de controles específicos para estos servicios, tales como, el despliegue de herramientas de monitoreo, instalación de componentes de resiliencia y redundancia, segregación y cifrado del tráfico de voz del resto del tráfico de red utilizando VLAN, esquema de gestión de Vulnerabilidades, aplicación de correctivos y actualizaciones de Software, cifrado del tráfico de voz, registro de eventos, así como, la protección de los buzones de voz contra el Acceso no autorizado.~~	Favor verificar porque consideramos que la comunicación de voz no forma parte de las comunicaciones electrónicas.	
Art. 14	**Bolsa y Mercados de Valores de la República Dominicana, S. A. (BVRD)**	Respecto al artículo 14, numeral 2) sobre requisitos de seguridad a los proveedores externos, en su literal c), recomendamos la inclusión de las disposiciones para considerar a cuáles proveedores aplicará lo siguiente: "c) Obligar al proveedor de entregar periódicamente un informe sobre la efectividad de los controles y el acuerdo sobre la corrección oportuna de las cuestiones pertinentes planteadas en el mismo". Es importante señalar que no todos los proveedores tienen la misma naturaleza y pudiera ser insostenible para algunos poder cumplir con un reporte de cumplimiento de controles realizado por un tercero. En este sentido, sugerimos que dicho requerimiento	Artículo 3, numeral 9 de la Ley 107-13, Principio de Proporcionalidad.	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		pueda ser solicitado a proveedores que el participante considere como críticos, tomando en cuenta la sensibilidad de la información que se maneja en el servicio prestado por el proveedor. De conformidad con lo referido, sugerimos considerar incluir la aclaración que se establece en el Reglamento de Seguridad Cibernética y de la Información en el Mercado de Valores, revisado en consulta pública, el cual dispone en el párrafo del artículo 41 lo siguiente: "En los casos que los servicios provistos consideren Información financiera u otro tipo de Información sensible, los participantes del mercado de valores deben solicitar a la entidad proveedora una evaluación enfocada en los Riesgos de Integridad, disponibilidad y Confidencialidad. Dicha evaluación debe ser realizada por un tercero independiente utilizando modelos de reportes de Riesgo y controles en la provisión de servicio (Tal como: SOC 2, etc., u otras que puedan aplicar conforme a la naturaleza del servicio contratado)". En tal sentido, recomendamos establecer la misma disposición en el instructivo, con la finalidad de que dicho informe aplique en los casos de los servicios provistos que cumplan con las condiciones de proveedor crítico (que los servicios provistos consideren Información financiera u otro tipo de Información sensible), como se establece el referido reglamento de consulta pública, a fin de que esto sea sostenible para los participantes y sus proveedores, así como también, evitar generar confusión en el cumplimiento y aplicación de ambos documentos		
Art. 14	**Centro Financiero BHD**	Reconsiderar la obligatoriedad de los puntos 2a, 2c y 4e.		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		Sugerimos que el requerimiento contemplado en el numeral 4e se puede exigir para los proveedores de servicios tercerizados materiales.		
Art. 14	**ADOSAFI**	Tal como indicamos en nuestros comentarios sobre el proyecto de Reglamento, se debe hacer una revisión y categorización de a cuáles proveedores aplica cada obligación 1. a) iii. Selección de proveedores acreditados~~,~~ y fiables ~~y homologados que deberán estar registrados en una Base de Datos de proveedores, categorizando los mismos desde la perspectiva de Seguridad Cibernética y de la Información;~~ 1. v. Asistencia a los comités de adquisiciones en los procesos de negociaciones de los contratos, incorporando los requisitos de Seguridad Cibernética y de la Información de los mismos; 2) Requisitos de seguridad a los proveedores externos: Dentro de los requisitos de seguridad que los Participantes del Mercado de Valores deben efectuar se encuentran los siguientes: 2. a) Revisar los aspectos de Seguridad Cibernética y de la Información de las	No existe una base de datos de proveedores en el país y es importante pensar en caso de crearla cuál autoridad con capacidad es la que determinaría si son fiables para las necesidades de nuestro mercado. Se debe especificar a qué se refiere a los comités de adquisiciones y quién estaría asistiendo. Creemos que esta debería ser una atribución del Subcomité Funcional de Seguridad Cibernética y de la Información bajo la dependencia del Comité de Riesgos conforme propuesta realizada en el proyecto de Reglamento. Sugerimos que el numeral 2) se limite sólo a proveedores externos de servicios críticos, conforme se defina en el Programa de Seguridad Cibernética y de la Información de cada Participante del Mercado de Valores. Esta obligación se debe limitar solo a los proveedores relacionados al Participante. Este requisito debería delimitarse sólo para proveedores de servicios críticos.	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		relaciones del proveedor ~~con sus propios proveedores~~ 2. b) Validar que el proveedor mantiene la suficiente capacidad de servicio junto con los planes realizables diseñados para asegurar que los niveles de continuidad de servicio acordados se mantienen después de fallas o desastres importantes; y, 2. c) ~~Obligar~~ **Solicitar** al proveedor ~~de~~ entregar periódicamente un informe sobre la efectividad de los controles y el acuerdo sobre la corrección oportuna de las cuestiones pertinentes planteadas en el mismo. 3) Adquisición o arrendamiento de equipos y sistemas tecnológicos: El proceso de adquisición o arrendamiento de equipos y sistemas tecnológicos debe basarse en guías de referencia para la selección y aprobación de proveedores de equipos, aplicaciones y servicios, así como prever los requerimientos técnicos de seguridad aprobados por el Subcomité Funcional de Seguridad Cibernética ~~comité funcional de Seguridad Cibernética y de la Información~~ o por el órgano correspondiente, asegurando que estos brinden la funcionalidad requerida y no comprometan la Seguridad Cibernética y de la Información sensible del Participante del Mercado de Valores durante su ciclo de vida; y,	Es posible tratar de establecer los mecanismos para que el proveedor se comprometa a entregar este informe, pero es imposible obligarlo. Sugerimos que en vez de crear un Comité Funcional de Seguridad Cibernética y de la Información, se cree un Subcomité Funcional de Seguridad Cibernética y de la Información bajo la dependencia del Comité de Riesgos. Sugerimos delimitar esas obligaciones por tipo de proveedor y, por tanto, el tipo de obligación aplicable. Solicitamos cambiar la redacción porque seguramente muchos	

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		4) Inclusión de aspectos de Seguridad Cibernética y de la Información en los contratos con proveedores de servicios, especificando lo siguiente: (…) 4. e) Derechos a ~~auditar~~ solicitar detalle de los procesos y controles de los proveedores relacionados con el acuerdo.	proveedores, especialmente aquellos más robustos y con mayor reputación, difícilmente permitirán este tipo de auditorías.	
Art. 14, numeral 1, literal a, literal iii	**CEVALDOM, S.A.**	Se requiere la selección de "Proveedores acreditados, fiables y homologados", términos todos jurídicamente no definidos y que se prestan a interpretación. No todos los proveedores estarán acreditados ante un organismo y no queda claro qué quiere decir la noma con homologado (¿ante quién o en base a qué?). La selección de los proveedores debe ser realizadas tomando en consideración el resultado del correspondiente análisis de riesgos, el cual es el que, en definitiva, en base a los riesgos identificados sobre el servicio a tercerizar, va a servir de orientación respecto a los requisitos que debe cumplir el proveedor y los controles a ser exigidos.	Principio de Seguridad jurídica, de previsibilidad y certeza normativa Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	
Art. 14, numeral 2, literal c	**CEVALDOM, S.A.**	Se sugiere delimitar el tipo de proveedores a los que se les hará exigible estos requisitos. Ejemplo: aquellos con los que se mantiene interconexión.	Principio de Seguridad jurídica, de previsibilidad y certeza normativa	
Art. 14, numeral 4, literal d	**CEVALDOM, S.A.**	Se sugiere revisar redacción y especificar los casos en los que aplicaría basado en un análisis de riesgos. En este sentido se recomienda agregar "según aplique".	Principio de Seguridad jurídica, de previsibilidad y certeza normativa Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	
Art. 15	**Centro Financiero BHD**	En cuanto al numeral 15.2: Favor aclarar cuál será el método de comunicación para la		

Título, Capítulo, Artículo	Institución	Observaciones	Base legal o fundamento	RESPUESTA OP/DRI
		realización de auditorías y ejercicios de identificación de vulnerabilidades. En cuanto al numeral 15.3: Solicitamos identificar cuáles serán las herramientas a utilizar para llevar a cabo los ejercicios de identificación de vulnerabilidades. Tomar en cuenta lo previsto en la normativa de ciberseguridad emitida por la Junta Monetaria.		
Art. 15, numeral 1, literal b, literal ii	**CEVALDOM, S.A.**	Recomendamos sustituir el literal ii por el requisito de realizar pruebas de vulnerabilidades sobre el código. Estas pruebas pueden ser realizadas por personas o de forma automática a través de aplicaciones especiales.	El documento limita la revisión a un ser humano, sin considerar que el proceso puede ser realizado de forma automática	
Art. 15, numeral 1, literal b, literal iv	**CEVALDOM, S.A**.	Sugerimos la siguiente redacción: segregación de funciones en los procesos de desarrollo, prueba e implementación.	Claridad en el texto	
Art. 15, numeral 1, literal e	**CEVALDOM, S.A.**	Sugerimos la siguiente redacción: Uso por parte de proveedores externos de desarrollo software de la metodología de desarrollo aprobada por el participante.	Claridad en el texto	
Numeral 3	**CEVALDOM, S.A.**	Recomendamos establecer o aclarar que tales ejercicios serán realizados en coordinación con la entidad y a través de mecanismos apropiados según el tipo de plataforma a ser evaluada, siendo la Superintendencia del Mercado de Valores responsable de las incidencias que puedan surgir de dicho ejercicio	Principio de Seguridad jurídica, de previsibilidad y certeza normativa Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8	