MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Título, Capítulo, Artículo	**Observaciones**	**Base legal o fundamento**
Comentario General	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. Sugerimos especificar los lineamientos y puntos relativos a que los participantes del mercado de valores que son parte de Grupos Financieros en la forma de su aplicabilidad. De acuerdo con el espíritu de este Proyecto de Reglamento el participante podrá optar por uno o varios Marcos de Trabajo conforme a sus requerimientos y necesidades, es relevante que en todos los requisitos y exigencias de la norma se confirme que sólo le aplicarían aquellos conforme al Marco de Trabajo seleccionado.	Considerar que este proyecto de Reglamento de Ciberseguridad del mercado de valores no se solape con la normativa de ciberseguridad de la Junta Monetaria.
Comentario General	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.	Considerar que este proyecto de Reglamento de Ciberseguridad del mercado de valores no se solape con la normativa de ciberseguridad de la Junta Monetaria. En todo caso, considerar establecer prelación según el regulador en cuestión.
Artículo 2	En la medida en la que los Emisores no requieran interconectarse con otros participantes del mercado de valores, sugerimos considerar la posibilidad de no aumentar los requisitos regulatorios que le son aplicables a fin de que las obligaciones que estos conllevan no constituyan un desincentivo para su financiamiento a través del mercado de valores.	Evitar la creación de desincentivos para emitir en el mercado de valores.
Título I, Capítulo I, Art. 2	Considerar hacer una exclusión expresa en este reglamento de las EIFs que funjan como emisores, por encontrarse reguladas bajo el marco del Reglamento de Seguridad Cibernética y de la Información y su instructivo de aplicación, emitidos por la Junta Monetaria y el Banco Central, respectivamente.	Considerar hacer una exclusión expresa en este reglamento de las EIFs que funjan como emisores, por encontrarse reguladas bajo el marco del Reglamento de Seguridad Cibernética y de la Información y su

		instructivo de aplicación, emitidos por la Junta Monetaria y el Banco Central, respectivamente.
Art. 2. Alcance.	9) **Los emisores**, en tanto a los requerimientos mínimos que determine la Superintendencia del Mercado de Valores mediante norma técnica u operativa. **Párrafo II.** Los participantes del mercado de valores que no se encuentren sujetos al sistema de pagos y liquidaci6n de valores…	9) 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. Asimismo, sugerimos que los Emisores en general no estén sujetos a cumplir con todos los requerimientos de un participante ordinario. Al efecto, considerar incluir un articulado especial para emisores particularidades aplicables a estos, no todos los requisitos de carácter general. La regulación debe estar alineada a las normas emitidas por la Junta Monetaria y SIMV. La regulación de su sector deberá prevalecer sobre el presente Reglamento.
Título I Disposiciones Generales Capítulo I Artículo 2 sobre el Alcance Párrafo I.	Se propone ajustar la expresión *"así como el establecimiento de disposiciones relativas al gobierno interno de los participantes del mercado de valores"*, para dotar de mayor precisión el Alcance establecido en el Párrafo I, notando que el gobierno interno de cada participante del mercado de valores sólo está limitado por principios y lineamientos mínimos, en virtud de la Ley 249-17 y su normativa complementaria, por lo que no debe soslayarse la libertad que éstos tienen de decidir sobre la dirección y administración de sus estructuras internas, sin perjuicio de las obligaciones regulatorias que los vinculan como personas jurídicas. En tal virtud, se sugiere indicar "así como lineamientos mínimos que a tales efectos deberán implementar los participantes de mercado de valores".	Artículos 215 y siguientes de la Ley 249-17. Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.
Título I Capítulo I	En el *Artículo 2* respecto al Alcance para el numeral 9) donde refiere a *"Los emisores, en tanto a los requerimientos mínimos que determine la*	Artículo 3 Numeral 4 de la Ley 107-13 Principio de la Racionalidad.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Objeto y Alcance Artículo 2.	*Superintendencia del Mercado de Valores mediante norma técnica u operativa”,* sugerimos que esta norma técnica considere requerimientos mínimos basados en su estructura y que estos requisitos no constituyan cargas muy elevadas para los emisores.	
Artículo 2 sobre el Alcance. Párrafo I	Con el objetivo de contribuir con el cumplimiento, objetividad y coherencia en las obligaciones establecidas en las leyes, reglamentos y normativas aplicables a los participantes del mercado, sugerimos re evaluar el alcance determinado en el Proyecto de Reglamento y la inclusión dentro de este, de los participantes del mercado de valores que, en virtud de su participación en el sistema de pagos y liquidación, ya se encuentran dentro del ámbito de aplicación de la normativa especializada emitida al respecto por la Junta Monetaria. Esto con la finalidad de evitar posibles contradicciones o duplicidades en los contenidos de ambas reglamentaciones.	Ley del Mercado de Valores, párrafo IV del artículo 299. Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.
Art. 2, párrafo I	De conformidad con las disposiciones del párrafo III del artículo 299 de la Ley No. 249-17 del Mercado de Valores, se reconoce que los administradores de sistemas de compensación y liquidación de valores requieren habilitación para operar tanto de la Superintendencia del Mercado de Valores como de la Junta Monetaria, estando obligados en consecuencia a cumplir las disposiciones emanadas de la Junta Monetaria y el Banco Central aplicables a los administradores de sistemas de pagos y de liquidación de valores, y las normas dictadas por el Consejo Nacional del Mercado de Valores y la Superintendencia del Mercado de Valores. En virtud de lo anterior y las disposiciones legales vigente concernientes al Sistema de Pagos de la República Dominicana, CEVALDOM se encuentra obligado al cumplimiento del Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria. Dicho Reglamento establece una serie de requisitos y controles alineados a mejores prácticas que en su conjunto constituyen un estándar de seguridad de primer nivel.	Principio de utilidad y pertinencia, reconocido en el numeral 2 del artículo 4 de la Ley 167-2021. Ley 249-17: artículo 299 Principio de Racionalidad aplicable a las actuaciones de la Administración Pública

	El Proyecto de Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores (en lo adelante, el "Proyecto de Reglamento") incluye controles similares a los contenidos en el Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria, pero aborda algunos controles con un mayor detalle y específicos, incluyendo especificaciones que van más allá del mero requerimiento del control (por ejemplo, se han identificado aspectos adicionales relacionados a controles establecidos en el Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria que el Proyecto de Reglamento determinación varía respecto de: periodicidad de actividades, asignación de responsabilidades a determinados órganos de gobierno, delimitación específica del alcance del control limitándolo su alcance o ampliándolo, extensión de controles a terceros, ampliación de responsabilidades del Consejo de Administración, cambios en la estructura organizacional, entre otros). De conformidad con el párrafo I del artículo 2 del Proyecto de Reglamento se establece que "*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*". En este sentido, en virtud de lo indicado en el párrafo anterior, los participantes del mercado obligados al cumplimiento del Reglamento de Seguridad Cibernética y de la Información que ya han implementado los controles requeridos por dicho reglamento, determinando su alcance o forma de aplicación en base a una evaluación de riesgos, se verán obligados a modificar lo ya implementado para cumplir con las especificaciones supletorias incorporadas en el Proyecto de Reglamento para el mismo control, lo cual implica un esfuerzo adicional para el participante, sin que se considere el costo de haber implementado el control ni la efectividad de dicho control. Sobre el particular, consideramos que el alcance de los controles establecidos en el Reglamento de Seguridad Cibernética y de la Información cumplen con estándares internacionales y que los costos de implementar cambios en tales	

	controles para cumplir con especificaciones adicionales relativas al mismo control superan los beneficios de la regulación, no justificando la consecución de los objetivos de política pública perseguidos. Por otro lado, cabe destacar que existe el riesgo de disposiciones regulatorias contradictorias o no compatibles, producto de modificaciones futuras (incluyendo la posible contradicción respecto a instructivos de desarrollo que pudieran ser dictados por el BCRD). En virtud de lo anterior, muy respetuosamente y tomando en consideración que la propia ley del mercado de valores, en los párrafos III y IV del artículo 299, reconoce que ciertos participantes deben sujetarse a las normas y procedimientos que la Junta Monetaria determine, incluyendo el Reglamento de Seguridad Cibernética y de la Información, tenemos a bien proponer lo siguiente: i. Excluir del alcance del Proyecto de Reglamento a los participantes del mercado que, en su calidad de participantes del Sistema de Pagos de la República Dominicana o de administradores de sistemas de compensación y liquidación de valores, se encuentren obligados al cumplimiento del Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria, estableciendo que dichos participantes deberán cumplir solamente con las disposiciones de un capítulo especial del propio Proyecto de Reglamento cuyo alcance indicaremos a continuación. ii. Establecer la obligación a cargo de los participantes sujetos al Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria de entregar a la SIMV un ejemplar del informe de auditoría independiente exigido por dicho reglamento. iii. Indicar que los participantes sujetos al Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria se encuentran sometidos a la supervisión de la SIMV en el cumplimiento de dicho Reglamento, pudiendo dicha entidad exigir su cumplimiento	

	y sancionar su inobservancia (esto último en coordinación con el BCRD a fin de evitar duplicidad de sanciones por el mismo hecho). iv. Establecer cualquier control o requisito puntual adicional, no contemplado en el Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria, el cual la Superintendencia del Mercado de Valores considere que debe ser exigido a los participantes del mercado de valores.	
Art. 2, párrafo II	En base a las disposiciones del Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria, a la fecha los participantes del sistema de pagos y administradores de sistemas de compensación y liquidación envían al Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) reportes de incidentes, pero no de vulnerabilidades. En este sentido, recomendamos revisar la redacción de esta disposición.	Artículo 52 del Reglamento de Seguridad Cibernética y de la Información dictado por la JM
Artículo 2, Párrafo II	**Párrafo II.** Los participantes del mercado de valores que no se encuentren sujetos al sistema de pagos y liquidación de valores, podrán remitir los requerimientos relativos a incidentes y Vulnerabilidades al ~~Centro Sectorial de Respuesta a Incidentes de Ciberseguridad para el Sistema Financiero y de Pagos (SPRICS~~) **Equipo de Respuesta a incidentes de Seguridad Cibernética para el Sector Financiero (CSIRT) bajo la dependencia administrativa del Banco Central y funcional del Consejo Sectorial**, de conformidad a lo establecido en el Reglamento de Seguridad Cibernética y de la Información emitido por la Junta Monetaria.	Sugerimos utilizar el mismo nombre del Artículo 52 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria, para evitar confusión. Adicionalmente, favor aclarar bajo qué modelo o esquema se estaría reportando.
Art. 3. Definiciones.	Incluir otras definiciones.	También sugerimos incluir en el capítulo de DEFINICIONES los siguientes términos relativos a la información: • Privilegiada • Reservada • Confidencial
Artículo 3	**Se recomienda insertar las siguientes definiciones extraídas del Reglamento de Seguridad Cibernética del Banco Central:**	Más claridad y mayor armonización con otros reglamentos del sistema financiero dominicano.

	Apetito de Riesgo: Es el límite agregado en función de los tipos de riesgos que el Consejo de Administración y la Alta Gerencia están dispuestos a asumir y gestionar para cumplir sus objetivos de negocios; Ataque: Intento de obtener acceso no autorizado a los sistemas, sus recursos, servicios o información, o de comprometer la integridad de los mismos. Comprende 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; Sistema de Información: Conjunto de activos de información utilizado para obtener, almacenar, manipular, administrar, controlar, procesar, transmitir y/o recibir datos, con el objetivo de satisfacer una necesidad de información; Información privilegiada: Es la información referida a uno o varios participantes del mercado, a sus negocios, a sus valores de oferta pública o al mercado que pudiera afectar su posición jurídica, económica o financiera, cuando no sea de dominio público. Información Reservada: Es la información privilegiada que se encuentra fuera del acceso público, debido a que su difusión puede poner en riesgo la estabilidad o seguridad financiera del mercado de valores o sus participantes. Información Confidencial: Es la información que por su naturaleza o posible impacto debe ser manejada con estricta discreción, por parte de los Miembros del Consejo Nacional del Mercado de Valores, los funcionarios y el personal de la Superintendencia **Asimismo, se recomienda insertar definiciones relativas a los siguientes términos:** **Información Sensible**	

	Activos de Tecnologías y de la Información **Disponibilidad de Entorno**	
Art. 3. Definiciones.	Incluir otras definiciones.	También sugerimos incluir en el capítulo de DEFINICIONES los siguientes términos relativos a la información: • Privilegiada • Reservada • Confidencial Igualmente, entendemos oportuno referir u homologar definiciones conforme la Ley de Mercado de Valores o el Reglamento de Información Privilegiada, Confidencial o Reservada. Tales como, los conceptos de privilegiado y confidencial. O en su defecto, definir el alcance de estos conceptos desde el contexto de esta materia, ciberseguridad.
Artículo 3 sobre Definiciones.	1. En el numeral 2 sugerimos modificar la definición de amenaza incluyendo que una amenaza puede tener causas naturales, ser accidental o intencionada. 2. Sugerimos la modificación del término "*hardware*" en el numeral 18, de manera que en lo adelante se incluya lo sobresaltado: "*conjunto de equipos físicos que componen una computadora**, sistema o infraestructura tecnológica***". 3. En lo concerniente a los numerales 22 y 23 que definen los términos "Incidente" e "Incidentes Cibernéticos y de la Información" llamamos a su atención que el Reglamento tiene como propósito establecer prácticas para la gestión de riesgos de seguridad cibernética, por lo que, para mayor precisión y conformidad al	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.

	alcance de la normativa, se propone enunciar que los procedimientos dispuestos en el mismo atañen a la ocurrencia de "Incidentes Cibernéticos y de la Información". Por consiguiente, en línea al objeto del Reglamento, toda referencia a "Incidente" ha de aludir a la definición de "Incidentes Cibernéticos y de la Información". De igual modo, se sugiere armonizar en toda la normativa el uso del término "Incidentes Cibernéticos y de la Información" o establecer su equivalencia a "Incidentes de Seguridad Cibernética y de la Información" que es utilizado en varias ocasiones en la propuesta reglamentaria. 4. En el numeral 43), sugerimos reformular la definición de "Problema", bajo el entendido de que la causa de un problema pudiera ser determinable y por lo tanto no necesariamente tendría que ser desconocida. Asimismo, atendiendo al alcance del Reglamento, proponemos delimitar que el tipo de Incidente que abarca el Problema, es un incidente de índole cibernético y de la información, con el propósito de agregar mayor precisión a la obligación que tienen los participantes de establecer procedimientos para responder a problemas o incidentes de seguridad cibernética y de la Información (y tal como detalla el artículo 33 de la propuesta de Reglamento). 5. En el numeral 46), en la definición de "Riesgo", recomendamos remplazar la redacción actual para que en lo adelante se lea "*afectar negativamente la correcta operación"* partiendo de que el objetivo de la disposición es salvaguardar el correcto funcionamiento del mercado.	
Art. 3, numeral 2	Se recomienda agregar la definición de "Activos de Información": Bien tangible o intangible, que almacena, procesa y/o transmite información.	Término utilizado por estándares en la materia que permitiría hacer referencia a distintos componentes de la infraestructura utilizando un solo término o palabra.
Art. 3, numeral 3	Recomendamos ajustar el texto para aportar mayor claridad:	Aportar mayor claridad al texto.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

	Base de Datos: Serie de datos organizados relacionados entre sí, almacenados en los sistemas de información del participante del mercado de valores o de un proveedor de éste, en caso de tercerización o licenciamiento de la infraestructura tecnológica.	Entre las principales características de las bases de datos se encuentra que los datos sean almacenados, la referencia al intercambio de información o conexión sin hacer alusión a almacenamiento puede conllevar confusión debido a que si la conexión es únicamente como medio o canal de comunicación el dato no se almacena y no habría base de datos.
Art. 3, numeral 7	Se recomienda ajustar la definición debido a que la información, a pesar de ser confidencial podría ser compartida con terceros sin autorización del titular en una diversidad de escenarios como, por ejemplo, el cumplimiento de una obligación legal (entrega de información confidencial a la SIMV, en virtud de una orden judicial, a un embargante en posesión de un título ejecutorio, a la UAF, etc). A continuación, propuesta de redacción: "Preservación de la información de forma que la misma sólo pueda ser accedida por las personas o sistemas autorizados".	Evitar incluir definiciones con un alcance limitado que al ser utilizados en el contexto normativo generen obligaciones de imposible cumplimiento o que requieran de aclaraciones en cada caso.
	13) Entidad Interconectada: Persona jurídica habilitada mediante una relación contractual para mantener una conexión electrónica **que implique un flujo periódico y automático de Información Esencial**. ~~o intercambio de Información con un participante del mercado de valores.~~	A fin de homogeneizar con el Artículo 9, Proyecto de Reglamento sobre Seguridad Cibernética y de la Información en el Mercado de Valores, sugerimos especificar el tipo de información.
	17) Gestión de Riesgo ~~Tecnológico~~: Método para determinar, analizar, valorar y clasificar el Riesgo con el objeto de implementar mecanismos que permitan controlarlo.	Sugerimos eliminar la palabra "Tecnológico", ya que entendemos que la definición incluye la gestión de riesgo en todas las áreas de la entidad, y no se limita a la gestión de riesgo tecnológico.
Art. 3, numeral 17	De acuerdo con los estándares y mejores prácticas internacionales, el riesgo puede ser aceptado, mitigado (controlado), transferido, aceptado o eliminado.	Entre los estándares que pueden ser citados se encuentran el ISO 31000:2018 sobre Gestión de Riesgos (cláusula 6.5).

	En este sentido, se recomienda sustituir el término “controlarlo” por “gestionarlo”.	
Art. 3, numeral 23	Se recomienda cambiar la redacción a: "Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la confidencialidad, integridad o disponibilidad de la información". Pues las consecuencias de un incidente de este tipo pueden ser muchas más de las que se mencionan en la definición.	Las consecuencias de un incidente de seguridad de información pueden extenderse a escenarios no contemplados en el enunciado, siendo limitativa.
Art. 3, numeral 24	Se sugiere eliminar palabra "similares" o incluir de forma expresa la representación material (por ejemplo en papel), ya que la redacción actual puede dar la impresión de que sólo se refiere a aquella almacenada en medios electrónicos o digitales, excluyendo los datos gestionados de forma física.	Aportar claridad y precisión al texto, evitando errores o diversidad de interpretación.
	24) Información: ~~Cualquier forma de registro~~ **Conjunto de datos** electrónicos, óptico, magnético u otros medios similares, susceptible de ser procesada, distribuida y almacenada.	- Ley 172-13 - tt) y uu), artículo 5, Reglamento de Seguridad Cibernética (2018) La definición de “Información” es muy amplia pudiendo abarcar todo tipo de datos manejados por el participante. Dependiendo el tipo de información hay obligaciones más rigurosas respecto a su recolección y tratamiento. Se recomienda distinguir por su tipo de contenido y nivel de acceso. Por igual, se recomienda homogeneizar definición a los tipos de informaciones que se definen en este artículo, los cuales refieren a esto como “Conjunto de datos” no “archivos”.
Art. 3, numeral 35	Recomendamos ajustar la definición con el objetivo de aportar mayor claridad y evitar diversidad de interpretaciones al momento de utilizar el término	Aportar claridad y precisión al texto, evitando errores o diversidad de interpretación.

	definido en el contexto de las obligaciones consideradas en el Proyecto de Reglamento. Sugerimos el siguiente texto: "Se refiere al o los estándares de referencia adoptados por el participante con el objetivo de gestionar los riesgos de seguridad de la información, sin que dicha adopción considere necesariamente la implementación de todos los controles o elementos de tales estándares, tales como BSA, CIS, CMMI, COBIT, COSO, GDPR, IAPP, ISF, ISO 9001, ISO 2000, ISO 27001, ISO 27002, ISO 31000, IEC, ITIL, NIST, OWASP, PMBOK, SWIFT, entre otros reconocidos internacionalmente.	
Art. 3, numeral 43	Recomendamos ajustar la definición de Problema a la siguiente: Es la causa conocida o desconocida de un incidente.	La causa del problema puede ser conocida y aún no contar con solución.
Título II, Capítulo I	Sugerimos cambiar el título a: **CAPÍTULO I** **"Programa de Seguridad Cibernética y de la Información"**	Este capítulo se refiere al Programa de Seguridad Cibernética y de la Información, por lo que se recomienda refiera a esto el titular.
Artículo 4	Recomendamos el siguiente cambio: **Artículo 4. Programa de Seguridad Cibernética y de la Información.** 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.	Ver justificación anterior.
Artículo 4	Entendemos que la adopción de un estándar por parte de un participante debe ser potestativa y no obligatoria, puesto que su programa de seguridad de la información puede encontrarse basado en el cumplimiento de los requerimientos y controles contemplados en el Proyecto de Reglamento. Por	Definición de marco de trabajo. Principio de Racionalidad aplicable a las actuaciones de la Administración Pública

	la redacción del artículo parecería que la adopción de uno o varios estándares (ver definición de marco de trabajo contenida en el actual Proyecto de Reglamento) es obligatoria. En este sentido, sugerimos la siguiente redacción: "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, pudiendo además optar por uno o varios marcos de trabajo conforme a sus requerimientos y necesidades".	
Articulo 4, Párrafo I.	Sugerimos aclarar bajo qué criterios se determina la complejidad, tamaño y perfil de riesgo del participante dado que se señala que: **Párrafo I.** El programa de Seguridad Cibernética y de la Información requerido en este Reglamento debe ser diseñado de acuerdo con la naturaleza, tamaño, complejidad y perfil de Riesgos del negocio de cada participante del mercado de valores.	Claridad y homologación de condiciones.
Artículo 4 sobre Marco de Trabajo. párrafo II	En el párrafo II, sugerimos incluir en la última oración lo siguiente: "(…) *impacto financiero, humano y reputacional <u>previsible</u> sobre el participante del mercado de valores"*. Esto a fines de proveer mayor exactitud al alcance de las gestiones que son puestas a cargo de los participantes. Igualmente, apreciamos un error ortográfico en el párrafo III, numeral 3), donde se incorpora la práctica identificada con el literal d), debiéndose mostrar con un numeral adicional (4).	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.
Artículo 4 sobre Marco de Trabajo. párrafo III	Es importante señalar que los requerimientos que sean determinados para los emisores de valores, se encuentren basados en su estructura y que estos requisitos no constituyan cargas muy elevadas para estos, con el objetivo de no incrementar las exigencias para este tipo de participantes del mercado, toda vez que los mismos no requiera n interconectarse con los sistemas de los demás participantes del mercado.	Artículo 3 Numeral 4 de la Ley 107-13 Principio de la Racionalidad.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Articulo 4, Párrafo III.	**Sugerimos revisar numeración:** **“Párrafo III.** (…) 3) Identificar marcos y estándares para abordar la ciberseguridad; ~~**d.**~~ **4) Utilizar métricas y umbrales para informar los procesos de gobernanza**; y, ~~4)~~ 5) Realizar evaluaciones internas de Riesgos de ciberseguridad.”	Comentario de forma. Tabular numerales incluyendo la práctica arriba resaltada.
Título II, Capítulo I, Art. 4, Párrafo 3. Capítulo VI, Art. 46. **Título III, Capítulo I, Art. 54, Párrafo 3.**	Ver comentario anterior al respecto, incluir una exclusión expresa en este sentido, es decir, de remitir para no objeción de la SIMV, esta documentación, debido a que para las EIFs lo relacionado con seguridad cibernética y de la información se encuentra contemplado en normativas supervisadas por el Banco Central.	
Art. 4, párrafo III	En la medida en la que los Emisores no requieran interconectarse con otros participantes del mercado de valores, sugerimos considerar la posibilidad de no aumentar los requisitos regulatorios que le son aplicables a fin de que las obligaciones que estos conllevan no constituyan un desincentivo para su financiamiento a través del mercado de valores. En caso de mantener obligación, aclarar si estas disposiciones son aplicables a los emisores diferenciados. Asimismo, aclarar si los criterios de información del artículo 5 tienen por objetivo garantizar la seguridad de la información dirigida a los inversionistas y que debe ser entregada a la SIMV o si el alcance aplica a la seguridad de la información del negocio o actividad del emisor.	Evitar la creación de desincentivos para emitir en el mercado de valores.
Art. 4 Párrafo III.	Párrafo III. Los Emisores deben adoptar un marco de gobernanza de ciberseguridad **especial.**	1.No se especifica el significado de especial, no se hace mayor referencia a las características del Marco, es un tema interpretativo, asimismo, especificar los puntos relativos a PB que son parte de Grupos o Centros Financieros en la forma de su aplicabilidad; 2. Somos de una opinión que existen emisores de valores que no pertenecen a grupos financieros o participantes del

		mercado de valores, por lo que su empresa y objeto de la misma no debe adherirse a estos requerimientos regulatorios. Asimismo, es importante reconocer que el incentivo de la ley de mercado, asi como la ley de fomento de acciones, tiene como finalidad motivar a las empresas a utilizar como recurso de capitalización y financiamiento el mercado de valores. De por sí, ya los emisores tienen la obligación de cumplir con una serie de requerimientos regulatorios, lo cual asume un costo significante para la empresa, por lo que no es necesario aplicar mas regulaciones que no contribuyen, desde su sector, al inversionista, como es la aplicación de una gobernanza ciberseguridad especial; 3. Contemplar los lineamientos para Entidades que son del Centro Financieros.
Art. 4 Párrafo III.	Párrafo III. Los Emisores deben adoptar un marco de gobernanza de ciberseguridad **especial.**	No se especifica el significado de especial, no se hace mayor referencia a las características del Marco, es un tema interpretativo, asimismo, especificar los puntos relativos a que los participantes del mercado de valores que son parte de Grupos Financieros en la forma de su aplicabilidad 2. Contemplar los lineamientos para Entidades que son del Grupos Financieros.
Art. 4 Marco de Trabajo Párrafo III.	Realización de evaluaciones internas	No especifica si debe de hacerse bajo el modelo de las 3 líneas de defensa, es decir, si es una función de la segunda y/o tercera línea, así como no define la participación del equipo de auditoría externa o un tercero que apoye en esta función. Difiere con artículo 3 sobre el alcance, establece requerimientos adicionales como la obtención de su no objeción en cuanto al marco de ciberseguridad.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 4 Marco de Trabajo Párrafo III.	Realización de evaluaciones internas	No especifica si debe de hacerse bajo el modelo de las 3 líneas de defensa, es decir, si es una función de la segunda y/o tercera línea, así como no define la participación del equipo de auditoría externa o un tercero que apoye en esta función.
Artículo 5 sobre Criterios de Información.	1. En el numeral 5) se establece que "*los recursos y la Información deben estar disponibles en el tiempo y la forma requerida por los* <u>*usuarios*</u> *o las autoridades competentes en el ejercicio de sus facultades legales"*. Recomendamos modificar esta redacción para que en lo adelante rece de la manera siguiente: "*los recursos y la Información deben estar disponibles* <u>*a los usuarios*</u> *en el tiempo y la forma requerida por las autoridades competentes, conforme los plazos razonables establecidos en el ejercicio de las facultades legales otorgadas según el caso"*. Lo anterior, en vista de que los usuarios no tendrían facultades para imponer plazos a los participantes en la entrega de información y recursos.	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.
Artículo 6 sobre Responsabilidades en materia de seguridad.	1. En lo concerniente al numeral 2) se propone revisar la formalidad de que las políticas y procedimientos en la especie deban ser aprobadas por el consejo de administración. Como se apunta "ut supra", la dirección y organización interna corresponde a cada entidad, según sus disposiciones estatutarias, sin perjuicio de los lineamientos mínimos que establece la Ley en cuanto al gobierno de los participantes del mercado de valores y notándose que en ese tenor la Ley 249-17 no otorga facultad exclusiva al Consejo de Administración para la adopción de políticas en esta índole. Por ello, debe reservarse a los participantes la facultad de decidir el órgano que, de conformidad con sus Estatutos Sociales, tendrá por aprobar tales procedimientos. *2.* En el numeral 10), a fin de garantizar la proporcionalidad de la obligación que recae en el participante del mercado de valores, en lo que respecta a	Artículos 216 y siguientes de la Ley 249-17. Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.

	las capacitaciones, se sugiere modificar la expresión a fin de que la responsabilidad del participante del mercado de valores rece de la forma siguiente: *"Orientar cuando corresponda, capacitar a sus empleados sobre la forma de interconectar con la Superintendencia"*.	
Artículo 6	Sugerimos la siguiente redacción: **"Artículo 6. Responsabilidades en materia de seguridad.** A los efectos del presente Reglamento, es responsabilidad de los participantes del mercado de valores: 1) Establecer y mantener actualizado un sistema de gestión que proporcione un enfoque estándar, formal y continuo para la Seguridad Cibernética y de la Información y procesos del negocio; 2) Definir políticas y Procedimientos para la Seguridad Cibernética y de la Información conforme **al Marco de Trabajo elegido por el participante del mercado de valores** ~~**Mejores Prácticas**~~. Dichas políticas y Procedimientos deben procurar que la ejecución de los criterios de control interno relativos a eficacia, eficiencia y cumplimiento se encuentren alineados a los objetivos y las actividades del participante del mercado de valores. Las políticas y Procedimientos en la materia deben ser aprobadas por el consejo de administración; 3) Asegurar la Integridad, Confidencialidad y disponibilidad de la Información almacenada en sus sistemas y de la Información en tránsito, almacenada y procesada, **cuando aplique;** 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, **conforme haya sido seleccionado**	Sugerencia conforme a lo definido en esta Proyecto de Resolución Aclarar la diferencia entre la obligación desarrollada en el numeral 3 y el 4. De acuerdo con el Artículo 4, el participante podrá optar por uno o varios Marcos de Trabajo conforme a sus requerimientos y necesidades, confirmar que sólo le aplicarían aquellos seleccionados.

	previamente por el participante del mercado de valores. 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**, conforme haya sido seleccionado previamente por el participante del mercado de valores,** 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 y resultados de las autoevaluaciones y mantener evidencia del Monitoreo Continuo realizado; 8) Identificar ~~brechas~~ 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) Capacitar a sus empleados sobre la forma de interconectar con la Superintendencia**, según aplique**; y,	¿Existirá algún lineamiento para las autoevalauciones? Aclarar a qué se refiere con “interconectar”. Dado que los insumos de interconexión dependen de la SIMV, ¿dicha capacitación será apoyada por la SIMV?

	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, **conforme haya sido seleccionado previamente por el participante del mercado de valores**."	
Art. 6. Responsabilidades en materia de seguridad.	En el punto 1 hace referencia a establecer un sistema de gestión, sin embargo, esto no se menciona en ninguna otra parte del documento ni se define, esto genera confusiones ya que en el documento se refieren a la creación de un Programa de Seguridad Cibernética y de la Información, por esto recomendamos que esto sea aclarado en torno a qué se refieren o Sistema de Gestión o que sea eliminado. Adicionalmente, tenemos las siguientes observaciones: 1) Establecer y mantener actualizado un sistema de gestión que proporcione un enfoque estándar, formal y continuo para la Seguridad Cibernética y de la Información y procesos del negocio; 2) Definir políticas y Procedimientos para la Seguridad Cibernética y de la Información conforme a las Mejores Prácticas. Dichas políticas y Procedimientos deben procurar que la ejecución de los criterios de control interno relativos a eficacia, eficiencia y cumplimiento se encuentren alineados a los objetivos y las actividades del participante del mercado de valores. Las políticas y	1. Aclarar si se espera un Plan de trabajo o un Sistema de gestión. 2. Sugiere que las Políticas se apruebe en el Comité de Ciberseguridad, y luego escalado al Consejo de Administración. Y que los procedimientos sean escalados para conocimiento al Comité de Ciberseguridad. 5. Se marco requiere referenciar el estándar internacional que se espera de forma puntual. Evitar ambigüedad en la definición del marco normativo. Abordar los puntos: • Gestión de Vulnerabilidades. • Seguridad de Aplicaciones. • Inteligencia de Amenaza. • Caza de Amenaza y Respuesta a Incidentes (Monitoreo Activo). • Arquitectura de Seguridad y Redes. • Forense Digital. • Análisis de Malware. • Pruebas de Penetración (Pentest). • Gestión de Plan de Recuperación y Desastres (DRP-RTO-RPO 7. ¿Cómo se realizarán las autoevaluaciones?

	Procedimientos en la materia deben ser aprobadas por el consejo de administración; 3) Asegurar la Integridad, Confidencialidad y disponibilidad de la Información almacenada en sus sistemas y de la Información en tránsito, almacenada y procesada; 4) Preservar la Información privilegiada, reservada y confidencial; Página 21 de 55; 5) Gestionar la privacidad de los datos en la forma contemplada en las leyes, normativa vigente aplicable y los Marcos de Trabajo reconocidos internacionalmente sobre la materia. De igual forma, guiar y coordinar la implementación de políticas, Procedimientos y actividades para asegurar que se cumplan las directivas sobre privacidad de los datos; 6) Formular, mantener y ejecutar un plan de tratamiento de Riesgos de Seguridad Cibernética y de la Información alineado con los objetivos estratégicos y operativos del participante del mercado de valores. Dicho plan debe de identificar las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, las responsabilidades y las prioridades asociadas para gestionar los 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 y		8. Se sugiere cambiar la palabra Brecha por Amenazas. 10. Se sugiere aclarar este punto, no se identifica claramente lo que se espera.

	resultados de las autoevaluaciones y mantener evidencia del Monitoreo Continuo realizado; 8) Identificar brechas y Vulnerabilidades de manera periódica; 9) Definir y evaluar las responsabilidades y competencias de sus empleados y de los proveedores de servicios en lo concerniente a la Seguridad Cibernética y de la Información; 10) Capacitar a sus empleados sobre la forma de interconectar con la Superintendencia; y, 11) Establecer, implementar, mantener y monitorear los controles, procesos y Procedimientos de continuidad de negocio o de recuperación que aseguren un nivel aceptable de Seguridad Cibernética y de la Información ante desastres o situaciones adversas	
Art. 6, numeral 2	Según la norma ISO 9001, un procedimiento es un modo específico de llevar a cabo una actividad o proceso. Es decir, cuando un proceso cuenta con unos pasos establecidos y ordenados para obtener un resultado, se llama procedimiento. Los procedimientos nos dicen en cada momento qué pasos hay que seguir. Como puede ser observado, la definición y aprobación de un procedimiento constituye una actividad claramente operativa y que requiere un conocimiento sobre la ejecución paso a paso sobre un proceso o actividad del negocio. Los Principios de Gobierno Corporativo de la OCDE establecen que: “El marco para el gobierno corporativo deberá garantizar la orientación estratégica de la empresa, el control efectivo de la dirección ejecutiva por	Principios de Gobierno Corporativo de la OCDE (principio IV) Guía Práctica de Gobierno Corporativo, Experiencias del Cirulo de Empresas de la Mesa Redonda Latinoamericana Reglamento de Gobierno Corporativo: Artículo 14

	parte del directorio y la responsabilidad de éste frente a la empresa y los accionistas. Las mejores prácticas de gobierno corporativo apuntan hacia una segregación de funciones del consejo de administración y la administración de la sociedad que garantice que el consejo de administración pueda exigir una rendición de cuentas actuando con objetividad. Al respecto, los Principios de Gobierno Corporativo de la OCDE, indican lo siguiente: "*Además de dirigir la estrategia corporativa, el Consejo es principalmente responsable de controlar los resultados de la dirección y ofrecer una rentabilidad adecuada a los accionistas, al tiempo que debe evitar conflictos de intereses y lograr un equilibrio entre las exigencias contrapuestas que afronta la empresa.* ***Para cumplir eficazmente sus responsabilidades, debe poder formular juicios objetivos e independientes.*** […] *Para cumplir su deber de controlar el desempeño de la dirección, evitar los conflictos de intereses y lograr un equilibrio entre las exigencias contrapuestas que se dan en la empresa, es fundamental que el Consejo pueda realizar juicios de valor objetivos. En primer lugar, ello exige independencia y objetividad respecto de la dirección, con importantes consecuencias para la composición y la estructura del Consejo. En estas circunstancias, esta independencia requiere, por lo general, que un número suficiente de consejeros sea ajeno a la dirección."* Por su parte, en su Guía Práctica de Gobierno Corporativo, el IFC indica: *"Además de guiar la estrategia empresarial, el directorio debe supervisar el desempeño gerencial y obtener un rendimiento adecuado para los accionistas, evitando conflictos y equilibrando intereses. Para cumplir con sus responsabilidades eficazmente, el directorio debe poder emitir juicios objetivos e independientes*	

	[…] *La documentación interna de la empresa debe definir y separar claramente las responsabilidades del directorio y de la alta gerencia. El directorio debería dedicarse a las labores de supervisión y los gerentes profesionales a las tareas ejecutivas.”* Como puede ser observado, en base a las mejores prácticas es recomendable que la adecuada separación o segregación de funciones entre el Consejo de Administración y la Administración. De esta forma, se logra un equilibrio que permite un adecuado sistema de rendición de cuentas y el mantenimiento de la objetividad del Consejo. Por otro lado, la exigencia de que el Consejo de Administración se involucre en temas operativos, como lo sería la definición de un procedimiento técnico en materia de seguridad de la información, afecta el régimen de responsabilidad de los miembros del Consejo. En este sentido, la regulación estaría asignando responsabilidades operativas técnicas a personas que carecen de las competencias necesarias para tomar la decisión, haciéndole además responsables de las consecuencias de la decisión adoptada frente a terceros. Lo anterior se encuentra alineado con las disposiciones del artículo 14 del Reglamento de Gobierno Corporativo, el cual reconoce entre las funciones del Consejo de Administración el promover la existencia de una rendición de cuentas efectiva (la cual requiere como bien se establece en los Principios de Gobierno Corporativo de la OCDE la segregación de funciones para mantener la objetividad del Consejo), el aprobar políticas (por definición las políticas constituyen declaraciones de alto nivel que incluyen el compromiso y objetivos de una organización en relación a un tema específico y la estructura o lineamientos para alcanzar dichos objetivos. Las políticas no incluyen la definición de procesos o procedimientos).	

	Cabe destacar el hecho de que el rol del Consejo de Administración de garantizar una adecuada gestión de riesgos es cónsono con lo antes expuesto, no implicando En virtud de lo anterior, tenemos a bien recomendar la eliminación del Proyecto de Reglamento de la asignación de la responsabilidad de aprobar procedimientos.	
Art. 6, numeral 9	En lo que respecta a las exigencias y obligaciones a ser extendidas a los proveedores, tenemos a bien solicitar que las mismas se limiten a proveedores críticos y proveedores que mantengan una interconexión con la infraestructura tecnológica de los participantes. El referirse de forma genérica a proveedores implicaría la aplicación de medidas innecesarias o no proporcionales al servicio prestado, lo cual impactaría negativamente al participante al reducir significativamente las opciones de proveedores elegibles y al establecer tareas de evaluación que requieren un esfuerzo del participante con su correspondiente costo. En este sentido, sugerimos la modificación del numeral 9 del artículo 6 para que se lea: Definir las responsabilidades y obligaciones en materia de Seguridad Cibernética y de la Información de sus empleados y proveedores críticos o aquellos con que mantengan una interconexión con su infraestructura tecnológica, así como definir y evaluar las competencias que en dicha materia sean requeridas para el ejercicio de sus funciones.	Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Principio de utilidad y pertinencia, reconocido en el numeral 2 del artículo 4 de la Ley 167-2021.

Art. 7	Recomendamos que el monitoreo de los riesgos que implica el uso de determinada tecnología sea exigido de forma periódica y no diaria. El monitoreo diario debería ser limitado a las amenazas de seguridad e incidentes. El monitoreo de riesgos y la actualización de los correspondientes perfiles y matrices de riesgos es realizado usualmente con una periodicidad mínima anual o cuando ocurren cambios en el contexto de la organización, en base a mejores prácticas. En este sentido, sugerimos la siguiente redacción: "Los participantes del mercado deben monitorear de manera periódica los riesgos que implican el uso de la tecnología de la información, contemplado todo su ciclo de vida."	
Artículo 7 sobre Gestión de Riesgos Tecnológicos	El artículo 7, sobre Gestión de Riesgos Tecnológicos, donde indica *"Los participantes del mercado de valores deben monitorear diariamente los Riesgos que implica el uso actual y futuro de la Tecnología"* la periodicidad indicada como "diaria" sea modificada por "periódica", tomando en cuenta que el monitoreo a los diferentes riesgos se realiza por los distintas metodologías y tecnología o herramientas. El monitoreo diario debería ser limitado a las amenazas de seguridad e incidentes que estas cuentan con herramientas que apoyan este proceso, sin embargo, el monitoreo de riesgos y la actualización de los correspondientes perfiles y matrices de riesgos es realizado usualmente con una periodicidad mínima anual o cuando ocurren cambios en el contexto de la organización, en base a mejores prácticas.	Artículo 3 Numeral 4 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 7	**Artículo 7. Gestión de Riesgos Tecnológicos.** Los participantes del mercado de valores deben **evaluar y tratar adecuadamente los riesgos tecnológicos en sus sistemas de información e infraestructura tecnológica, desde su concepción desarrollo e implementación, incluyendo entornos y procesos internos, en función del análisis de amenazas, vulnerabilidades, controles, impacto, y apetito de riesgo establecido por cada entidad de intermediación financiera y del alcance de dichas evaluaciones**. ~~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.~~	Sugerimos homogeneizar con el Artículo 13 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria.
Art. 8	Tomando en consideración que en algunos escenarios no será posible para el participante utilizar metodologías cuantitativas para evaluar el riesgo, se recomienda la siguiente redacción: 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".	Evitar la inclusión de obligaciones que pudieran ser de imposible cumplimiento para el participante del mercado o cuyo costo de cumplimiento supera sus beneficios.
Art.9	Las disposiciones de este artículo implican que una entidad como CEVALDOM deba evaluar el cumplimiento de las disposiciones de este Reglamento (o del Reglamento de Seguridad Cibernética y de la Información y de las disposiciones supletorias de lugar, según aplique) a todos sus clientes (participantes del depósito, miembros liquidadores, usuarios del sistema de registro de operaciones sobre valores, Ministerio de Hacienda, Mecanismos Centralizados de Negociación, Proveedores de Precios), sus reguladores (SIMV y BCRD), así como de determinados proveedores. Al respecto, consideramos lo siguiente:	Principio de utilidad y pertinencia, reconocido en el numeral 2 del artículo 4 de la Ley 167-2021. Principio de Racionalidad aplicable a las actuaciones de la Administración Pública Ley No. 249-17: Artículo 17, Numeral 8

	i. La evaluación del cumplimiento de las disposiciones regulatorias que le son aplicables a los participantes del mercado de valores constituye una función del órgano regulador. ii. La obligación a cargo de un participante del mercado de evaluar el cumplimiento de las disposiciones del Proyecto de Reglamento por parte de entidades de la Administración Pública pudiera resultar de imposible cumplimiento. Por otro lado, las disposiciones de este artículo parecerían extender la exigencia de cumplimiento de los requisitos y controles contenidos en el Proyecto de Reglamento a los proveedores de servicios interconectados con participantes del mercado de valores, sin considerar la aplicabilidad de tales controles. Por citar un ejemplo, parecería que debe evaluarse si el proveedor cumple con las disposiciones de gobierno corporativo contempladas en el Proyecto de Reglamento (responsabilidades del Consejo, conformación de un comité funcional de seguridad de la información, contratación de un Responsable de Seguridad de la Información, que por demás debe reportarse el Consejo de Administración). En este sentido, consideramos que la evaluación debe ser limitada a la validación de los controles de seguridad de la información aplicables a fin de mitigar los riesgos de seguridad asociados a la interconexión entre el proveedor y el participante del mercado de valores.	
Artículo 9 sobre Gestión de Riesgos Tecnológicos de terceros.	Sugerimos modificar la redacción de este artículo de manera tal que se indique que los participantes del mercado acordarán con las entidades interconectadas que éstas deberán cumplir con las disposiciones del Reglamento, pues la redacción actual establece una obligación de “supervisión” del participante respecto al cumplimiento a estas normas por parte de dichas entidades; toda vez que la redacción da a entender que debe exigirse al tercero todas las formalidades del Reglamento.	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad.

	En ese tenor, la medida razonable sería otorgar al participante la facultad de evaluar que el tercero cumple los principios que propician la seguridad cibernética y de la Información y no así exigir el cumplimiento de todas las formalidades del Reglamento. Por consiguiente, sugerimos considerar la siguiente redacción: "*Los participantes del mercado de valores deberán evaluar y procurar la gestión de riesgos tecnológicos a las entidades interconectadas con las que mantengan una relación contractual. Cuando la evaluación de riesgos tecnológicos realizada a estas entidades no sea satisfactoria, podrán proceder con la desconexión preventiva de la entidad interconectada y con el tratamiento de los riesgos que puedan producirse, tomando en consideración el apetito de riesgo establecido por cada participante del mercado de valores, hasta tanto dicha entidad interconectada realice las acciones correspondientes para la mitigación de sus riesgos y en la medida en que dicha vinculación pueda comprometer la estabilidad del mercado de valores y la salvaguarda de la Información que manejan*".	
Art. 9. Gestión de Riesgos Tecnológicos de terceros.	Debemos velar porque las disposiciones del reglamento sean cumplidas por cualquier entidad interconectada mediante el mantenimiento de una conexión electrónica o por el intercambio de información esencial, a través de cualquier medio digital, en la medida en que dicha vinculación pueda comprometer la estabilidad del mercado y la salvaguarda de la información	Cuando se refiere a cualquier entidad interconectada del mercado de valores (Las entidades del Mercado de Valores), se refieren a que nosotros como también entidad interconectada debemos de mantener el cumplimiento de lo que emite este reglamento para mantener la estabilidad del mercado.
Artículo 9	Proponemos utilizar un lenguaje alterno que permita que se proteja al mercado como un todo pero sea algo posible de realizar y acorde con los demás aspectos de este Proyecto de Resolución: **Artículo 9. Gestión de Riesgos Tecnológicos de terceros.** Los participantes del mercado de valores ~~**verificar**~~ **procurarán** que ~~las disposiciones de este Reglamento son cumplidas por~~ cualquier Entidad Interconectada **a estos, cumpla con las políticas y procedimientos internos que el participante del**	Entendemos que no todas las entidades interconectadas están sujetas a este Reglamento, debido a que no todas son participantes del mercado de valores. Asimismo, cada una representa un riesgo diferente el cual podrá ser mitigado en base al apetito de riesgo de la entidad.

	mercado de valores establezca en virtud de este Reglamento, mediante el mantenimiento de una conexión electrónica o por el intercambio de Información Esencial, a través de cualquier medio digital, en la medida en que dicha vinculación pueda comprometer la estabilidad del mercado de valores y la salvaguarda de la Información que manejan.	
Art. 10. Políticas y Procedimientos de seguridad.	Los participantes deben diseñar, implementar y mantener políticas que contemplen los procedimientos para la gestión de la Seguridad Cibernética y de la Información.	Considerar el escenario de los Grupos Financieros. ¿Qué sucede con la documentación existente a nivel Banco, es esta aplicable al PB o a la SAFI?, se debe de adecuar específicamente a una versión de PB o SAFI, ¿se puede usar una documentación corporativa? Se debe incluir la gestión de para Entidades que tienen soporte corporativo.
Artículo 10	**Solicitamos evaluar la siguiente redacción:** **"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, **según aplique**. Párrafo I Las políticas citadas anteriormente deben ser aprobadas por el consejo de administración y posteriormente comunicadas, bajo su contexto de aplicabilidad, a los empleados, proveedores de servicio, entidades interconectadas y las demás partes externas relevantes, cuando enmarque temas de aplicabilidad puntual a las partes."	Se propone que solo se divulguen las políticas que la entidad considere necesarias en dependencia de su aplicabilidad. Existen políticas y procedimientos que bajo el contexto de aplicabilidad no pueden ser divulgados a todas las partes debido a que no todas aplican bajo políticas o procedimientos creados en la institución o por temas de confidencialidad.
Art. 10. Políticas y Procedimientos de seguridad.	Los participantes deben diseñar, implementar y mantener políticas que contemplen los procedimientos para la gestión de la Seguridad Cibernética y de la Información.	¿Qué sucede con la documentación existente a nivel Banco, es esta aplicable a PB?, se debe de adecuar específicamente a una versión de PB, ¿se puede usar una documentación corporativa?

		Se debe incluir la gestión de para Entidades que tienen soporte de Centro Financiero.
Art. 10. Políticas y Procedimientos de seguridad. Párrafo I	**Párrafo I** Las políticas citadas anteriormente deben ser aprobadas por el consejo de administración y posteriormente comunicadas a los empleados, proveedores de servicio, entidades interconectadas y las demás partes externas relevantes.	Consideramos que, existen políticas y procedimientos que bajo el contexto de aplicabilidad no pueden ser divulgados a todas las partes debido a que no todas aplican bajo políticas o procedimientos creados en la institución, sugeriría Anexar la palabra "bajo su contexto de aplicabilidad" "Siempre que enmarque temas de aplicabilidad puntual a las partes" Tomando en cuenta que ciertas políticas tienen como intención aplicar un sistema o régimen de seguridad de información, que involucra inclusive el monitoreo y los controles contra los proveedores y empresas interconectadas, bajo cual razonamiento tendríamos la obligación de compartir dichas políticas a externos de la empresa, a menos que, sean políticas de cumplimiento por parte de estos proveedores/externos hacia la entidad, por lo cual deben tener conocimiento para su aplicación. Entendemos oportuno realizar esta salvedad. Consideramos que toda política ciertamente debe ser aprobada, a través del comité de ciberseguridad, y el consejo de administración conoce de estas, o rectifica las previamente aprobadas. No es de buena práctica asumir roles operativos al consejo de administración.
Art. 10 párrafo I	Ver comentarios al Artículo 6, numeral 2	Ver comentarios al Artículo 6, numeral 2
Art. 10. Políticas y Procedimientos	**Párrafo I** Las políticas citadas anteriormente deben ser aprobadas por el consejo de administración y posteriormente comunicadas a los empleados,	Consideramos que, existen políticas y procedimientos que bajo el contexto de aplicabilidad no pueden ser divulgados a todas las partes debido a que no todas

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

de seguridad. Párrafo I	proveedores de servicio, entidades interconectadas y las demás partes externas relevantes.	aplican bajo políticas o procedimientos creados en la institución, sugeriría Anexar la palabra "bajo su contexto de aplicabilidad" "Siempre que enmarque temas de aplicabilidad puntual a las partes"
Art. 11 Educación y creación de conciencia.	Educación y creación de conciencia	La palabra "Creación de conciencia" sugerimos sea sustituida por la palabra "Concientización" este punto solo como sugerencia.
Artículo 11 sobre Educación y creación de conciencia.	Se recomienda modificar el Artículo 11 que establece la provisión de entrenamiento periódico sobre las políticas y Procedimientos de Seguridad Cibernética y de la Información, a fin de delimitar la obligación de los participantes del mercado de valores, toda vez que tales capacitaciones formales resultan necesarias para determinado personal, mientras que existen otros colaboradores respecto a los cuales resulta más razonable proveer orientación sobre las políticas y Procedimientos, sin perjuicio de las obligaciones que se tiene de comunicar y difundir ampliamente estas políticas internas. En tal sentido, se propone la siguiente modificación: *"Los empleados del participante del mercado de valores y, cuando sea pertinente, los proveedores de servicios, afiliados o usuarios deben recibir orientación o entrenamiento apropiado y periódico, según corresponda, sobre las políticas y Procedimientos de Seguridad Cibernética y de la Información. [...]"*	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad.
Artículo 12 sobre Gestión del ciclo de vida de los activos de Tecnologías y de la Información.	En el Artículo 12, Gestión del ciclo de vida de los activos de Tecnologías y de la Información, numeral 4), sugerimos que el literal *e) Clasificación según su Confidencialidad y Riesgo asociado"* sea modificado por: *e) Clasificación según la metodología definida"*. Esto para dejar al participante que pueda definir los criterios que considere idóneos y esta se encuentre definida según los riesgos ya asociados y no se dupliquen esfuerzos.	Claridad del requerimiento

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 12, numeral 4, literal b)	La información relacionada al impacto o implicaciones relacionadas a la pérdida del activo es parte de la matriz de riesgos (lo cual ya es requerido por el Proyecto de Reglamento). El exigir que la misma se incluya además en el inventario de activos no agrega valor para la entidad (al tratase simplemente de una duplicidad de la información) y genera el riesgo de desactualización del documento.	Redundancia en el requisito
Art. 12, numeral 4, literal e)	Se recomienda modificar el literal e) para que se lea: Clasificación según su criticidad para los servicios del negocio.	Claridad del requerimiento
Artículo 12, numeral 5	Sugerimos aclarar si se refiere al permiso de acceso a las aplicaciones, a la asignación de equipos de cómputo y móviles que den acceso a la información o a ambos.	Aclaración.
Art. 12 Gestión del ciclo de vida de los activos de Tecnologías y de la Información. Párrafo V	**Párrafo V.** Procedimientos de control para la devolución y asignación de los activos de Tecnología y de la Información a los usuarios, con aceptación y firma de responsabilidades según corresponda	Se sugiere aclarar ¿aplicar ante el permiso de acceso a las aplicaciones o asignación de equipos de cómputo y móviles?
Art. 13. Aplicaciones de estaciones de trabajo	Los participantes del mercado de valores deben establecer procesos para la gesti6n adecuada de la Seguridad Cibernética y de la información de las aplicaciones instaladas en las estaciones de trabajo.	Sugerimos eliminar el presente artículo.
Art. 14 Aplicaciones del negocio.	**Párrafo 1**. Protección de las aplicaciones: Deben utilizar funcionalidades de Seguridad Cibernética y de la información alineadas a la infraestructura técnica. **Párrafo II.** Protección de las aplicaciones basadas en navegación.	Párrafo 1 se presta ambigüedad de los conceptos sobre "funcionalidades". Párrafo II. Ambigüedad en la definición, qué específicamente se espera en este lineamiento.
Artículo 14	Solicitamos añadir al numeral 1: “1) **Protección de las aplicaciones:** Deben utilizar funcionalidades de Seguridad Cibernética y de la Información alineadas a la infraestructura	De acuerdo con el Artículo 4, el participante podrá optar por uno o varios Marcos de Trabajo conforme a sus requerimientos y necesidades, confirmar que sólo le aplicarían aquellos seleccionados.

	técnica de seguridad, que permitan el cumplimiento de los requerimientos de Confidencialidad e Integridad de la Información, **conforme al Marco de Trabajo elegido por el participante del mercado de valores**;”	
Artículo 16	**Artículo 16. Privacidad de la Información.** Los participantes del mercado de valores deben desarrollar políticas y Procedimientos de protección de datos personales y de privacidad de la información según las leyes y normativas vigentes y el Marco de Trabajo **seleccionado**. Dichas políticas y Procedimientos deben establecer, como mínimo, lo siguiente: (…)” En el numeral 6 se habla del enmascaramiento de datos pero no se limita a cierto tipo de información o ciertos contextos específicos, sugerimos la siguiente redacción: “6) Uso de técnicas de enmascaramiento de datos para, **al buen criterio del participante a la luz del Marco de Trabajo elegido,** ocultar partes de la Información al momento de ser almacenada o transmitida;	Pertinencia de cumplir según lo posible y en concordancia con el Marco de Trabajo escogido. El enmascaramiento no debe ser obligatorio, pues depende de las interacciones y uso que se dé a la información.
Art. 16 Privacidad de la Información. Numeral 6	6) Uso de técnicas de enmascaramiento de datos.	No define las técnicas ni tampoco ¿en qué casos es aplicable?
Artículo 16 sobre Privacidad de la información	En el Artículo 16 sobre Privacidad de la información, tenemos las siguientes observaciones: Numerales 6) y 7), solicitamos su consideración para establecer los límites a los casos que aplique según el análisis de riesgos, dado que no todas las entidades requieren que se establezca este proceso y es muy ambigua su aplicación.	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad; y Numeral 4 Principio de Seguridad jurídica, de previsibilidad y certeza normativa.
Art. 16	Tomando en consideración que la adopción de un Marco de Trabajo es opcional, sugerimos la siguiente redacción:	Claridad en la Redacción Principio de Seguridad jurídica, de previsibilidad y certeza normativa

	"Los Participantes del mercado de valores deben desarrollar políticas y procedimientos de protección de datos personales según las leyes y normativas vigentes, pudiendo adoptar además un marco de trabajo." En el numeral 6, establecer limitar a los casos que aplique según en análisis de riesgos. Ante la ausencia de regulación o normativa relacionada a los metadatos que sirva de marco de referencia, sugerimos eliminar el numeral 7. En el Proyecto de Reglamento se ha incluido como un requisito mínimo y por tanto obligatorio, pero no existe un marco de referencia en República Dominicana que permita aportar mayor contexto a la obligación, y la forma en la que se aborda en el Proyecto de Reglamento constituye una obligación, sin considerar los escenarios en los que pueda aplicar. El contemplar la obligación en ausencia de mayor contexto regulatorio genera riesgos de diversidad de interpretación entre los regulados y el propio regulador, lo cual genera inseguridad jurídica. Dado su nivel de la complejidad y a los fines de evitar inseguridad jurídica, en Europa, donde su Reglamento General de Protección de Datos es de los más avanzado siendo ejemplo en otras jurisdicciones, el tema tuvo que ser abordado mediante una regulación especial (Reglamento sobre la Privacidad y las Comunicaciones Electrónicas).	
Art. 17	Tal y como hemos comentado anteriormente, entendemos que las obligaciones relativas a proveedores deben considerar el tipo de servicio brindado, pues en algunos casos no son aplicables los controles establecidos en el Proyecto de Reglamento. En este sentido, recomendamos establecer que las obligaciones mencionadas en el artículo en cuestión serán incluidas en los casos que aplique según el servicio contratado y el correspondiente análisis de riesgo.	Principio de Racionalidad La obligación establecida no considera la realidad del servicio contratado ni los riesgos asociados. Los controles exigidos deben encontrarse asociados al nivel de riesgo, a fin de que el costo del control no exceda sus beneficios.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 17 sobre Obligaciones Contractuales.	Consideramos que es importante delimitar las obligaciones sobre la Seguridad Cibernética respecto a los proveedores, considerando el tipo de proveedor y los servicios que provee y tomando en consideración la criticidad de los mismos. Sugerimos que se modifique la redacción de la última oración de manera que se elimine la palabra "*definido*", para mayor claridad del artículo.	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad; y
Art. 17 Obligaciones contractuales.	**Párrafo.** Asimismo, el participante del mercado de valores debe conservar el derecho de auditar los procesos y controles de dichos proveedores de servicios o Entidad Interconectada.	¿Cómo se espera que se pueda cumplir esto? El estar conectado con un proveedor o entidad no nos otorga poder de regulación para poder auditar a un tercero. Sugerimos homologar criterio conforme el reglamento de ciberseguridad de BCRD. El hecho de encontrarnos conectados con un tercero, por obligación para poder cumplir con las actividades autorizadas del participante del mercado, o debido a que son funciones y servicios de terceros (Cevaldom / BVRD / otros) no nos da el derecho de auditar los controles de los mismos. Esto es importante, considerado igualmente para el caso contrario, en caso de un participante del mercado donde posee usuarios conectados a estos, como es el caso de un puesto de bolsa, solicite auditar nuestras políticas, procesos y controles internos. Igual, considerar proveedores extranjeros, donde su alcance en estos aspectos puede encontrarse limitados de aplicación por su jurisdicción. Delimitar los requerimientos necesarios y de alcance, que nos permita conocer que una empresa conectada posee control en estos aspectos de ciberseguridad.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 17	Favor añadir la siguiente redacción: **"Artículo 17. Obligaciones contractuales.** Los contratos suscritos entre los participantes del mercado de valores y sus empleados, proveedores de servicios, Entidades Interconectadas y demás partes externas a los cuales se les concede Acceso a la Información, deben establecer las responsabilidades generales de las partes, disposiciones sobre la Confidencialidad y no divulgación de la Información, protección de datos y especificaciones sobre Seguridad Cibernética y de la Información. De igual forma, las disposiciones sobre las citadas materias deben prolongarse luego de la finalización de la relación contractual por el período definido ~~que se defina~~ en el acuerdo en virtud de la naturaleza del Acceso a la Información concedido, **conforme al Marco de Trabajo elegido por el participante del mercado de valores**."	De acuerdo con el Artículo 4, el participante podrá optar por uno o varios Marcos de Trabajo conforme a sus requerimientos y necesidades, confirmar que sólo le aplicarían aquellos seleccionados.
	Se recomienda eliminar el párrafo o en su defecto modificar su contenido: ~~**Párrafo.** Asimismo, el participante del mercado de valores debe conservar el derecho de auditar los procesos y controles de dichos proveedores de servicios o Entidad Interconectada.~~	Un participante del mercado de valores no tiene la potestad de realizar auditorías a un tercero. Adicionalmente, no debe aplicarse a todo tipo de proveedores, y en este caso, la forma de realizarlo deberá estar definida en la política de cada entidad, de acuerdo con su apetito de riesgo.
Art. 17 Obligaciones contractuales.	**Párrafo.** Asimismo, el participante del mercado de valores debe conservar el derecho de auditar los procesos y controles de dichos proveedores de servicios o Entidad Interconectada.	Un participante del mercado de valores no tiene la potestad de realizar auditorías a un tercero. Considerar eliminar este artículo
Art. 18 Protección contra la fuga de Información.	Deben mantener políticas, procedimientos y mecanismos de protección contra la fuga de información (DLP) a los sistemas, Infraestructura tecnológica y entornos locales. Unificar políticas y procedimientos.	No define las técnicas ni tampoco ¿en qué casos es aplicable? Se sugiere aplicar un lineamiento con el conglomerado de todas las políticas y requerimientos requeridas en un solo artículo.
Artículo 18	Atentamente solicitamos evaluar que la implementación del sistema DLP sea opcional.	La implementación del sistema DLP tiene altos costos de implementación y las políticas y procedimientos sobre la protección de la información pueden ser aptos

		para aplicar el tratamiento apropiado en los datos sensibles de la entidad.
Art. 18 Protección contra la fuga de Información.	Deben mantener políticas, procedimientos y mecanismos de protección contra la fuga de información (DLP) a los sistemas, Infraestructura tecnológica y entornos locales	No define las técnicas ni tampoco ¿en qué casos es aplicable?
Art. 20 Gestión de identidades y Mecanismo de Control de Acceso.	1. Procedimientos documentados para la administración y autenticación de identidades a nivel institucional incluyendo doble autenticación. 4. Directrices generales para la asignación y utilización de cuentas privilegiadas en los sistemas de información y aplicaciones de negocio. Párrafo I. Los mecanismos de Control de Acceso deben considerar al menos los siguiente: Contraseña o token físico o digital, tarjeta inteligente, certificado digital o similar Y elementos biométricos.	1) Aclarar ¿debe ser aplicable para todos los aplicativos? ¿No establece un criterio de uso? ¿cuáles son los tipos de MFA? Evaluar incluir en las definiciones. 4) Directrices generales no define los tratamientos. Ambigüedad. Párrafo I. Solicita varios factores de autenticación y elementos biométricos, las aplicaciones, sobre todo los legacy, será complicado implementarlos, evaluar cambiar los niveles de factores de autenticación Los ciclos de autenticación son: 1) algo que el usuario sabe cómo una clave, un pin o una respuesta a una pregunta secreta, 2) algo que el usuario tiene que pasar a ser un 2FA como un token físico o digital, un USB o un llavero y 3) algo que el usuario es, facial, Voz, huella digital, retina o biometría de comportamiento. Entendiendo esto no es coherente poner estos 3 renglones en solo 2. Dividir la gestión de accesos en los siguientes renglones acorde a los mejores estándares utilizados: • Controles de Accesos Físicos • Controles de Accesos Lógicos • Controles de Accesos Administrativos

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

		Contemplar accesos: • Discretionary access control (DAC) • Mandatory access control (MAC) Role-based access control (RBAC)
Artículo 20 sobre Gestión de identidades y Mecanismos de Control de Acceso	1. Notamos que se desprende del numeral 1) que los mecanismos de Control de Acceso deben incluir "procedimientos documentados para la administración y autenticación de identidades a nivel institucional, incluyendo la doble autenticación"; En tal virtud, traemos a su consideración que la autenticación de doble factor sea aplicada en casos que se estime necesario, en atención al tipo de privilegio de la Información. 2. En lo que respecta al párrafo que cita los Mecanismos de Control de Acceso, entendemos que debe utilizarse la conjunción "o", para expresar que se trata de alternativas, tal y como se desprende del párrafo II del indicado Reglamento al señalar que los participantes podrán establecer uno o más Mecanismos de Control de Acceso, según el grado de criticidad de los sistemas.	Artículo 3 numeral 4 de la Ley 107-13 Principio de Racionalidad.
Artículo 20	Los mecanismos de control deben ser determinados por las políticas y procedimientos de la entidad, por tanto, recomendamos reconsiderar toda la redacción de este Artículo y sus párrafos. En caso de no acoger nuestra solicitud considerar la siguiente sugerencia: **"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, **conforme al Marco de Trabajo elegido por el participante del mercado de valores**, incluyendo:	Los mecanismos de control deben ser determinados por las políticas y procedimientos de la entidad. Solicita varios factores de autenticación y elementos biométricos, las aplicaciones, sobre todo los legacy, será complicado implementarlos, evaluar cambiar los niveles de factores de autenticación Los ciclos de autenticación son: 1) algo que el usuario sabe , por ejemplo una clave, un pin o una respuesta a una pregunta secreta; 2) algo que el usuario tiene que pasa a ser un 2FA como un token físico o digital, un USB o un llavero y 3) algo que el usuario es, facial,

	(…) Párrafo I. Los Mecanismos de Control de Acceso, **según aplique**, deben considerar:~~, al menos, lo siguiente:~~ a) Contraseña, preguntas secretas o pin. **b)** tóken físico o digital, tarjeta inteligente, certificado digital o similar; **o** ~~y~~, ~~b)~~ **c)** Elementos biométricos, como huella dactilar, patrón de iris, reconocimiento de voz, estilo de escritura o similares. (…)”	Voz, huella digital, retina o biometría de comportamiento. Entendiendo esto no es coherente poner estos 3 renglones en solo 2.
Art. 20, numeral 1	Se recomienda modificar el artículo en su numeral 1) para que se lea de la siguiente forma: Procedimientos documentados para la administración y autenticación de identidades a nivel institucional, eliminando la referencia a doble autenticación, la cual se encuentra establecida en el párrafo de este artículo. Al ver la referencia, nos preguntamos si la intención de la referencia es porque se desea exigir que todos los sistemas tengan doble factor de autenticación. En caso afirmativo sugerimos revisar el requerimiento, ya que de acuerdo con las buenas prácticas el uso de doble factor de autenticación depende de la criticidad del sistema y de los resultados de análisis de riesgos de cada empresa.	Principio de Racionalidad Claridad de la Norma Los controles exigidos deben encontrarse asociados al nivel de riesgo, a fin de que el costo del control no exceda sus beneficios.
Art. 20, numeral 2	Se sugiere que en lugar de "por tipo de usuario" el requerimiento se encuentre basado en los principios de mínimo privilegio y lo que se necesita saber (need to know).	Mejor práctica
Art. 20, párrafo I,	Las necesidades de uso de uno o más factores de autenticación deben ser determinadas a partir de los resultados de un análisis de riesgos y las	Principio de Racionalidad Claridad de la Norma

	necesidades de cada institución. Tomar en consideración que de mantener el uso de la conjunción "y" este párrafo y el párrafo II serían incongruentes. A los fines de reducir riesgos y la protección de los derechos del interesado, el uso de datos biométricos debe considerarse sólo para escenarios que lo ameriten. En tal virtud, recomendamos eliminar el uso de la conjunción "y". Además de evaluar la redacción a fin de que los mecanismos de control de acceso exigidos sean determinados por el propio participante en función del análisis de riesgo y la criticidad del activo de información	Los controles exigidos deben encontrarse asociados al nivel de riesgo, a fin de que el costo del control no exceda sus beneficios.
Art. 21 Gestión de contraseñas.	Formato de contraseñas y reglas relativas a la longitud.	No define los criterios de contraseñas, se propone definir el de las mejores prácticas sin embargo esto no está definido.
Art. 21, numeral 3	Se sugiere delimitar: impedimento de reutilización conforme a criterios establecidos y/o mejores prácticas. De quedar abierto se puede interpretar que nunca podrá ser reutilizada una contraseña, cuando la realidad práctica es distinta	
Art. 21 párrafo	Se recomienda cambiar la palabra "contraseñas" por "credenciales", pues la confidencialidad abarca además el usuario.	Mejor práctica
Artículo 22	Para masificar el mercado debemos pensar en puntos de servicios con menos complejidades, por lo que sugerimos que los mecanismos de control sean obligatorios exclusivamente para aquellos puntos de atención u oficinas que no tengan limitado el acceso de visitantes a áreas en las que se maneje información sensible o confidencial. Asimismo, sugerimos aclarar que los mecanismos de control de visitas pueden ser centralizados en los puntos de acceso de las edificaciones en las que el participante tiene sus oficinas o puntos de servicio. **Sugerimos la siguiente redacción:**	Promoción del mercado y salvaguarda de estándares de seguridad para el mercado.

	Párrafo I, Numeral 2: “(…) 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, <u>en las oficinas que no tengan limitado el acceso de visitantes a áreas en las que se maneje información sensible o confidencial</u>; (…)”	
Artículo 22	“(…) **Párrafo II**. Los mecanismos para la protección de la seguridad física y el entorno de las instalaciones del negocio, **<u>de acuerdo a la naturaleza de la entidad</u>**, deben asegurar: (…)” […]	Las medidas y mecanismos deben ser propicios según las funciones, operación, tamaño, política de riesgo, etc, de cada entidad.
Artículo 22 sobre Seguridad física y del entorno.	En el párrafo II, numerales 2 y 3, así como párrafo III: favor considerar que los requisitos de “*ventanas y puertas blindadas*” y despliegue de “*guardianes de seguridad en las instalaciones físicas*” de los participantes implican un costo excesivo que pudiera afectar negativamente a los participantes. En este sentido, sugerimos eliminar estos requerimientos. En efecto, hay que notar que sobre el participante del mercado de valores recae una obligación principal que es la de asegurar la protección física y del entorno. En ese sentido, para lograr esa obligación, puede tomar múltiples acciones, atendiendo a sus posibilidades. De modo que, resulta razonable que los requerimientos citados tengan categoría optativa o facultativa para el participante, sin perjuicio de la obligación principal de seguridad que debe satisfacer.	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad. Artículo 3 numeral 4 de la Ley 107-13 Principio de racionalidad.
Art. 22 párrafo II	Se sugiere que en el numeral 1) se elimine la palabra “ocultamiento” y colocar “la protección".	Aportar claridad a la norma

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 22 párrafo III	Se sugiere modificar el párrafo para que lea de la siguiente forma: Párrafo III. Los entornos críticos deben contar con sistemas de detección y mitigación de incendios conforme a los riegos asociados de cada institución. Esto se debe a que dependerá de los resultados del análisis de riesgos de cada empresa respecto a amenazas externas. Recomendación: tomar como referencia art 39 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria: Los entornos críticos deben ser protegidos contra accidentes, ataques, acceso físico no autorizado, así como estar protegido contra incendios, inundaciones y otras amenazas naturales. El uso de Marcos de Trabajos es opcional.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos

Art. 23 Sistemas informáticos e Infraestructura Tecnológica.	Sistemas informáticos e Infraestructura tecnológica, los participantes del mercado de valores deben procurar que los sistemas informáticos y la infraestructura tecnológica puedan ser protegidos contra toda amenaza. 2) Administración centralizada de sistemas a través centros de operaciones de red, sistemas y seguridad, o mecanismos equivalentes; 3) Gestión adecuada de actualizaciones de seguridad. 4)Diseño adecuado de la red.	El termino de ser protegidos contra toda amenaza es amplio y ambiguo, ¿cómo se define su tema de cumplimiento? 2) Es muy amplio el concepto, se solicita se desarrolle el concepto a lo esperado. 3) ¿Qué se considera adecuado? 4) ¿Qué se considera adecuado?
Artículo 23	Solicitamos considerar la siguiente redacción: **“Artículo 23. Sistemas informáticos e Infraestructura Tecnológica.** Los participantes del mercado de valores deben procurar que los sistemas informáticos y la Infraestructura Tecnológica puedan ser protegidos contra toda Amenaza **previsible**. Por lo que, deben configurar adecuadamente los controles de Seguridad Cibernética y de la Información integrados por defecto, incluyendo: (…)” Solicitamos aclarar los siguientes aspectos: “(…)	Sólo se puede mitigar aquello que se prevee. Es imposible protegerse contra toda amenaza. 2) Es muy amplio el concepto, se solicita se desarrolle el concepto a lo esperado.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 23	Se sugiere la siguiente redacción: “Los participantes del mercado de valores deben procurar que los sistemas informáticos y la Infraestructura Tecnológica puedan ser protegidos contra las Amenazas”. De acuerdo con las buenas prácticas, las empresas protegerán los sistemas de información de acuerdo con los resultados de los análisis de riesgos y su nivel de apetito de riesgo, por tales razones sugerimos remplazar la palabra “toda,	Principio de Racionalidad Claridad de la Norma Realidad del contexto mundial con relación a las amenazas cibernéticas
Art. 23, numeral 2)	Se recomienda que el artículo se redacte como sigue 2) Administración de sistemas a través de centros de operaciones de red, sistemas y seguridad, o mecanismos equivalentes. Se debe a que, la administración centralizada o no, dependerá de los riesgos y necesidades de cada institución.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos
Art. 24	Se recomienda que se elimine la palabra “y de mantenimiento” ya que los cambios de mantenimiento no son de emergencia y deben ser programados.	Mejor Práctica

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 24	Sugerimos especificar que la gestión de cambios se realice sobre las aplicaciones de alta relevancia para la entidad. **"Párrafo II. Sobre las aplicaciones de alta relevancia para 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."	Principios de eficiencia y razonabilidad.
Art. 26 Instalación de Software.	**Párrafo.** La instalación y actualización de Software y aplicaciones en los sistemas operativos solo podrán ser implementados luego de realizar pruebas adecuadas en un ambiente separado de producción. Las pruebas realizadas deben contemplar los aspectos siguientes: 1) Ensayo de rendimiento; 2) Carga de trabajo; 3) Seguridad; 4) Disponibilidad operativa; 5) Efectos sobre otros sistemas; y, 6) Copia de respaldo y de recuperación.	Esta parte genera incertidumbre sobre cómo se espera que se le dé Cumplimiento a este punto cuando no siempre los ambientes de prueba pueden replicarse tal cual están en producción por cuestiones que van desde lo técnico hasta lo presupuestario.
Art. 26, párrafo	Se recomienda eliminar el los numerales 1, 2 y 6, ya que las disposiciones contenidas en los mismos no son aplicables para las actualizaciones de todos los sistemas.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos Evitar inclusión de obligaciones cuyo cumplimiento no sea posible
Artículo 27	**Sugerimos la siguiente redacción:** "**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 procurando el almacenamiento de las copias de resguardo en formato digital en la nube o en un ambiente con diferentes niveles de acceso y de localización.**"	Según el modelo de negocio o marco de trabajo, la entidad puede optar por tener sus copias de resguardo de forma física, de forma digital o de ambas maneras.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 27 Respaldos.	**Párrafo III.** Almacenamiento apartado a una suficiente distancia. **Párrafo IV.** Participantes cuya Infraestructura tecnológica sea administrada por un proveedor de servicios en términos de respaldos. **Párrafo VI.** Tiempo de retención de pistas de auditoría.	**Párrafo III** ¿Cuál es el concepto de suficiente distancia??, las mejoras practicas hablan de más de 15 km de distancia según las condiciones geográficas, sísmicas, de las entidades. **Párrafo IV.** ¿Como es la aplicabilidad de esta regla para Puestos de Bolsas con en términos contractuales por los servicios provistos por el otra filial ejemplo Banco? ¿Esclarecer las responsabilidades y alcances? **Párrafo VI.** Los criterios de la Superintendencia de Bancos son diferentes en términos de tiempos de resguardo, favor evaluar homologar.
Art. 27, numeral 4	Se recomienda agregar que esto solo aplica para sistemas que realicen copias en cintas.	Claridad de la Norma
Art. 27, párrafo V	La información esencial no necesariamente es confidencial. El control de cifrado debe aplicar de acuerdo con el nivel de confidencialidad y no depender de si es vital o no.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos Delimitación del control a la realidad que aplicable
Artículo 30	Solicitamos tener en cuenta la redacción sugerida a continuación: "(…) 2) **Análisis de Riesgo:** Consiste en identificar y evaluar los Riesgos **previsibles** que puedan afectar la operación de los procesos clave. De igual forma, identifica los desastres, Amenazas cibernéticas, eventos o accidentes que tienen una probabilidad de ocurrencia dentro de diferentes escenarios. 3) **Análisis de impacto del negocio:** Consiste en identificar funciones y Procesos Críticos del negocio con importancia estratégica y su clasificación según la criticidad, prioridades, impacto que su interrupción impondría y el tiempo de recuperación. Dicho análisis debe incluir, al menos, lo siguiente:	Razonabilidad y aplicabilidad regulatoria.

	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**; (..)"	
Artículo 30 sobre la Continuidad del Negocio.	1. De manera particular en el párrafo, numeral 2 sobre Análisis de Riesgo, proponemos que sea incluido en las definiciones del artículo 3 el concepto de "desastres". Considerando que estos conllevarán un protocolo para su identificación y evaluación. 2. Por otro lado, en el párrafo, numeral 3, sobre el Análisis de impacto del negocio se establecen los elementos que deben ser incluidos en el análisis, entre los cuales se encuentran; "*d) Escalas de tiempo aceptables para la recuperación de sistemas, aplicaciones y servicios; e) Tiempo de interrupción máxima aceptable de sistemas, aplicaciones y servicios del participante del mercado de valores* (…)". Considerando que la determinación de estos plazos se encuentra sujeta al curso normal de operaciones del participante del mercado de valores, así como de los efectos que esto tuviera en los usuarios, entendemos oportuno incluir una nota en este sentido.	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.
Art. 30, numeral 7	Se propone la modificación del artículo para que se agregue en la parte infine "de acuerdo con los resultados de análisis de impacto del negocio"	Aportar claridad al texto
Art. 30, párrafo	Se recomienda la modificación del artículo para que se lea de la siguiente forma: Los planes deben ser aprobados por la alta gerencia con el objeto de asegurar la viabilidad, efectividad y eficacia operativa de los mismos. Tal y como se explicó anteriormente, conforme a las buenas prácticas de gobierno corporativo, el Consejo de Administración no debería adoptar decisiones operativas. El contenido de los planes de descritos en el artículo en cuestión trata aspectos operativos.	Principios de Gobierno Corporativo de la OCDE (principio IV) Guía Práctica de Gobierno Corporativo, Experiencias del Cirulo de Empresas de la Mesa Redonda Latinoamericana Reglamento de Gobierno Corporativo: Artículo 14

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 32 sobre Registros y Monitoreo Continuo.	En el numeral 12 se hace referencia a "*eventos falsos*", no obstante, estos no han sido claramente definidos en el Reglamento. Recomendamos incluir la definición de este término en el artículo 3, de manera que el participante del mercado de valores tenga mayor claridad al momento de determinar la obligación de mantener esta información en los registros. Igualmente, el párrafo I crea un plazo de cinco (5) años para el mantenimiento en registro de las informaciones. Considerando los costos operativos del almacenamiento de esta información y su impacto en participantes de menor volumen, sugerimos limitar este plazo a un periodo más reducido a dos (2) años.	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa. Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad.
Art. 32 Registros y Monitoreo Continuo.	**Art. 32** Registros y monitoreo continuo política para mantener y revisar regularmente los registros de eventos de las actividades realizadas por los usuarios.	Criterios para el monitoreo de la información resguardada, en qué consisten las revisiones periódicas, así como la definición de eventos que se consideren relevantes.
Art. 32 Registros y Monitoreo Continuo.	En este apartado solicitamos especificar en el punto **7) Uso de privilegios;** **8) Uso de utilidades y aplicaciones del sistema;** y **9) Archivos accedidos y tipo de Acceso;** se debe delimitar más claramente lo que se requiere registrar y monitorear debido a que la redacción lo deja abierto. 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;	7) ¿De cuáles privilegios estamos hablando porque el tener una cuenta de acceso en sí es un privilegio? Los puntos 7, 8 y 9 se prestan ambigüedad que podría dificultar su cumplimiento, favor especificar que se espera. **Párrafo I.** En cuanto al período de retención se debe especificar si este es en línea o recuperable.

	4) Identificación o ubicación del dispositivo, si es posible, y el identificador del sistema o los intentos de Acceso a los datos y otros recursos; 5) Registros de intentos de Acceso al sistema; 6) Cambios en la configuración del sistema; 7) Uso de privilegios; 8) Uso de utilidades y aplicaciones del sistema; 9) Archivos accedidos y tipo de Acceso; 10) Direcciones IP, origen, destino y protocolos de red; 11) Activación y desactivación de los sistemas de protección; 12) Procedimientos para identificar eventos falsos menores y eventos significativos; y, 13) Otros registros de eventos que la entidad considere relevantes conforme a su matriz de Riesgos. **Párrafo I.** Las informaciones referidas en este artículo deben ser conservadas a través de los medios electrónicos definidos por la entidad por un período que, en ningún caso, será inferior a cinco (5) años. **Párrafo I**. Las informaciones referidas en este artículo deben ser conservadas a través de los medios electrónicos definidos por la entidad por un período que, en ningún caso, será inferior a cinco (5) años.	
Art. 32, párrafo I	Sugerimos que el plazo de conservación de registros sea reducido a tres (3) años a fin de hacerlo coincidir con el plazo establecido en el artículo 30 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria	Artículo 30 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria
Título II, Capítulo IV, Artículo 32, Párrafo I	Considerar ajustar el tiempo de retención de 5 años a 3 años	El objetivo es estar homologado con el Reglamento de Seguridad Cibernética y de la Información del Banco Central, el establece 3 años, Art. 30 literal d
Artículo 32, Párrafo I.	En cuanto al período de retención que se señala se debe especificar si se trata de una retención que deba estar en línea o recuperable. Solicitamos que se	Aclaración para aplicación normativa

	evalúe si el tiempo solicitado no es muy extenso para las necesidades del mercado.	
Título II, Capítulo IV, Artículo 33 2)	Considerar ajustar el tiempo de retención de 5 años a 3 años	El objetivo es estar homologado con el Reglamento de Seguridad Cibernética y de la Información del Banco Central, el cual establece 3 años, Art. 30 literal d
Art. 33 Gestión de Problemas e Incidentes	2) Establecimiento de un Procedimiento para la gestión de Problemas e Incidentes de Seguridad Cibernética y de la Información que cubra las fases de identificación, respuesta, recuperación y seguimiento conforme al Marco de Trabajo, así como el mecanismo para su identificación, registro, categorización y clasificación. El tiempo de retención de los registros no podrá ser menor a cinco (5) años;	Especificar si el periodo de retención es en línea o recuperable. Validar si los plazos en otra normativa es el mismo.
Artículo 33 sobre Gestión de Problemas e Incidentes	1. En el numeral 2 se establece un plazo de cinco (5) años para la retención de los registros. Considerando los costos operativos para el almacenamiento de esta información y su impacto en participantes de menor volumen, sugerimos limitar este plazo a un periodo más reducido de dos (2) años. 2. En cuanto a la obligación establecida en el literal c) sobre uso de herramientas para asistir en el proceso de gestión de incidentes, sugerimos establecer que el participante debe cumplir con esta asistencia, no obstante, los medios para ejecutarla dependerían de los procesos establecidos por cada uno de estos.	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad.
Art. 33 numeral 1, literal d	Se recomienda modificar el artículo, para que se lea: Datos sobre Problemas o Incidentes a ser documentados, incluyendo la Información de contacto, entorno de negocios afectados y aspectos técnicos, ya que la información requerida depende del incidente.	Delimitación del control a la realidad que aplicable
Art. 33, numeral 2	Sugerimos que el plazo de conservación de registros sea reducido a tres (3) años a fin de hacerlo coincidir con el plazo establecido en el artículo 30 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria	Artículo 30 del Reglamento de Seguridad Cibernética y de la Información de la Junta Monetaria

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 33, Numeral 2.	En cuanto al período de retención que se señala se debe especificar si se trata de una retención que deba estar en línea o recuperable. Solicitamos que se evalúe si el tiempo solicitado no es muy extenso para las necesidades del mercado.	Aclaración para aplicación normativa
Art. 33, numeral 3	Consideramos que el uso de herramientas y sistemas especializados queda sujeto a la realidad de cada participante, pudiendo éste lograr el objetivo perseguido a través de otros medios.	El objetivo perseguido puede ser alcanzado a través de otros medios que corresponden al propio participante definir
Art. 34 Gestión de parches	Gestión de parches. Los participantes del mercado de valores deben gestionar e "**instalar de parches seguridad**" para proteger los sistemas de Información y la infraestructura de tecnología de la Información, así como mantener el conocimiento actualizado de los parches Página 38 de 55 disponibles. La gestión e implementación de parches debe considerar los aspectos del artículo 24 (Gestión de cambio) del presente Reglamento.	Aclarar la actualización de parches. **Corregir** "" por instalar parches de seguridad.
Art. 35 Monitoreo Continuo.	Monitoreo Continuo	No se definen los criterios, componentes ni alcances de los servicios / infraestructura a someter al monitoreo continuo
Artículo 36 sobre Prevención y detección de intrusos.	En el numeral 3, literal d) se sugiere incluir "*estimada*" por tratarse de un análisis previo al hecho ocurrido.	N/A
Art. 36, numeral 3	Se recomienda mover este acápite completo, ya que todo esto forma parte del procedimiento de eventos e incidentes. En ese sentido se recomienda colocarlo en dicho procedimiento.	Claridad del texto y congruencia de la norma
Artículo 37 sobre Protección de Software malicioso.	Sugerimos limitar la obligación de capacitación hasta los empleados y proveedores de servicios, considerando que el control de los participantes del mercado sobre el uso que dan los usuarios a sus ordenadores se encuentra limitado a los controles de seguridad establecidos en sus plataformas. A tales fines, sugerimos la siguiente redacción: "*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*	Artículo 3 numeral 4 de la Ley 107-13 Principio de racionalidad.

	los sistemas e Infraestructura Tecnológica, así como Procedimientos y capacitación continua y adecuada para concientizar a los empleados sobre el Software Malicioso. <u>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.</u>”	
Art. 37, párrafo I	Se sugiere modificar el artículo para que se lea: “…Software malicioso en todos los dispositivos finales que formen parte de la Infraestructura Tecnológica de la entidad”. Se propone delimitar la aplicación a dispositivos finales, pues la palabra dispositivo abarca todo tipo de equipo con sistema operativo, como equipos de redes y comunicaciones, firewalls, IPSs, etc.	Claridad del texto
Art. 37, párrafo II	Se propone cambiar por "deben mantener configuraciones adecuadas para...", pues los sistemas de prevención de código malicioso deben mantenerse en constante revisión y actualización para asegurarse de la efectividad de dicho control.	Mejor práctica
Art. 38 Gestión de la red	2) Gestión de la red física: Las redes deben ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales, los puntos de Acceso a la red deben estar protegidos por Mecanismos de Control de Acceso, tales como, la documentación de la arquitectura de red e Integridad. 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	2) La documentación de la arquitectura de la red e integridad no es un mecanismo de control de acceso. 5) Aclarar el análisis de mantenimiento no se entiende. 5) f) requerimos que se detalle más información sobre el tipo de análisis que se requiere y a qué se refieren con que sea independiente.

	objetivos y alcance del mantenimiento planificado, controles para el registro de Acceso individualizado por cada tercero, mecanismos de autorización de Acceso a los sistemas mediante credenciales únicas especializadas y su revocación tras la finalización del mantenimiento; f) Elaborar un análisis independiente de las labores de mantenimiento remoto; g) Supervisar los mantenimientos remotos durante su realización. Una vez terminadas las sesiones de mantenimiento, las sesiones de conexión deben finalizar automáticamente; h) Definir los controles para aplicaciones de gestión de mantenimiento remoto, contemplando aspectos de gestión de Acceso, análisis de origen y destino de conexiones, así como el Monitoreo Continuo de las actividades realizadas en cada sesión y la inhabilitación de la conexión tras la conclusión del mantenimiento. **f)** Elaborar un análisis independiente de las labores de mantenimiento remoto;	
Art. 38 Gestión de la red	2) Gestión de la red física: Las redes deben ser protegidas por controles físicos de seguridad, con el apoyo de documentación actualizada y el etiquetado de los componentes esenciales, los puntos de Acceso a la red deben estar protegidos por Mecanismos de Control de Acceso, tales como, la documentación de la arquitectura de red e Integridad. 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	2) La documentación de la arquitectura de la red e integridad no es un mecanismo de control de acceso. 5) Aclarar el análisis de mantenimiento no se entiende. 5) f) requerimos que se detalle más información sobre el tipo de análisis que se requiere y a qué se refieren con que sea independiente.

	de Acceso individualizado por cada tercero, mecanismos de autorización de Acceso a los sistemas mediante credenciales únicas especializadas y su revocación tras la finalización del mantenimiento; f) Elaborar un análisis independiente de las labores de mantenimiento remoto; g) Supervisar los mantenimientos remotos durante su realización. Una vez terminadas las sesiones de mantenimiento, las sesiones de conexión deben finalizar automáticamente; h) Definir los controles para aplicaciones de gestión de mantenimiento remoto, contemplando aspectos de gestión de Acceso, análisis de origen y destino de conexiones, así como el Monitoreo Continuo de las actividades realizadas en cada sesión y la inhabilitación de la conexión tras la conclusión del mantenimiento. **f)** Elaborar un análisis independiente de las labores de mantenimiento remoto;	
Art. 38, numeral 2	Se sugiere eliminar "tales como, la documentación de la arquitectura de red e integridad", ya que no mantiene una relación con la protección de los mecanismos de control de acceso a redes.	Claridad del texto y congruencia de la norma
Art. 38, numeral 3, literal b	Se sugiere eliminar lo siguiente "así como registro de potenciales violaciones a la política de seguridad interna" debido a que esto es parte de la gestión de incidentes.	Claridad del texto y congruencia de la norma
Artículo 38	Entendemos que se debe corregir el numeral 2) pues la documentación de la arquitectura de la red e integridad no es un mecanismo de control de acceso. En el **numeral 5)** solicitamos aclarar a qué se refiere el análisis de mantenimiento y en su literal **5) f)** atentamente requerimos que se detalle más información sobre el tipo de análisis que se requiere y a qué se refieren con que sea independiente	Aclaración para aplicación normativa
Art. 38, numeral 5, literal g	Se sugiere delimitar que esto aplica cuando el mantenimiento es realizado por un tercero.	Claridad del texto y congruencia de la norma

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 38, numeral 6, literal c	Se propone la modificación del artículo para que se lea: "Cifrado de conexiones inalámbricas". La forma o metodología de cifrado no debería ser estazblecida en la norma, sino determinada en función del nivel de riesgo y la tecnología disponible.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos
Art. 38, numeral 6, literal d	Se propone la modificación del artículo para que se lea: "Inventario de dispositivos de puntos de acceso redes inalámbricas"	Claridad del texto
Art. 38, numeral 6, literal j	Se sugiere eliminar el literal J, debido a que este punto no se relaciona con las redes inalámbricas	Claridad del texto y congruencia de la norma
Art. 38, numeral 7, literal b	Se recomienda que modifique para que se lea: b) Controles generales de red, y se elimine el resto, ya que estos controles deben ser determinadas de acuerdo con el perfil de riesgos de cada institución.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos
Art. 38, numeral 7, literales c y d	Se sugiere que se eliminen ya que estos controles deben ser determinados de acuerdo con el perfil de riesgos de cada institución.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos
Art. 38, numeral 7, literal e	Se recomienda que modifique para que se lea: e) Documentación de cambios realizados a las configuraciones de los servicios de telefonía y conferencia, debido a que estos controles deben ser determinadas de acuerdo con el perfil de riesgos de cada institución.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos
Art. 39 Dispositivos Móviles.	Dispositivos móviles	No se hace referencia a si los dispositivos son los dispositivos provistos por la Institución o si se considera en el alcance dispositivos personales.
Art. 40 Comunicaciones electrónicas.	Mensajería instantánea	No es clara la definición de controles a implementar, no menciona si la captación de operaciones está permitida o restringida.
Artículo 40 sobre comunicaciones electrónicas.	El numeral 1, literal a) establece que los correos electrónicos deberán contener firma digital. Sugerimos que esta obligación se encuentre limitada a correos electrónicos que versen sobre informaciones confidenciales o sensibles y a	Artículo 3 numeral 9 de la Ley 107-13 Principio de Proporcionalidad.

	aquellos enviados por altos ejecutivos de los participantes del mercado. Lo anterior, basado en que la obtención de firmas digitales para todos los colaboradores de los participantes del mercado de valores podría implicar complicaciones operativas y mayores costos operativos, limitando así las operaciones de participantes de menor volumen.	
Título II, Capítulo V, Artículo 40	**Sugerimos añadir la siguiente frase:** **"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, **conforme al Marco de Trabajo elegido por el participante del mercado de valores**, incluyendo: […]"	Debe obedecer al modelo de negocio o marco de trabajo elegido.
Artículo 41	En el entendido de que cada tipo de participante y cada tipo de servicio es distinto, sugerimos no enumerar y eliminar así: **"Párrafo.** En los casos que los servicios provistos consideren Información financiera u otro tipo de Información sensible, los participantes del mercado de valores deben solicitar a la entidad proveedora una evaluación enfocada en los Riesgos de Integridad, disponibilidad y Confidencialidad. Dicha evaluación debe ser realizada por un tercero independiente utilizando modelos de reportes de Riesgo y controles en la provisión de servicio. ~~(Tal como: SOC 2, etc., u otras que puedan aplicar conforme a la naturaleza del servicio contratado).~~" Aclarar si se indica que todos los proveedores deben de ser realizado por terceros ejemplificando SOC. Favor indicar si el participante tiene la opción de hacerlo según la política y proceso de evaluación que tengan la entidad de Tercerizado.	Libertad para escoger el marco y el modelo a implementar.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 41 Gestión de proveedores externos	Gestión de proveedores externos	¿Se indica que todos los proveedores deben de ser realizado por terceros ejemplificando SOC2? ¿Tenemos la opción de hacerlo según la política y proceso de evaluación que tengan la entidad de Tercerizado?
Art. 41, numeral 3	Considerando que sólo sería necesario analizar los riesgos si la solución criptográfica no cumple con las recomendaciones de la industria, recomendamos que este lineamiento es cuando aplique.	Claridad del texto y del alcance de la obligación
Artículo 43	**Artículo 43. Desarrollo de sistemas ~~subcontratados~~.** Los participantes de mercado de valores que mantengan en su estructura orgánica un área de desarrollo de sistemas, deben establecer un proceso de gestión de desarrollo de sistemas que contemple: […]	El artículo se refiere al participante del mercado de valores que tiene un área de desarrollo de sistemas en su estructura orgánica, por lo que sugerimos eliminar la palabra subcontratado, dado a que no le aplica.
Art. 43	Se propone la modificación del artículo y se redacte de la forma siguiente: “Desarrollo de sistemas subcontratados. Los participantes de mercado de valores que tercericen el servicio de desarrollo de software…” Se sugiere además revisar los requisitos de este artículo, debido a que los mismos son aplicables para desarrollo interno y no para el desarrollo subcontratado.	Claridad del texto y congruencia de la norma
Art. 43, numeral 2),	Se sugiere eliminar la palabra “producción” y colocar “desarrollo” para que se lea: “…los ambientes de preproducción (aseguramiento de la calidad) y desarrollo”	Claridad del texto y congruencia de la norma Mejor Práctica
Art. 44	Se sugiere eliminar la palabra “producción” y colocar “desarrollo” para que se lea: “… ambientes de preproducción (aseguramiento de la calidad) y desarrollo”.	Claridad del texto y congruencia de la norma Mejor Práctica

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 44 sobre Entornos de desarrollo de sistemas.	Sugerimos agregar las definiciones de los términos “entornos productivos”, “entornos de desarrollo” y “ambientes de producción” para mayor facilidad en la interpretación y aplicación del Reglamento.	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa.
Título II, Capítulo VI, Art. 44	Duplicado con el Art. 43 acápite 2	
Art. 46 Información a la Superintendencia.	Información a la Superintendencia. Los participantes del mercado de valores deben informar formalmente a la Superintendencia del Mercado de Valores (en lo adelante, la “Superintendencia”), a más tardar el día hábil siguiente, sobre la ocurrencia y las acciones tomadas para corregir los siguientes eventos. 4: La ocurrencia de Incidentes de seguridad relacionados con la realización exitosa de ataques externos o penetración a los sistemas de la entidad a través de los servicios de red y comunicaciones, previamente reportados al SPRICS;	El día hábil siguiente es muy rápido para el reporte, existen incidentes que incluso 48 horas no se tiene una conclusión definitiva de lo sucedido requerimos aumentar el plazo 4) No es claro la mecánica de los reportes de ataques exitosos, se dice previamente reportados al SPRICS, la redacción puede ser más específica. Sugerimos se defina porque medio se estará notificando a la SIMV de la ocurrencia de eventos y acciones tomadas, bajo qué criterios de criticidad, y si se tomaran los mismos criterios reportados al SPRICS en materia de categorización de eventos que conlleven a la Confidencialidad, Integridad y Disponibilidad de la información e infraestructura de TI.
Art. 46 Información a la Superintendencia.	Información a la Superintendencia. Los participantes del mercado de valores deben informar formalmente a la Superintendencia del Mercado de Valores (en lo adelante, la “Superintendencia”), a más tardar el día hábil siguiente, sobre la ocurrencia y las acciones tomadas para corregir los siguientes eventos. 3)La toma de decisión formal de realizar cambios en la plataforma central de operaciones y sistemas computarizados;	El día hábil siguiente es muy rápido para el reporte, existen incidentes que incluso 48 horas no se tiene una conclusión definitiva de lo sucedido requerimos aumentar el plazo. 3) Se sugiere eliminar. 4) No es claro la mecánica de los reportes de ataques exitosos, se dice previamente reportados al SPRICS, la redacción puede ser más específica. Sugerimos se

	4: La ocurrencia de Incidentes de seguridad relacionados con la realización exitosa de ataques externos o penetración a los sistemas de la entidad a través de los servicios de red y comunicaciones, previamente reportados al SPRICS; 5: La toma de decisión formal de implementar o cambiar la plataforma tecnológica utilizada para proporcionar servicios financieros por medios electrónicos;	defina porque medio se estará notificando a la SIMV de la ocurrencia de eventos y acciones tomadas, bajo qué criterios de criticidad, y si se tomaran los mismos criterios reportados al SPRICS en materia de categorización de eventos que conlleven a la Confidencialidad, Integridad y Disponibilidad de la información e infraestructura de TI. 5) Se sugiere eliminar este punto.
Artículo 46	Sugerimos considerar: 1. Establecer mediante cuál herramienta se remitirá esta información a la Superintendencia del Mercado de Valores; 2. Crear una unidad especializada que maneje esta información sensible; y, 3. Tomar en cuenta que las SAFIs no son parte de las SPRICS, por lo tanto no les debe aplicar el numeral 4. 4. No es clara la mecánica de los reportes de ataques exitosos, se dice previamente reportados al SPRICS, la redacción puede ser más específica. Sugerimos se defina por cuál medio se estará notificando a la SIMV de la ocurrencia de eventos y acciones tomadas, bajo qué criterios de criticidad, y si se tomaran los mismos criterios reportados al SPRICS en materia de categorización de eventos que conlleven a la Confidencialidad, Integridad y Disponibilidad de la información e infraestructura de TI. 5. Definir un plazo mayor al día hábil siguiente para el reporte, pues existen incidentes que incluso 48 horas no se tiene una conclusión definitiva de lo sucedido requerimos aumentar el plazo.	Realidad de la operatividad del mercado.
Art. 46, numerales 3 y 6	Se recomienda especificar el alcance de este requisito, pues entendemos que no deben reportarse todos los cambios de la plataforma y sistemas.	Claridad del texto y delimitación de la obligación. Existen diversos tipos de cambios que pueden ser realizados en los sistemas y consideramos no sostenible informar sobre todos ellos a la SIMV debido a que no agrega valor a su gestión.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 47	Adicionar la siguiente frase: "3) Análisis de Riesgos asociados al uso de soluciones criptográficas, incluyendo los algoritmos de Encriptación, **conforme al Marco de Trabajo elegido por el participante del mercado de valores**;"	Debe obedecer al modelo de negocio o marco de trabajo elegido.
Art. 48	Se sugiere modificar la parte infine con la siguiente redacción: "…Bases de Datos que permitan determinar las vulnerabilidades, impacto potencial y mejor curso de acción para corregir cada Vulnerabilidad."	Claridad del texto y congruencia de la norma
Artículo 49	Adicionar la siguiente frase: **"Artículo 49. Sincronización de reloj de sistemas e Infraestructura Tecnológica.** Los sistemas de procesamiento de Información relevantes o de dominio de seguridad de los participantes del mercado de valores debe estar sincronizados para asegurar la exactitud de los registros de auditoría, los cuales podrán requerirse para investigaciones o como pruebas en acciones legales o disciplinarias. Al efecto, se deben establecer las políticas y Procedimientos internos, **conforme al Marco de Trabajo elegido por el participante del mercado de valores**."	
Artículo 50	Sugerimos aclarar quiénes serían catalogados como "usuarios privilegiados" y reducir la periodicidad de las revisiones porque no siempre más es mejor. **"Artículo 50. Registros y monitoreo de los usuarios administradores.** Los participantes del mercado de valores deben contar con políticas, Procedimientos y mecanismos para proteger, revisar y registrar las actividades realizadas por los usuarios privilegiados de los sistemas e Infraestructura Tecnológica. Las revisiones deben realizarse **semestralmente** ~~por lo menos cinco (5) veces al año~~."	Optimización de recursos de los participantes del mercado.
Art. 50	Se sugiere que, en lugar de una frecuencia específica para las revisiones, estas sean en función de hallazgos anteriores y de la necesidad del negocio.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos
Art. 50 Registros y monitoreo de los usuarios administradores.	Registros y monitoreo de los usuarios administradores. Los participantes del mercado de valores deben contar con políticas, Procedimientos y mecanismos para proteger, revisar y registrar las actividades realizadas por los usuarios privilegiados de los sistemas e Infraestructura Tecnológica. Las revisiones deben realizarse por lo menos cinco (5) veces al año.	Consideramos que, bajo reglamento, un mínimo de 5 veces al año es bastante, entiendo que este podría considerarse 2 veces al año como mínimo. En este punto nuestra consulta es ¿sobre si las revisiones van sobre las actividades realizadas en el

		sistema o sobre los usuarios con privilegios de administrador?
Artículo 50 sobre Registros y monitoreo de los usuarios administradores.	Sugerimos la reevaluación de la periodicidad establecida, toda vez que la propuesta del Reglamento dispone que "*las revisiones deben realizarse por lo menos cinco (5) veces al año"* de manera que dicha frecuencia pueda ser definida por cada participante con base a criterios de evaluación de riesgo. Esto, considerando que la necesidad de la periodicidad puede variar de un participante a otro atendiendo a la complejidad de la infraestructura y los controles compensatorios automatizados mediante el uso de herramientas implementadas para esos fines.	Artículo 3 numeral 4 de la Ley 107-13 Principio de racionalidad.
Título II, Capítulo VII, Art. 51	El acápite 3 "Dispositivos Personales" no tiene relación con el "Ciclo de vida del desarrollo de sistemas y aplicaciones".	Dicho acápite debe pertenecer al Art. 39 "Dispositivos Móviles"
Art. 51, numeral 3	Se sugiere eliminar de los requisitos toda vez que el mismo no se relaciona con el Desarrollo de Software.	Claridad del texto y congruencia de la norma
Artículo 51, numeral 4)	Estas actividades también deben ser acordes con el marco elegido por cada participante: "4) **Compilación de sistemas y aplicaciones:** Las actividades de compilación de los sistemas y aplicaciones, incluyendo la codificación y personalización de paquetes, deben llevarse a cabo **de conformidad con el Marco de Trabajo** ~~de la industria~~ **elegido por el participante del mercado de valores**, 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;"	Debe obedecer al modelo de negocio o marco de trabajo elegido.
Art. 51, numeral 6	Se sugiere eliminar de la redacción del artículo "pruebas de intrusión" debido a que no siempre se debe o puede hacer pruebas de intrusión. Se debe delimitar el alcance a cambios significativos en la aplicación.	En base a las mejores prácticas los controles deben ser definidos en base al análisis de los riesgos

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 52 Gobierno de Seguridad Cibernética y de la Información.	Gobierno de Seguridad cibernética y de la información	Concepto de **adecuado** gobierno de Seguridad cibernética y de la Información, avaluar eliminar la palabra adecuado. Art. 52 Arreglar la palabra cibernética.
Artículo 52	Consideramos que todo lo solicitado normativamente debe ser suficiente y adecuado, por lo cual creemos se debe borrar esa palabra que resulta subjetiva: "**Artículo 52.** Gobierno de Seguridad Cibernética y de la Información. Los participantes del mercado de valores deben contar con ~~un adecuado~~ Gobierno de Seguridad Cibernética y de la Información, (…)"	Apreciación positiva de la normatividad vigente.
Artículo 53	Sugerimos hacer constatar en el documento que estas funciones del consejo dependen de la estructura de gobierno que exista en las instituciones, ya que muchos de estos aspectos van delegados a comités que se reportan a los consejos administrativos y luego de consumados se reportan a la alta gerencia, (consejos administrativos) para su evaluación y posterior aprobación, haciendo de estos comités más funcionales. Solicitamos aclarar la diferencia entre Gobierno y Programa en el numeral 4). Sugerimos eliminar la palabra "Garantizando la supervisión" en el numeral 6). Sugerimos cambiar por palabras "Asignar y Verificar" por decidir, aprobar, evaluar. Sugerimos que las responsabilidades de los numerales 3), 6), 7), 8), 9), 10) y 13) se eliminen y sean de la competencia del Comité o Subcomité Funcional de Seguridad Cibernética y de la Información: "(…) ~~6) Evaluar y aprobar las decisiones relativas a tecnología de la Información y velar que se han adoptado en línea con las estrategias y objetivos del participante del mercado de valores, garantizando la supervisión de los procesos de manera efectiva y transparente, el cumplimiento de los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del consejo de administración;~~	Mayor armonización regulatoria.

	~~7) Velar para que los Riesgos relacionados con Tecnología de la Información no excedan la tolerancia de Riesgo de la entidad;~~ ~~8) Evaluar que las adecuadas y suficientes capacidades relacionadas con la seguridad de Tecnología de la Información estén disponibles para soportar eficazmente los objetivos del participante del mercado de valores;~~ ~~9) Velar por el cumplimiento en la implementación de sistemas de Información propios, adquiridos o subcontratados, con la normativa vigente aplicable;~~ ~~10) Adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o Acceso no autorizado;~~ 11) ~~Evaluar~~, aprobar ~~y poner en funcionamiento~~ el Plan de Continuidad de Negocios, Plan de Contingencia y programas de pruebas de estrés, como parte de su proceso de gestión integral de Riesgo; 12) Asegurar que exista un sistema adecuado de delegación de responsabilidades y segregación de funciones en la entidad; y, ~~13) Asignar y verificar el cumplimiento de las funciones y responsabilidades de Seguridad Cibernética y de la Información para los roles definidos en el área correspondiente.~~”	
Art. 53 Responsabilidad del consejo de administración	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 […]:	Estas funciones deben ser propias del Comité de Ciberseguridad, mas no del Consejo de Administracion de una entidad. Lo primero es que, conforme los perfiles a los cuales están condicionados los PB para el cumplimiento del reglamento de gobierno corporativo no existen el perfil de conocimiento en aspecto de TI y menos de ciberseguridad. Esto es un tema meramente

		técnico y operativo, que no debe ser delegado a los miembros del consejo de administración, sino mas bien, al comité, quien este último estará apoyando al consejo de administración, y dando a conocer las políticas previamente aprobadas por este, pudiendo inclusive, el consejo, ratificarlas o modificarlas
Art. 53 Responsabilidad del consejo de administración	Responsabilidad del consejo de administración.	Sugerimos hacer constatar en el documento que estas funciones del consejo dependen de la estructura de gobierno que exista en las instituciones, ya que muchos de estos aspectos van delegados a comités que se reportan a los consejos administrativos y luego de consumados se reportan a la alta gerencia, (consejos administrativos) para su evaluación y posterior aprobación, haciendo de estos comités más funcionales. por ejemplo, en el mencionado en el artículo 54 de este reglamento. 4) Aclarar la diferencia entre Gobierno y Programa. 6) Sugerimos eliminar la palabra "Garantizando la supervisión". 10) Consejo de Admin no evalúa aspectos técnicos. Las políticas son aprobadas por tal vía. 13) Sugerimos cambiar por palabras "Asignar y Verificar" por decidir, aprobar, evaluar.
Artículo 53 sobre Responsabilidad del Consejo de Administración	En los numerales 2 y 4 se hace referencia a los siguientes conceptos: *sistema de gestión de seguridad cibernética y de la información* y *programa de seguridad cibernética y de la información*. En este sentido, sugerimos que sean elaborados estos conceptos de manera que puedan ser delimitadas las diferencias técnicas o de aplicación y las tareas de estas disposiciones se ejecuten de forma clara y precisa por el participante del mercado. Por otro lado, el numeral 10 establece que el Consejo de Administración deberá "*Adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y*	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa. Reglamento de Gobierno Corporativo, rectificado por la Cuarta Resolución del Consejo Nacional del Mercado de Valores, R-CNMV-2023-04-MV, de fecha 7 de febrero de 2023.

	eviten su alteración, pérdida, tratamiento, consulta o Acceso no autorizado". Entendemos oportuno que esta responsabilidad recaiga sobre el Comité funcional de Seguridad Cibernética y de la Información, toda vez que la función antes citada es de carácter operativo y las responsabilidades del Consejo de Administración son estratégicas con relación a la aprobación de presupuestos e iniciativas que apoyan el programa de seguridad de la información. Finalmente, con relación al numeral 11, entendemos oportuno recomendar que esta función para la puesta en funcionamiento sea establecida como una responsabilidad del Comité funcional de Seguridad Cibernética y de la Información considerando que esta tarea dispone de funciones operativas que no necesariamente deban ser realizadas por los miembros del Consejo de Administración.	
Art. 53	Tal y como comentamos anteriormente, en base a las buenas prácticas de gobierno corporativo, el rol del Consejo de Administración debe ser segregado de la operatividad de la empresa, de la cual es responsable la Administración. En tal virtud, recomendamos eliminar de las responsabilidades asignadas al Consejo las siguientes por tratarse de funciones con un matiz operativo: 6); 8); 10); 11); y 13)	Principios de Gobierno Corporativo de la OCDE (principio IV) Guía Práctica de Gobierno Corporativo, Experiencias del Cirulo de Empresas de la Mesa Redonda Latinoamericana Reglamento de Gobierno Corporativo: Artículo 14
Artículo 54 sobre el Comité funcional de Seguridad Cibernética y de la Información.	*1.* Recomendamos eliminar la responsabilidad del Comité funcional establecida en el *numeral 4)* de la propuesta de reglamento, que indica: *"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;"* Entendemos que esta función es operativa y debe estar a cargo del oficial de seguridad de la información, que puede ser el personal designado, tal como indica el *artículo 38, Gestión de la Red, numeral 3),* quien deberá	Artículo 3 Numeral 8 de la Ley 107-13 Principio de seguridad jurídica, de previsibilidad y certeza normativa. Reglamento de Gobierno Corporativo, rectificado por la Cuarta Resolución del Consejo Nacional del Mercado de Valores, R-CNMV-2023-04-MV, de fecha 7 de febrero de 2023.

	realizar una evaluación de los requerimientos de seguridad establecidos y análisis de riesgos que sustenten la factibilidad de las conexiones externas verificadas. Asimismo, establecer que estas se encuentren debidamente documentadas para verificaciones solicitadas y que se presente al comité funcional de manera informativa. 2. Proponemos sea modificado el párrafo I, del artículo 54 y se incorpore un párrafo adicional, con el objetivo de mantener coherencia con las estructuras y funciones de los comités dispuestas en el Reglamento de Gobierno Corporativo, así como, las funciones y responsabilidades establecidas para los miembros del Consejo de Administración. En otro orden y a fines de que el *Comité funcional de Seguridad Cibernética y de la Información* cumpla con la funcionalidad, operatividad y estructura del participante, recomendamos que, adicionalmente, las atribuciones que le correspondan puedan ser asumidas por uno de comités ya conformados por el participante, con funciones de naturaleza similar. Por tanto, sugerimos la siguiente redacción: *"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, quienes podrán ser miembros ejecutivos internos del participante del mercado de valores, designado por el Consejo de Administración.* *Párrafo II. El comité funcional de Seguridad Cibernética y de la Información podrá ser asumido por el comité de riesgos u otro comité de naturaleza similar de acuerdo con la composición establecida por el Reglamento de Gobierno Corporativo de la entidad."*	

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 54 Comité funcional de Seguridad cibernéticas y de la información	Párrafo I. El comité funcional de Seguridad Cibernética y de la Información estará integrado por un número impar, como mínimo, de tres (3) miembros con voz y voto: a) Un miembro del consejo de administración que no ocupe cargos ejecutivos en el participante del mercado de valores, quien lo presidirá. b) El ejecutivo principal del participante del mercado de valores; y, El oficial de seguridad cibernética y la Información, quien fungirá como secretario	¿Es valida la figura del Comité de Ciberseguridad del Centro Financiero donde se puedan tratar los temas de Puesto de Bolsa como parte del gobierno corporativo del Centro? Aclarar el alcance. Entendemos oportuno homologar criterio conforme el reglamento de ciberseguridad de BCRD. Conforme los perfiles condicionados y establecidos en el Reglamento de Gobierno Corporativo de esta SIMV, no esta incluido el perfil de Ciberseguridad y Seguridad informática. Esto es un tema totalmente técnico, que es de alcance y conocimiento de todos, ya que es una materia especializada. En ese sentido, entendemos que se debe desestimar incluir a un miembro del consejo como parte de este comité
Art. 54 Comité funcional de Seguridad cibernéticas y de la información	Comité funcional de Seguridad cibernéticas y de la información	¿Es valida la figura del Comité de Ciberseguridad del Centro Financiero donde se puedan tratar los temas de Puesto de Bolsa como parte del gobierno corporativo del Centro? Aclarar el alcance. 1) Sugiere cambiar la palabra “determinados” por evaluados y aprobados. 4) Sugiere eliminar de la aprobación del comité, por ser operativa. 5) Sugiere cambiar la palabra “Ratificar” Párrafo I. Se sugiere que Eliminar obligación de que sea un Ejecutivo "Principal", que exista la posibilidad de que sea un "Ejecutivo"
Art. 54, numeral 5	En relación con este numeral de este artículo se recomienda tomar en consideración que no aplica para todas las organizaciones, ya que en las empresas donde existe una gestión integral de riesgo y en este caso el responsable de este proceso es el Ejecutivo de Gestión de Riesgo.	

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 54, Párrafo I	En vista de las observaciones realizadas anteriormente en el artículo 6 numeral 2 sobre el rol del consejo de administración, las competencias de los consejeros y las responsabilidades legales de estos, solicitamos eliminar la exigencia de que un miembro del consejo de administración sea parte del comité funcional. Destacamos que, tal y como se evidencia en el referido artículo, dicho comité posee funciones operativas y técnicas que, en base a las mejores prácticas, no deben ser asignadas a un consejero, más aún cuando dicho consejero será responsable civilmente de las consecuencias derivadas de la aprobación realizada. En este sentido, sugerimos alinear las disposiciones del Proyecto de Reglamento sobre la conformación del comité funcional a las disposiciones del Reglamento de Seguridad Cibernética y de la Información.	Principios de Gobierno Corporativo de la OCDE (principio IV) Guía Práctica de Gobierno Corporativo, Experiencias del Cirulo de Empresas de la Mesa Redonda Latinoamericana Reglamento de Gobierno Corporativo: Artículo 14 Reglamento de Seguridad Cibernética y de la Información de la JM: Artículo 7
Artículo 54, Párrafo	Solicitamos considerar la siguiente redacción: "**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~~ **participe en el** mercado de valores, quien lo presidirá. b) ~~El ejecutivo principal del participante del mercado de valores~~ **Un miembro de la Alta Gerencia designado por el Consejo de Administración**; y, c) El oficial de seguridad cibernética y la Información, quien fungirá como secretario.	La criticidad y naturaleza de este comité, el cual requiere que sus miembros se encuentren permanentemente disponibles para la toma de decisiones, ante la materialización de escenarios de alto riesgo a la entidad.
Artículo 55	Entendemos que el Comité es un órgano de apoyo al Consejo de Administración, al cual debe hacer las recomendaciones y señalamientos de interés en esta materia tan especializada, por lo que es este organismo especial, que conoce los temas de seguridad cibernética y de la información, al que se debe reportar el Oficial de Seguridad Cibernética y la Información, considerando que dan seguimiento continuo a su gestión. Lo mismo vemos en	Lineamientos y estándares usuales de gobierno corporativo. Se sugiere alinearse al Art 29, Reglamento de Gob. Corporativo del MV

	otras áreas como son: Riesgos y Prevención de Lavado de Activos y Financiamiento del Terrorismo. 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. Proponemos la siguiente redacción: ***Artículo 55. Estructura gerencial y funciones de control de Seguridad Cibernética y de la Información. Los participantes del mercado de valores deben contar con una estructura gerencial para el control de Seguridad Cibernética y de la Información, acordes a su naturaleza, tamaño, y complejidad. El programa establecido en el marco de las responsabilidades definidas en este Reglamento será dirigido por la unidad funcional de Seguridad Cibernética y de la Información, la cual estará a cargo del oficial de Seguridad Cibernética y la Información y reportará al Comité Funcional de Seguridad Cibernética y de la Información.***	
Art. 55	El principal ejecutivo de la entidad es el responsable de la administración ordinaria de la sociedad, de ejecutar las estrategias y lineamientos del Consejo de Administración y ejecutar las acciones necesarias para el logro de los objetivos de la empresa. A estos fines, requiere un equipo de ejecutivos que le ofrezcan el soporte necesario, incluyendo el oficial de seguridad de la información. A diferencia de un auditor interno, las funciones que ejerce el oficial de seguridad de la información no requieren para su efectividad de la independencia de la Administración. En consideración de las observaciones realizadas sobre la segregación de funciones del Consejo de Administración y la Administración, solicitamos eliminar la exigencia de que el oficial de seguridad de la información se reporte directamente al Consejo de Administración.	Principios de Gobierno Corporativo de la OCDE (principio IV) Guía Práctica de Gobierno Corporativo, Experiencias del Cirulo de Empresas de la Mesa Redonda Latinoamericana Reglamento de Gobierno Corporativo: Artículo 14 Reglamento de Seguridad Cibernética y de la Información de la JM: Artículo 10

	En este sentido, sugerimos alinear las disposiciones del Proyecto de Reglamento sobre el oficial de seguridad de la información a las disposiciones del Reglamento de Seguridad Cibernética y de la Información.	
Artículo 55. Estructura gerencial y funciones de control de Seguridad Cibernética y de la Información	Artículo 55. Estructura gerencial y funciones de control de Seguridad Cibernética y de la Información. Los participantes del mercado de valores deben contar con una estructura gerencial para el control de Seguridad Cibernética y de la Información, acordes a su naturaleza, tamaño, y complejidad. El programa establecido en el marco de las responsabilidades definidas en este Reglamento será dirigido por la unidad funcional de Seguridad Cibernética y de la Información, la cual estará a cargo del oficial de Seguridad Cibernética y la Información y reportará directamente al consejo de administración	Insistimos en unificar criterio con el reglamento de ciberseguridad de BCRD. No podemos tener dos reguladores distintos con criterios diferentes sobre una misma materia. Dado que es un área totalmente operativa, técnica y de ejecución permanente e inmediata, es imposible que el CISO deba reportar directamente al consejo de administración, y esperar la aprobación o directrices de estos para desempeñar su rol. Para esto, esta la Dirección General (Alta Gerencia) e igualmente el comité de ciberseguridad, quienes estarán prestos al día a día operativo, que eventualmente serán conocidos, su ejecución conforme el programa de ciberseguridad anual de la entidad, al consejo de administración. Como parte de su rendición de cuenta o en su defecto, para conocer cualquier política que incida significativamente en la administración u operatividad de la empresa
Artículo 55. Estructura gerencial y funciones de control de Seguridad Cibernética y de la Información	Los participantes del mercado de valores deben contar con una estructura gerencial para el control de Seguridad cibernética y de la lnformaci6n, 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 lnformaci6n, la cual estará a cargo del oficial de Seguridad cibernética y la información y reportará directamente al consejo de administración.	Se sugiere alinearse al Art 29, Reglamento de Gob. Corporativo del MV, que considera Evaluar el art. 56 que aplica de igual forma.
Artículo 55 sobre Estructura gerencial y	Recomendamos modificar la redacción del artículo 55 eliminando la frase "(…) *la cual estará a cargo del oficial de Seguridad Cibernética y de la*	N/A

funciones de control de Seguridad Cibernética y de la Información	*Información y reportará directamente al Consejo de Administración"* de manera que dicho artículo sea reemplazado por el propuesto a continuación: *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 estará dirigido por la unidad funcional de Seguridad Cibernética y de la Información".* Lo anterior, en vista de que la función contemplada en este artículo puede ser suplida mediante el reporte de actividades al comité funcional de Seguridad Cibernética y de la Información u otros órganos intermedios donde se traten temas relacionados a la seguridad de la información.	
Artículo 56	Indicar si este Oficial puede ser un tercerizado o un profesional independiente del área de ciberseguridad.	Alternativas para contratación del más apropiado capital humano.
Artículo 56. Oficial de Seguridad Cibernética y de la Información	El oficial de Seguridad Cibernética y de la lnformaci6n 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 Informaci6n, debe tener suficiente autoridad e independencia para cumplir con sus responsabilidades.	Recomendamos aplicar las observaciones del ítem anterior
Artículo 57, numerales	Evaluar la siguiente propuesta de redacción: 1) Desarrollar, implementar y mantener actualizado el programa de Seguridad Cibernética y de la Información, el cual debe ser revisado y actualizado una vez al año; 2) Presentar informes periódicos o, al menos, un informe anual al consejo de administración sobre el contenido, aplicabilidad y actualización de las políticas establecidas en materia de Seguridad Cibernética y de la Información;	

	~~3) Implementar políticas, estándares y Procedimientos apropiados para apoyar el programa de Seguridad Cibernética y de la Información;~~ 4) Asignar las responsabilidades de los miembros que conforman las áreas especializadas; 5) Gestionar las acciones para el tratamiento del Riesgo tecnológico en coordinación con las áreas pertinentes del negocio; 6) ~~Cumplir~~ **Validar** con los límites de los niveles de Riesgos relevantes establecidos por el consejo de administración, relacionados con Amenazas o Incidentes de Seguridad Cibernética y de la Información; 7) Monitorear permanentemente el estado de estado de la Seguridad Cibernética y de la Información y rendir informes periódicos según la necesidad sobre los hallazgos y Riesgos identificados al comité funcional de Seguridad Cibernética y de la Información; 8) Cumplir con las atribuciones asignadas y decisiones tomadas por el consejo de administración; y, 9) ~~Definir y~~ evaluar las responsabilidades de los proveedores de servicios en lo concerniente a la Seguridad Cibernética y de la Información.	
Artículo 57 sobre Responsabilidades del Oficial de Seguridad Cibernética y de la Información.	1. Con relación al numeral 2), recomendamos que esta responsabilidad recaiga sobre el Comité funcional de Seguridad Cibernética y de la Información, en lugar del Oficial de Seguridad Cibernética y de la Información. A tales fines y con relación a las responsabilidades del Oficial objeto del artículo de que se trata, proponemos la siguiente redacción: “Recomendar actualizaciones a las políticas establecidas en materia de Seguridad Cibernética y de la Información ante el Consejo de Administración”. Esta modificación permitiría que se conozcan oportunamente las desviaciones y si es necesario el órgano superior apruebe las recomendaciones más estratégicas para el logro de los objetivos y requerimientos de seguridad de la información. 2. Para el numeral 4), recomendamos incluir la definición de “áreas especializadas”.	Artículo 3 numeral 4 de la Ley 107-13. Principio de racionalidad. Segregación de funciones Permitir la adaptación de la norma a las distintas estructuras de los participantes del mercado

	3. En relación al numeral 5), la responsabilidad de gestionar las acciones para el tratamiento de riegos recae en el Especialista de Riesgos, para los participantes que cuentan con esta área.	
Art. 57 Responsabilidades del oficial de Seguridad Cibernética y de la Información.	**Numeral 7** Monitorear permanentemente el estado de estado de la Seguridad Cibernética y de la Información y rendir informes periódicos según la necesidad sobre los hallazgos y Riesgos identificados al comité funcional de Seguridad Cibernética y de la Información;	**Corregir Ortografía:** el estado de estado de la Seguridad
Art. 57 Responsabilidades del oficial de Seguridad Cibernética y de la Información.	**Numeral 7** Monitorear permanentemente el estado de estado de la Seguridad Cibernética y de la Información y rendir informes periódicos según la necesidad sobre los hallazgos y Riesgos identificados al comité funcional de Seguridad Cibernética y de la Información;	**Corregir Ortografía:** el estado de estado de la Seguridad. 1) Eliminar palabra “Mantener”. 3) Eliminar por completo. 4) Definir cuáles son las áreas especializadas. 6) Cambiar la palabra “Cumplir” por Gestionar o validar los niveles de riesgo. 9) Sugerir dejar solo Evaluar, eliminar la palabra “Definir”.
Art. 57, numeral 4	Se recomienda incluir la definición de áreas especializadas.	Claridad del texto
Art. 57, numeral 5	Ese acápite no aplica para todas las organizaciones, debido a que en las empresas donde existe una gestión integral de riesgos, el responsable de este proceso es el Ejecutivo de Gestión de Riesgos.	Segregación de funciones Permitir la adaptación de la norma a las distintas estructuras de los participantes del mercado
Art. 57, numeral 6	Se propone modificar el artículo para que se lea de la siguiente forma: “Cumplir con los límites de los niveles de Riesgos relevantes establecidos por el consejo de administración”, eliminado el resto de la oración para no hacerlo limitativo.	Claridad del texto

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 57, numeral 9	Tal y como observamos anteriormente, se recomienda delimitar alcance de la revisión a los proveedores de servicios tecnológicos con los que se mantenga una interconexión o sean críticos para el negocio.	Principio de Racionalidad La obligación establecida no considera la realidad del servicio contratado ni los riesgos asociados. Los controles exigidos deben encontrarse asociados al nivel de riesgo, a fin de que el costo del control no exceda sus beneficios.
Art. 58	Entendemos oportuno aclarar a qué se refieren con la evaluación del nivel de exposición. En caso de que se refieran a la evaluación del nivel de exposición al riesgo o perfil de riesgos de seguridad cibernética y de la información, producto de una evaluación o análisis de riesgos de la entidad, recomendamos específica, pues una evaluación del nivel de cumplimiento del Proyecto de Reglamento no necesariamente arrojaría el nivel de exposición al riesgo de la entidad.	Claridad del texto
Art. 58 Autoevaluación	Autoevaluación. Los participantes del mercado de valores deben autoevaluar su cumplimiento normativo en materia de Seguridad Cibernética y de la Información con periodicidad anual. Los resultados de dicha evaluación, así como los de la evaluación del nivel de exposición en esta materia deben presentarse anualmente al consejo de administración.	¿Para no crear lo que ya existe se podría crear vinculo donde podamos usar la herramienta de autoevaluación del BCRD o que otra herramienta estaríamos utilizando para las autoevaluaciones? No se considera la función de 3 líneas de defensa, como se plantea ese modelo, ¿impulsado por la Superintendencia y por el banco Central en términos de PB?
Art. 59	En atención a lo dispuesto en este artículo es importante aclarar que la supervisión del programa de Seguridad Cibernética y de la información, ni el estado de esta debe ser responsabilidad de auditoría interna, sino del oficial de seguridad. Auditoría interna debe verificar o evaluar el cumplimiento con las disposiciones de este reglamento, las políticas internas definidas por la institución en materia de seguridad de la información, controles implementados y demás lineamientos aplicables.	Naturaleza independiente del auditor interno en base a las mejores prácticas de gobierno corporativo

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Artículo 59	En el caso de participantes del mercado que pertenecen a grupos financieros con entidades de intermediación financiera, ¿se podría crear vinculo donde podamos usar la herramienta de autoevaluación del BCRD para no crear lo que ya existe o que otra herramienta estaríamos utilizando para las autoevaluaciones?	**Mayor homogeneización y armonización entre Reguladores y la autoridad monetaria y financiera**
Artículo 60	Aclarar las evaluaciones de terceros independientes y quienes estarían calificados para hacerlo. Adicionalmente, sugerimos redactarlo así: "**Artículo 60. Evaluación de un tercero independiente**. Los participantes del mercado de valores deben realizar evaluaciones independientes sobre el cumplimiento normativo en materia de Seguridad Cibernética y de la Información, con una periodicidad no mayor de tres (3) años. **Párrafo I.** La evaluación inicial se llevará a cabo dentro de los tres (3) años contados a partir de la entrada en vigencia de este Reglamento. **Párrafo II.** La entidad debe contar por lo menos con cinco (5) años de experiencia y con las calificaciones e independencia necesaria para realizar la evaluación. **Párrafo III.** Los participantes del mercado de valores deben presentar las auditorías realizadas por auditores externos inscritos en el Registro al consejo de administración, **previa evaluación** ~~cada vez que se realicen por parte~~ del comité de auditoría."	
Art. 60, párrafo III	Sugerimos aclarar la redacción de este artículo pues parecería que las auditorias serian realizadas por el comité de auditoría, el cual es un comité de apoyo del consejo.	Claridad del texto
Art. 60	Agradeceremos aclarar que los participantes del mercado a los que nos aplica el Reglamento de Seguridad Cibernética y de la Información dictado por la Junta Monetaria podrán remitir a la Superintendencia, el informe de auditoría independiente exigido por dicho reglamento. Ver comentarios al artículo 2, párrafo I.	Principio de utilidad y pertinencia, reconocido en el numeral 2 del artículo 4 de la Ley 167-2021. Ley 249-17: artículo 299 Principio de Racionalidad aplicable a las actuaciones de la Administración Pública

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

Art. 63	Considerando nuestra experiencia en la implementación de un sistema de gestión de seguridad de la información, basado en la Norma ISO / IEC 27001:2013, y en la experiencia por los participantes del sistema de pagos durante el proceso de adecuación al reglamento de seguridad cibernética y de la información, entendemos que el plazo de 9 meses debería ser aumentado al menos 18 tomando en cuenta los participantes que no poseen un sistema de gestión de seguridad implantado.	Principio de Racionalidad
Art. 63 Entrada en vigencia	Entrada en vigencia. Las disposiciones de este Reglamento entran en vigencia en el plazo de nueve (9) meses, contados a partir del día hábil siguiente a su publicación.	Evaluar los tiempos de implementación, 9 meses puede resultar corto sobre todo considerando los ejercicios presupuestales necesarios. No estamos en total acuerdo con la proximidad a la entrada en vigor que es dentro de 9 meses al momento del día hábil de su aplicación. Pedimos se extienda a por lo menos 1 año.
Artículo 63 sobre Entrada en Vigencia.	En vista de que en el artículo 64 se establece que los participantes deberán adecuarse a las disposiciones del Reglamento previo a su entrada en vigencia, se recomienda aumentar el plazo otorgado para la entrada en vigencia de manera que en lo adelante se lea de la manera siguiente: “Las disposiciones de este Reglamento entran en vigencia en el plazo de un (1) año, contado a partir del día hábil siguiente a su publicación”. Lo anterior, considerando que dicha adecuación implica el desarrollo de un nuevo sistema regulatorio interno, la captación de personal capacitado y la potencial inversión en infraestructura tecnológica para su posterior habilitación, todo lo cual requiere de un plazo razonable para su materialización.	Artículo 3 numeral 4 de la Ley 107-13. Principio de racionalidad.
Artículo 63	Sugerimos incrementar la entrada en vigencia a veinte cuatro (24) meses dada la envergadura de este Reglamento que incluye, elaboración e implementación de políticas, procedimientos, inversión en tecnología, infraestructura y recursos humanos.	Capacidad, posibilidad y esfuerzo de las AFI para poder implementarlo satisfactoriamente.

	Artículo 63. Entrada en vigencia. Las disposiciones de este Reglamento entran en vigencia en el plazo de ~~nueve (9)~~ **veinte cuatro (24)** meses contados a partir del día hábil siguiente a su publicación.	
Artículo 64	Sugerimos aumentar el plazo para cumplir este requerimiento, dado a que el participante del mercado de valores debe establecer el presupuesto y la asignación de los recursos, así como realizar un análisis de la brecha, de cara al cumplimiento de la regulación y realizar un plan. Les agradecemos permitir la siguiente redacción: “(…) Párrafo I. Para el fin anterior, los participantes del mercado de valores deben remitir a la Superintendencia un cronograma de adecuación gradual que, al menos, se ajuste a la siguiente distribución en su implementación: Frecuencia % ~~Año Trimestre 1~~ **Al segundo semestre** 20% ~~Año Trimestre 2~~ **Al tercer semestre** 40% ~~Año Trimestre 3~~ **Al cuarto semestre** 40% Párrafo II. El cronograma de adecuación indicado en párrafo anterior debe remitirse a la Superintendencia dentro de **noventa (90) días calendarios** ~~treinta (30) días hábiles~~, contados a partir del día hábil siguiente a la publicación de este Reglamento.”	
Artículo 64 sobre Plazo de Adecuación.	Considerando nuestros comentarios sobre el artículo anterior, sugerimos que sea modificado el cronograma de adecuación contemplado en los párrafos I y II, de manera que los participantes cuenten plazo de un (1) año en lugar de nueve (9) meses para la adecuación.	Artículo 3 numeral 4 de la Ley 107-13. Principio de racionalidad.
Art. 64 Plazo de adecuación. Los participantes	Los participantes del mercado de valores deben adecuarse a las disposiciones del presente Reglamento previo a su entrada en vigencia. **Párrafo I**. Para el fin anterior, los participantes del mercado de valores deben remitir a la Superintendencia un cronograma de adecuación gradual que, al menos, se ajuste a la siguiente distribución en su implementación:	En el artículo solicitamos la revisión y reconsideración de los tiempos especificados, consideramos que 9 meses es un periodo muy corto para estar en cumplimiento con este reglamento, teniendo en cuenta que para lograr su cumplimiento se deben realizar cambios estructurales, operacionales y culturales, además de la inversión económica que esto representa.

MATRIZ DE OBSERVACIONES PROYECTO DE REGLAMENTO SOBRE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN EN EL MERCADO DE VALORES.

	Frecuencia % Trimestre 1 20% Trimestre 2 40% Trimestre 3 40% **Párrafo II.** El cronograma de adecuación indicado en párrafo anterior debe remitirse a la Superintendencia dentro de treinta (30) días hábiles, contados a partir del día hábil siguiente a la publicación de este Reglamento. **Párrafo III.** Participantes del mercado de valores con nivel de sofisticación alto	**Párrafo III.** ¿Cuál es el criterio para saber que es un nivel alto y cuál es el mecanismo para notificación a la Superintendencia?
Título III, Capítulos I y II (Órgano de Gestión y Estructura Gerencial)	Inclusión de un párrafo aclaratorio donde permita que los participantes del mercado de valores, cuya empresa matriz sea una Entidad de Intermediación Financiera (EIF) regulada por la Superintendencia de Bancos (SB) y que se encuentren dentro del ámbito de aplicación del Reglamento de Seguridad Cibernética y de la Información emitido por la Junta Monetaria, o con cuya entidad matriz se haya suscrito la contratación de los servicios de Gestión Integral de Riesgos, Tecnología y Seguridad de la Información, puedan estar incluidos dentro del régimen de Gobierno de Seguridad Cibernética y de la Información que la EIF lleve a cabo, permitiendo que el Comité funcional de Seguridad Cibernética y de la Información, la Estructura gerencial y funciones de control de Seguridad Cibernética y de la Información y el Oficial de Seguridad Cibernética y de la Información de la EIF incluyan dentro de sus respectivas funciones y facultades lo concerniente tanto a la EIF como al participante del mercado de valores con que guarde relación por ser su matriz o tener contratados los servicios indicados con la EIF.	Evitar duplicidad de estructuras; eficientización de recursos económicos y humanos; centralización de procesos y control de riesgos. Principio de Racionalidad y Principio de Proporcionalidad, (Numerales 4 y 9, Art. 3, Ley 107-13). Importante el aporte de Freddy o quienes sean técnicos en esto, para incluir una redacción correcta que explique que el sistema de ambas entidades corre en la misma plataforma/herramienta.
Capítulo III, Título IV, Art. 64, Párrafo 3.	Considerar ampliar más y especificar a quiénes se refiere este párrafo y qué tanto nivel de avance significa puntualmente.	