**-DESIGNACION-**
RESOLUCION JM 181101-02

**-FECHA-**
2018/11/01

**-TITULO-**
SEGUNDA RESOLUCION DE FECHA 01 DE NOVIEMBRE DEL 2018 QUE AUTORIZA LA PUBLICACION DEL REGLAMENTO DE SEGURIDAD CIBERNETICA Y DE LA INFORMACION

**-MODIFICACION-**
NINGUNA

**-DESCRIPTORES-**
AUTORIZACION; PUBLICACION; REGLAMENTO; SEGURIDAD CIBERNETICA Y DE LA INFORMACION; LEY NO.183-02 MONETARIA Y FINANCIERA; ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2018-2021; RIESGO OPERACIONAL; BANCO CENTRAL; SUPERINTENDENCIA DE BANCOS; SIPARD

**-TEXTO-**
JUNTA MONETARIA
ADMINISTRACION MONETARIA Y FINANCIERA

Para los fines procedentes, se hace de público conocimiento que la Junta Monetaria ha dictado su **Segunda Resolución** de fecha **1 de noviembre del 2018**, cuyo texto se transcribe a continuación:

**"VISTA** la comunicación No.12591 de fecha 11 de septiembre del 2018, dirigida al Gobernador del Banco Central y Presidente de la Junta Monetaria por el Gerente de dicha Institución, mediante la cual remite para el conocimiento y aprobación definitiva de la Junta Monetaria, el Proyecto de Reglamento de Seguridad Cibernética y de la Información;

**VISTA** la Matriz comparativa de las observaciones al Proyecto de Reglamento de Seguridad Cibernética y de la Información;

**VISTO** el Proyecto de Reglamento de Seguridad Cibernética y de la Información;

…/

**VISTA** la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002 y sus modificaciones;

**VISTO** el Reglamento de Sanciones, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 18 de diciembre del 2003 y sus modificaciones;

**VISTO** el Reglamento de Riesgo Operacional, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 2 de abril del 2009;

**VISTO** el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos, aprobado mediante la Tercera Resolución dictada por la Junta Monetaria en fecha 16 de marzo del 2017;

**VISTO** el Decreto No.230-18 que establece y regula la Estrategia Nacional de Ciberseguridad 2018-2021, de fecha 19 de junio del 2018;

**VISTA** la Tercera Resolución adoptada por la Junta Monetaria en fecha 12 de abril del 2018, que autorizó la publicación para fines de consulta de los sectores interesados, del Proyecto de Reglamento de Seguridad Cibernética y de la Información;

**VISTOS** los demás documentos que integran este expediente;

**CONSIDERANDO** que expresa la Gerencia del Banco Central, que esta normativa ha sido desarrollada como respuesta a los incidentes de seguridad cibernética acaecidos en los sistemas monetarios y financieros de otras economías del mundo, cuyos efectos y consecuencias han elevado la prioridad dada a este tema a nivel internacional. Igualmente, debido a la digitalización e interconexión acelerada de todos los servicios y sistemas financieros, se requiere establecer mecanismos de protección de la información, que es su activo principal, para evitar acceso y uso ilegal de la misma, así como de la infraestructura tecnológica que soporta la operatividad de dichos servicios y sistemas;

**CONSIDERANDO** que indica la Gerencia del Banco Central, que se elaboró un Proyecto de Reglamento bajo los estándares más modernos en la materia, que viene a cubrir el vacío normativo en estos temas y permitirá que todas las entidades a las que

aplica, es decir, entidades de intermediación financiera, los administradores y participantes del Sistema de Pagos de la República Dominicana (SIPARD), los participantes de los sistemas de pagos y liquidación de valores que lo componen, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, se rijan por reglas comunes en materia de Seguridad Cibernética y de la Información, a la vez que se contribuye a proteger a los clientes finales del sistema financiero, su información, sus accesos y sus cuentas;

**CONSIDERANDO** que este Proyecto de Reglamento sienta las bases para la creación de una estructura centralizada de respuestas a incidentes de seguridad cibernética en el sistema financiero, lo cual ayudaría a mitigar los efectos y la propagación de los posibles eventos de ciberseguridad a todas las entidades del sistema y riesgo sistémico que hoy en día está latente en todos los mercados;

**CONSIDERANDO** que este Proyecto de Reglamento de Seguridad Cibernética y de la Información, está en consonancia con los esfuerzos realizados por el Estado dominicano para fortalecer las capacidades nacionales en esa materia, conforme las disposiciones establecidas en el Decreto No.258-16 que crea el Programa de República Digital, de fecha 16 de septiembre del 2016 y, el Decreto No.230-18 que define y regula la Estrategia Nacional de Ciberseguridad 2018-2021, de fecha 19 de junio del 2018;

**CONSIDERANDO** que mediante la citada Tercera Resolución, se autorizó la publicación para fines de recabar la opinión de los sectores interesados del referido Proyecto de Reglamento de Seguridad Cibernética y de la Información. Como resultado de dicha consulta pública, se recibieron observaciones y comentarios, los cuales se centraron fundamentalmente en los aspectos siguientes:

a) Marco de trabajo y estructura de la gobernanza de la seguridad de la información;

b) La gestión de riesgos tecnológicos;

c) El marco de control de Seguridad Cibernética y de la Información; y,

d) La coordinación sectorial de respuesta a incidentes de seguridad cibernética.

**CONSIDERANDO** que las observaciones antes mencionadas, fueron debidamente analizadas y ponderadas por el equipo técnico del Banco Central y se preparó una matriz en la cual se analizaron cada una de ellas y la pertinencia o no, de su incorporación al citado Proyecto de Reglamento;

**CONSIDERANDO** que con la recomendación favorable, la Gerencia del Banco Central presenta a la ponderación de la Junta Monetaria, para su aprobación definitiva el Proyecto de Reglamento de Seguridad Cibernética y de la Información;

Por tanto, la Junta Monetaria

**R E S U E L V E:**

1. Aprobar la versión definitiva del Proyecto de Reglamento de Seguridad Cibernética y de la Información, que tiene por finalidad establecer los principios y lineamientos generales que deberán adoptarse para la integridad, disponibilidad y confidencialidad de la información, el funcionamiento óptimo de los sistemas de información y de la infraestructura tecnológica, la adopción e implementación de prácticas para la gestión de riesgos de la Seguridad Cibernética y de la Información, así como, la coordinación sectorial de respuesta a incidentes de seguridad cibernética, el cual reza de la forma siguiente:

**'REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN**

**TÍTULO I**
**DISPOSICIONES GENERALES**

**CAPÍTULO I**
**OBJETO, ALCANCE, ÁMBITO DE APLICACIÓN Y PRINCIPIOS RECTORES**

**Artículo 1. Objeto.** Este Reglamento tiene por objeto establecer los principios y lineamientos generales que servirán de base a las entidades de intermediación financiera, los administradores y participantes del Sistema de Pagos y Liquidación de Valores de la República Dominicana (SIPARD), a los participantes de los

…/

sistemas de pago y liquidación de valores que lo componen; y, a las entidades de apoyo y servicios conexos interconectadas con las entidades de intermediación financiera y con el SIPARD, para procurar la integridad, disponibilidad y confidencialidad de la información, y el funcionamiento óptimo de los sistemas de información y de la infraestructura tecnológica. Asimismo, la adopción e implementación de prácticas para la gestión de riesgos de la Seguridad Cibernética y de la Información, acorde a su naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica, conforme a la Ley No.183-02, Monetaria y Financiera de fecha 21 de noviembre del 2002 y sus modificaciones, y a los estándares internacionales en la materia.

**Artículo 2. Alcance.** El alcance de este Reglamento comprende los principios y lineamientos generales que deberán adoptarse para la integridad, disponibilidad y confidencialidad de la información, el funcionamiento óptimo de los sistemas de información y de la infraestructura tecnológica, así como la adopción e implementación de prácticas para la gestión de riesgos de la Seguridad Cibernética y de la Información.

**Artículo 3. Ámbito de Aplicación.** Las disposiciones establecidas en este Reglamento son de aplicación para las entidades que se identifican a continuación:

a) Bancos Múltiples;
b) Bancos de Ahorro y Crédito;
c) Corporaciones de Crédito;
d) Asociaciones de Ahorros y Préstamos;
e) Entidades Públicas de Intermediación Financiera;
f) Administradores de Sistemas de Pago y Liquidación de Valores;
g) Participantes del SIPARD autorizados por la Junta Monetaria; y,
h) Cualquier otro tipo de entidad del SIPARD, que la Junta Monetaria autorice en el futuro.

**Párrafo:** La aplicación de este Reglamento se extenderá a las entidades de apoyo y servicios conexos vinculadas, mediante el mantenimiento de una conexión electrónica o el intercambio de información esencial, a través de cualquier medio digital, en la medida en que dicha vinculación pueda comprometer los objetivos del SIPARD.



…/

**Artículo 4. Principios Rectores.** Este Reglamento tendrá como principios rectores básicos, los siguientes:

a) **Principio de Cooperación**. Cooperar de forma abierta, eficaz y transparente para el intercambio de la información que sea pertinente; y,

b) **Principio de Territorialidad**. Gestionar los riesgos de Seguridad Cibernética y de la Información en los casos en que la amenaza tenga incidencia en la República Dominicana.

## CAPÍTULO II
## DEFINICIONES

**Artículo 5. Definiciones**. Para efectos de este Reglamento, los términos y conceptos que se detallan a continuación, tendrán los significados siguientes:

a) **Acceso:** Capacidad y medios para comunicarse o interactuar con un sistema, utilizar recursos del mismo para manejar y adquirir conocimiento de la información contenida en el sistema o controlar componentes y funciones del mismo;

b) **Activo de Información:** Bien tangible o intangible, que almacena, procesa y/o transmite información;

c) **Administrador de un Sistema de Pagos o de Liquidación de Valores:** El Banco Central de la República Dominicana u otra entidad debidamente autorizada por la Junta Monetaria que opere un sistema de pagos; o una entidad autorizada a ofrecer servicios de registro, transferencia, compensación y liquidación de valores en lo relativo al traspaso de los valores negociables;

d) **Alta Gerencia:** La integran los principales ejecutivos u órganos de gestión, responsables de planificar, dirigir y controlar las estrategias y operaciones generales de las entidades, que han sido previamente aprobadas por el Consejo;

e) **Amenaza:** Circunstancia desfavorable que puede ocurrir y que, de suceder, tendría consecuencias negativas sobre la Seguridad Cibernética y de la Información. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad;

f) **Apetito de Riesgo:** Es el límite agregado en función de los tipos de riesgos que el Consejo y la Alta Gerencia están dispuestos a asumir y gestionar para cumplir sus objetivos de negocios;

g) **Arquitectura Empresarial:** Conjunto de sistemas de información de una empresa, su configuración, integración, así como su interacción con el entorno interno y externo, y la forma de operar para respaldar la misión y contribuir a la posición de seguridad general de la misma;

h) **Arquitectura de Seguridad Cibernética y de la Información:** Parte integral de la Arquitectura Empresarial, que describe la estructura y el comportamiento de los esquemas de Seguridad Cibernética y de la Información de una entidad, sus departamentos, colaboradores y los sistemas de información e Infraestructura Tecnológica que los apoyan, mostrando su alineación a las políticas definidas por la misma y sus planes estratégicos;

i) **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;

j) **Ataque Cibernético:** Ataque a la Infraestructura Tecnológica a través del ciberespacio;

k) **Autenticación:** Acto de validar la identidad de un usuario para otorgarle acceso a recursos tecnológicos;



…/

l) **Ciberespacio:** Dominio global dentro del entorno de información que consiste en una red interdependiente de Infraestructuras Tecnológicas, el Internet, redes de telecomunicaciones, procesadores y controladores integrados, sin menoscabo de otros componentes que puedan surgir en el futuro;

m) **Cifrado:** Proceso mediante el cual la información o archivos son alterados en forma matemática, mediante un control de acceso con el objetivo de evitar que una persona no autorizada, al verlos o copiarlos pueda interpretarlos;

n) **Colaboradores:** Personal interno que presta sus servicios de manera permanente o temporal a una entidad, a cambio de una contraprestación económica y que está asociado a la misma por un contrato de trabajo;

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

p) **Consejo**: Órgano máximo de dirección que tiene todas las facultades de administración y representación de la entidad, responsable de velar por el buen desempeño de la Alta Gerencia en la gestión, no pudiendo delegar su responsabilidad. Se refiere al consejo de directores, consejo de administración o junta de directores, según corresponda;

q) **Control de Acceso:** Proceso de concesión o denegación de solicitudes específicas, para obtener y utilizar información y servicios de procesamiento de información relacionados, o entrar en instalaciones físicas específicas;

r) **Copias de Resguardo:** Proceso de copiar información para facilitar la recuperación de las mismas, en caso de que sea necesario.

s) **Data:** Subconjunto de información en formato electrónico que permite ser recuperado o transmitido;



…/

t) **Datos de Carácter Personal:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables;

u) **Disponibilidad:** La propiedad de la información, de ser accesible y utilizable a pedido de un usuario, entidad o proceso autorizado;

v) **Dispositivo Móvil**: Dispositivo informático portátil que: (i) es de tamaño pequeño, de modo que puede ser transportado fácilmente por un solo individuo; (ii) está diseñado para funcionar sin una conexión física (por ejemplo, transmitir o recibir información de forma inalámbrica); (iii) posee almacenamiento de datos local, no extraíble; y, (iv) opera durante largos períodos con una fuente de alimentación autónoma. Los dispositivos móviles también pueden incluir capacidades de comunicación de voz, sensores electrónicos que les permiten capturar y procesar información (por ejemplo, imágenes, videos, datos biométricos, ubicación, entre otros) y/o características integradas para sincronizar datos locales con ubicaciones remotas;

w) **Documento Digital:** Información codificada en forma digital sobre un soporte lógico o físico, que se constituye en representación de actos, hechos o datos jurídicamente relevantes y a la cual se accede utilizando métodos electrónicos, ópticos o similares;

x) **Empresa de Adquirencia o Adquirente:** Entidad que, a través de dispositivos electrónicos, sirve de enlace entre una entidad emisora de tarjetas bancarias y el establecimiento donde se realiza una operación de pago a través de dichas tarjetas;

y) **Entidad de Apoyo y Servicios Conexos:** En adición a las entidades previstas en el Artículo 41 de la Ley Monetaria y Financiera, son las empresas de adquirencia, sociedades impresoras de cheques, proveedores de escáner, software y cualquier otra empresa proveedora de servicios y equipos a participantes y administradores de un sistema de pago, interconectadas con las entidades de intermediación financiera y con el SIPARD;



…/

z) **Entidad de Intermediación Financiera:** Persona jurídica autorizada por la Junta Monetaria al amparo de la Ley Monetaria y Financiera, a realizar de forma habitual captación de fondos del público con el objeto de cederlos a terceros, cualquiera que sea el tipo o la denominación del instrumento de captación o cesión utilizado, así como otras operaciones y servicios previstos en la referida Ley;

aa) **Entidad Interconectada:** Persona jurídica que, habilitada mediante una relación contractual, mantiene una conexión electrónica y/o intercambio de información con una entidad de intermediación financiera;

bb) **Entidad Receptora de Información:** Persona jurídica que captura datos de carácter personal a título propio o bajo la modalidad de servicio contratado por otra persona, para el uso, procesamiento, almacenamiento o transmisión de los mismos;

cc) **Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT por sus siglas en inglés):** Grupo de personas, habitualmente integrado por analistas de seguridad cibernética, organizado para desarrollar, recomendar y coordinar acciones inmediatas de mitigación para la contención, erradicación y recuperación como resultado de incidentes de seguridad cibernética, apoyado en Infraestructuras Tecnológicas diseñadas para tales fines;

dd) **Factores de Riesgo:** Fuentes generadoras de posibles eventos de pérdida por Ataques Cibernéticos;

ee) **Firma Digital:** Valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y el texto del mensaje, y que el mensaje inicial no ha sido modificado después de efectuada la transmisión;

ff) **Firmware:** Conjunto de datos e instrucciones para el funcionamiento de un dispositivo de computación, almacenado como software de solo lectura en dicho dispositivo, debiendo permanecer inalterado durante su ejecución;

gg) **Gestión de Riesgos:** Conjunto de políticas y procedimientos mediante el cual se identifican, miden, evalúan, monitorean y controlan los riesgos inherentes al negocio, con el objeto de conocer su grado de exposición en el desarrollo de sus operaciones y definir los mecanismos de cobertura para proteger los recursos propios y de terceros que se encuentran bajo su control y administración;

hh) **Incidente:** Evento que pone en peligro la confidencialidad, integridad o disponibilidad de la Infraestructura Tecnológica o la información procesada, almacenada o transmitida por dicho sistema, o que constituye una violación o amenaza inminente de violación de políticas, o procedimientos de seguridad o políticas de uso aceptable;

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

jj) **Información Esencial:** Conjunto de datos que facilita el desarrollo de las actividades fundamentales de la entidad, que sustenta la operatividad de la Infraestructura Tecnológica;

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

ll) **Información Esencial de Tipo Transaccional:** Conjunto de datos, cuyos registros contienen información sobre las transacciones realizadas en un sistema de información;

mm) **Infraestructura Tecnológica:** Equipos y sistemas con que cuenta la entidad para procesar la información, así como las adecuaciones del espacio físico que los aloja;

nn) **Integridad:** Propiedad que poseen los datos, que asegura que los mismos no han sido alterados de manera no autorizada o destruidos de manera inadecuada, durante su creación, transmisión o almacenamiento;



…/

oo) **Lineamiento Funcional de Seguridad Cibernética y de la Información:** Control técnico o estratégico aplicable para el tratamiento de los riesgos inherentes a la Seguridad Cibernética y de la Información;

pp) **Mecanismos de Control de Acceso:** Salvaguardas o medidas de seguridad físicas o lógicas diseñadas para detectar, restringir y permitir el acceso a un sistema de información o a un entorno local físico. Se refiere de manera individual o combinada, a características de hardware y software, controles, procedimientos operativos y procedimientos de gestión;

qq) **Mensaje de Datos:** Información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares;

rr) **Mensajería Instantánea:** Servicio de mensajería que ofrece transmisión de texto, imágenes, audio y video en tiempo real a través de redes de comunicación;

ss) **Monitoreo Continuo:** Proceso implementado para mantener en estado de vigilancia el funcionamiento de los controles de seguridad de los sistemas de la información y la Infraestructura Tecnológica de los que depende la operación de la entidad;

tt) **Nivel de acceso a la Información:** Es el que se puede tener según su contenido, la cual se clasifica en los niveles siguientes:

i. **Público:** Información que en virtud de la ley es catalogada como no confidencial y, en consecuencia, puede divulgarse sin ninguna responsabilidad para la entidad;

ii. **De Uso Interno:** Información perteneciente a la entidad cuyo acceso está disponible a los colaboradores;

iii. **Confidencial del Cliente:** Datos de carácter personal de los clientes cuyo acceso es restringido; y,

iv. **Confidencial de la Entidad:** Información utilizada por la entidad para el funcionamiento esencial de la misma, cuyo acceso está restringido según el grado de responsabilidad.

uu) **Nivel de Sensibilidad de la Información:** Grado de exposición de una información según su contenido, clasificándose en los niveles siguientes:

i. **No Sensible:** Información personal o de negocio, que al ser accedida no puede identificar de manera individual al dueño o titular de la información, ni puede generar daño alguno, sea por pérdida, robo, alteración, uso inadecuado o divulgación de la misma; y,

ii. **Sensible:** Información personal o de negocio, que al ser accedida puede identificar de manera individual al dueño o titular de la información, y que la pérdida, robo, alteración, uso inadecuado o divulgación de la misma puede perjudicar al dueño o titular de la información.

vv) **Participantes del SIPARD:** Entidades que poseen una cuenta corriente en el Banco Central y se encuentren interconectadas a uno o varios sistemas de pagos o de liquidación de valores, así como las personas jurídicas prestadoras de servicios que, a través de otro participante, forman parte de un sistema de pagos y liquidación de valores;

ww) **Pista de Auditoría:** Registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

xx) **Plan de Contingencia:** Conjunto de procedimientos alternativos a la operatividad normal de la entidad, cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto operativo y financiero que pueda ocasionar cualquier evento inesperado;

yy) **Plan de Continuidad de Negocio:** Conjunto formado por planes de actuación, de emergencia, financiero, de comunicación y de contingencia, destinados a

mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una sociedad;

zz) **Procedimiento:** Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de los cuales se asegura el cumplimiento de una función operativa;

aaa) **Proceso Crítico:** Proceso indispensable para la continuidad del negocio y las operaciones de la entidad, y cuya falta de identificación o aplicación deficiente puede generar un impacto financiero negativo;

bbb) **Programa de Seguridad Cibernética y de la Información:** Comprende las políticas, estrategias, procesos y actividades que las entidades deben documentar, desarrollar e implementar, a fin de cumplir las disposiciones y requerimientos establecidos en este Reglamento;

ccc) **Punto de Interacción (PDI):** Punto inicial donde se leen los datos de una tarjeta bancaria. Consiste en sistemas y equipos electrónicos para habilitar a un tarjetahabiente para realizar una transacción;

ddd) **Red Privada Virtual (VPN por sus siglas en inglés):** Tecnología de red, que permite una extensión segura de una red de área local (LAN, por sus siglas en inglés) sobre una red pública o no controlada como internet, garantizando la seguridad de la misma mediante el cifrado de la comunicación;

eee) **Riesgo:** Posibilidad de que se produzca un hecho que genere pérdidas que afecte los resultados, el patrimonio, la solvencia y liquidez de las entidades;

fff) **Riesgo Operacional:** Posibilidad de sufrir pérdidas debido a la falta de adecuación o a fallos de los procesos y sistemas internos, personas, o sistemas internos, o bien a causa de acontecimientos externos. Incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional;

ggg) **Riesgo Tecnológico:** Posibilidad de sufrir un impacto adverso relacionado con la afectación de la confidencialidad, integridad o disponibilidad de la información o de la Infraestructura Tecnológica;



…/

hhh) **Seguridad Cibernética:** Protección de la información en todos sus formatos durante el almacenamiento, trasmisión y procesamiento de la misma a través del Ciberespacio;

iii) **Seguridad de la Información:** La protección de los sistemas de información y de la información en todos sus formatos, durante su almacenamiento, procesamiento o transmisión, contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, a fin de proporcionar confidencialidad, integridad y disponibilidad de la información a lo interno de la entidad;

jjj) **Servicio de Computación en la Nube:** Tipo de servicio que permite a las entidades acceder a recursos basados en tecnología a través de internet sin necesidad del conocimiento, experiencia o control sobre la infraestructura tecnológica que los respalda. Este modelo de computación se compone de 5 (cinco) características esenciales: autoservicio bajo demanda, acceso universal a redes interconectadas, agrupación de recursos independiente de la ubicación, flexibilidad y calidad del servicio;

kkk) **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;

lll) **Sistema de Pagos:** Conjunto de instrumentos, procedimientos y sistemas de transferencia de fondos que aseguran la circulación del dinero. Posee un administrador y participantes;

mmm) **Sistema de Pagos y Liquidación de Valores de la República Dominicana (SIPARD):** Servicio público de titularidad exclusiva del Banco Central, compuesto por los diferentes sistemas de pago y liquidación de valores reconocidos, al cual se encuentran adscritas las entidades de intermediación financiera, así como otras entidades debidamente autorizadas;

nnn) **Tarjetahabiente Titular:** Persona física o jurídica que, previo contrato suscrito con la entidad emisora de tarjeta de crédito, es autorizada a girar en su favor sobre una línea de crédito, a través del uso de una tarjeta de crédito, haciéndose responsable de pagar o saldar todos los consumos, cargos, intereses y

…/

comisiones, realizados por sí mismo y por los Tarjetahabientes adicionales autorizados por él;

ooo) **Tarjeta Bancaria:** Tarjetas de débito, crédito y prepagadas, emitidas por las entidades de intermediación financiera (incluyendo cualquier otro tipo de tarjeta que se emita en el futuro), asociadas o no a una cuenta bancaria;

ppp) **TI (Tecnología de Información):** Conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software (aplicaciones, sistemas operativos, sistemas de administración de bases de datos, etc.), redes, multimedia, servicios asociados, entre otros; y,

qqq) **Vulnerabilidad:** Es una debilidad en un sistema de información, sus procedimientos de seguridad, su implementación o en sus controles internos, que podrían permitir la materialización de una amenaza.

## CAPÍTULO III
## MARCO DE TRABAJO Y ESTRUCTURA DE LA GOBERNANZA PARA EL PROGRAMA DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN

**Artículo 6. Marco de Trabajo.** Las entidades de intermediación financiera, administradores y participantes del SIPARD, entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer las acciones para el desarrollo, implementación y mantenimiento del Programa de Seguridad Cibernética y de la Información.

**Párrafo:** En las subsidiarias o sucursales de entidades extranjeras, el marco de trabajo para el Programa de Seguridad Cibernética y de la Información puede ser realizado por la unidad funcional de seguridad cibernética de la casa matriz o una unidad regional especializada, que tenga un mandato para el grupo financiero completo o para la región a la que pertenece la entidad de intermediación financiera que opera en el país.

**Artículo 7. Estructura.** Las entidades de intermediación financiera, administradores y participantes del SIPARD, entidades públicas de intermediación financiera y las entidades de apoyo y servicios conexos, deben contar con una estructura gerencial y funciones de control de Seguridad Cibernética y de la Información, acordes a su naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica. Dicha estructura estará conformada por un comité funcional de seguridad cibernética y de la información, una unidad funcional de seguridad cibernética y de la información y sus respectivas áreas especializadas. El citado comité reportará directamente al consejo. La unidad funcional de seguridad cibernética y de la información dirigirá el programa de seguridad cibernética y de la información, en el marco de las responsabilidades definidas en este Reglamento, podrá ser conformada por las áreas especializadas y estará a cargo del Oficial de Seguridad Cibernética y de la Información.

**Párrafo I**: Las labores del comité funcional de seguridad cibernética y de la información podrán ser asumidas por el comité de gestión de riesgos u otro comité de naturaleza similar (los cuales no alterarán su composición en estos casos), para las entidades que, por su naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica así lo requieran. En estas entidades, el proceso de gestión integral de riesgos debe tomar en consideración el Programa de Seguridad Cibernética y de la Información, en lo que respecta a la gestión de riesgos de Seguridad Cibernética y de la Información.

**Párrafo II**: Las labores del comité funcional de seguridad cibernética y de la información, en el caso de los administradores y participantes de sistemas de pagos y liquidación de valores (SIPARD) y las entidades de apoyo y servicios conexos, pueden ser asumidas por otro comité de naturaleza similar y estructura según lo dispuesto por este Reglamento.

**Párrafo III**: El comité funcional de seguridad cibernética y de la información será dirigido por un alto ejecutivo designado por el consejo u órgano societario equivalente y no podrá desempeñar funciones en las unidades funcionales y áreas especializadas de tecnología de la información. Este ejecutivo deberá ser distinto al Oficial de Seguridad Cibernética y de la Información.

**Párrafo IV**: Dicha estructura deberá ser revisada por el consejo u órgano societario equivalente, a medida que cambien las estrategias y/o estructura de las entidades de intermediación financiera, administradores y participantes del SIPARD, entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, para verificar su idoneidad e independencia de las áreas de negocios, tecnologías de la información y operaciones.

**Artículo 8. Aprobación del Programa de Seguridad Cibernética y de la Información.** Las políticas del Programa de Seguridad Cibernética y de la Información de las entidades de intermediación financiera, administradores y participantes del SIPARD, entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben ser sometidos al consejo u órgano societario competente, para su aprobación, por parte del comité funcional de seguridad cibernética a más tardar entre el tercer y sexto mes posterior a la entrada en vigencia de este reglamento.

**Artículo 9. Responsabilidades del Comité Funcional de Seguridad Cibernética y de la Información.** El comité funcional de seguridad cibernética y de la información asumirá, de manera enunciativa, pero no limitativa, las responsabilidades siguientes:

a) Diseñar los lineamientos funcionales de Seguridad Cibernética y de la Información, y el mantenimiento del Programa de Seguridad Cibernética y de la Información, en consonancia con los objetivos estratégicos de la entidad, determinados por el consejo u órgano societario equivalente;

b) Someter al consejo u órgano societario competente, para su aprobación, las políticas del Programa de Seguridad Cibernética y de la Información;

c) Evaluar la efectividad del Programa de Seguridad Cibernética y de la Información, en consonancia con los objetivos estratégicos de la entidad;

d) Ratificar las decisiones de tratamiento de riesgo, en coordinación con las áreas pertinentes de negocio, previamente presentadas por el Oficial de Seguridad Cibernética y de la Información; y,

e) Comunicar al consejo u órgano societario competente, los resultados de sus valoraciones sobre los aspectos de Seguridad Cibernética y de la Información.

**Artículo 10. Oficial de Seguridad Cibernética y de la Información.** El personal asignado a este rol, debe contar con la competencia y capacidad requerida para la implementación del programa de la naturaleza descrita en este Reglamento. La función del Oficial de Seguridad Cibernética y de la Información, aunque de naturaleza funcional y operativa, tendrá suficiente jerarquía, según la estructura de cada entidad, para asegurar que cuenta con la autoridad e independencia necesarias para cumplir con sus responsabilidades, debiendo reportar al principal ejecutivo de la entidad o a quien éste delegue.

**Párrafo I:** El Oficial de Seguridad Cibernética y de la Información será miembro del comité funcional de seguridad cibernética y de la información, y llevará la agenda concerniente a los aspectos de Seguridad Cibernética y de la Información, en calidad de secretario del comité.

**Párrafo II**: El Oficial de Seguridad Cibernética y de la Información podrá pertenecer a otros comités de la entidad, por la naturaleza de su rol.

**Párrafo III**: El Oficial de Seguridad Cibernética y de la Información debe reportar periódicamente al Equipo de Respuestas a Incidentes de Seguridad Cibernética y de la Información (CSIRT) un informe de situación de la infraestructura tecnológica bajo su supervisión y cualquier otra información que le sea requerida por el mismo.

**Párrafo IV:** Las funciones del Oficial de Seguridad Cibernética y de la Información podrá ser desempeñada por cualquier otro ejecutivo no perteneciente al área de tecnología de la información, cuyas funciones sean compatibles con dicho rol y cumpla con los requisitos de este Reglamento y sus instructivos.

**Artículo 11. Responsabilidades del Oficial de Seguridad Cibernética y de la Información.** El Oficial de Seguridad Cibernética y de la Información debe cumplir, de manera enunciativa, pero no limitativa, con las responsabilidades siguientes:

a) Desarrollar, implementar y mantener actualizado el Programa de Seguridad Cibernética y de la Información;

b) Implementar las políticas, estándares y procedimientos apropiados para apoyar el Programa de Seguridad Cibernética y de la Información;

c) Asignar las responsabilidades de los miembros que conforman las áreas especializadas**;**

d) Gestionar las acciones para el tratamiento del riesgo tecnológico en coordinación con las áreas pertinentes del negocio, previa aprobación del comité funcional de seguridad cibernética y de la información;

e) Cumplir con los límites de los niveles de riesgo tecnológico relevantes establecidos por el consejo relacionados con amenazas o incidentes de Seguridad Cibernética y de la Información; y,

f) Definir y evaluar las responsabilidades de los proveedores en lo concerniente a la Seguridad Cibernética y de la Información de los servicios provistos.

**Artículo 12. Áreas Especializadas.** Las entidades de intermediación financiera, administradores y participantes del SIPARD, entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben contar con una o varias áreas especializadas operativas y funcionales, responsables de la ejecución del Programa de Seguridad Cibernética y de la Información, las cuales podrán estar bajo la dependencia del Oficial de Seguridad Cibernética y de la Información.

**Párrafo I:** Las áreas especializadas deberán estar conformadas por personal técnico con la competencia y capacidad requerida y con funciones y responsabilidades definidas. Las mismas deberán contar con los recursos necesarios para garantizar la adecuada gestión del Programa de Seguridad Cibernética y de la Información. Cada unidad estará liderada por un profesional designado por el Oficial de Seguridad Cibernética y de la Información.

**Párrafo II.** En los casos en que el comité de gestión de riesgos asuma las funciones del comité funcional de seguridad cibernética y de la información, en atención a lo dispuesto en el Párrafo I, del Artículo 7, las áreas especializadas que se conformen,

estarían bajo la supervisión del encargado de la unidad de gestión integral de riesgos.

## TÍTULO II
## DEL PROGRAMA DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN

### CAPÍTULO I
### GESTIÓN DEL RIESGO TECNOLÓGICO

**Artículo 13. Gestión de Riesgos Tecnológicos.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, 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.

**Artículo 14. Gestión de Riesgos Tecnológicos en las Entidades Interconectadas.** Las entidades de intermediación financiera, deben procurar, de manera periódica, la gestión de riesgos tecnológicos a las entidades interconectadas con las que actualmente mantengan una relación contractual. Cuando la evaluación de riesgos tecnológicos realizada a estas entidades no sea satisfactoria, deben 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 entidad de intermediación financiera. En caso de que la entidad interconectada no realice las acciones correspondientes a la mitigación de sus riesgos de manera adecuada, se procederá a su desconexión definitiva.

**Párrafo I:** El apetito de riesgo debe ser establecido por el Consejo u Órgano de Administración superior correspondiente, en base a una clasificación previamente establecida. Las Entidades de Intermediación Financiera, no debe establecer interconexión con entidades cuyo riesgo sea mayor que el definido por su Consejo.

**Párrafo II:** En el marco del establecimiento de una nueva relación contractual que procure la interconexión o el intercambio de información con las entidades de intermediación financiera, deben abstenerse de concretizar dicha relación, en caso de que la evaluación de riesgos tecnológicos no sea calificada como satisfactoria, tomando en consideración el apetito de riesgo establecido por cada entidad de intermediación financiera.

**Artículo 15. Metodologías para la Gestión de Riesgos Tecnológicos.** La gestión de riesgos tecnológicos, deben llevarse a cabo a través de metodologías estructuradas que contemplen la identificación de las amenazas y vulnerabilidades tecnológicas, la probabilidad de ocurrencia y el posible impacto previsto a las operaciones del negocio para determinar el riesgo potencial.

**Párrafo I:** Las evaluaciones deben contemplar la divulgación no autorizada de información, la corrupción accidental o deliberada, la manipulación de la información y la disponibilidad de los entornos en cualquier período.

**Párrafo II:** Los riesgos tecnológicos deben ser tratados de acuerdo con los requerimientos del negocio y el enfoque aprobado por el comité funcional de seguridad cibernética y de la información.

## CAPÍTULO II
## MARCO DE CONTROL DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN

**Artículo 16. Política de Seguridad Cibernética y de la Información.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y las entidades de apoyo y, servicios conexos, deben implementar y mantener una política general o varias políticas segregadas que contemplen los aspectos, procesos y procedimientos para la gestión de la Seguridad Cibernética y de la Información, debiendo dar a conocer dichas políticas a sus colaboradores.

**Artículo 17. Contratos con Colaboradores.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben

incorporar en los contratos con colaboradores, las responsabilidades generales y específicas de Seguridad Cibernética y de la Información hasta la finalización de los mismos. Los colaboradores deberán firmar un documento formal que establezca tales responsabilidades.

**Párrafo:** Para el caso de los contratos que hayan sido perfeccionados de manera verbal o escrita, con colaboradores existentes a la fecha de entrada en vigor de este Reglamento, deben procurar la firma de un documento en el cual se hagan constar los aspectos generales y específicos de Seguridad Cibernética y de la Información, acorde con las responsabilidades de los mismos hasta su finalización. De no ser ésta la práctica, los colaboradores deberán firmar un documento formal que establezca dichas responsabilidades con la periodicidad establecida en el Programa de Seguridad Cibernética y de la Información de cada entidad.

**Artículo 18. Cultura de Seguridad Cibernética y de la Información.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben promover una cultura de Seguridad Cibernética y de la Información, contemplando al menos los aspectos siguientes:

a) El establecimiento de programas continuos de sensibilización sobre el rol de los colaboradores en la Seguridad Cibernética y de la Información, el uso correcto de los sistemas de información e infraestructura tecnológica, y la gestión de sus riesgos a través de los programas de inducción, cápsulas informativas, boletines, charlas concernientes a la seguridad y cualquier otro mecanismo de notificación hábil;

b) La definición de las responsabilidades de los colaboradores relacionados con la Seguridad Cibernética y de la Información en todos los niveles de la organización;

c) La instauración de programas continuos de capacitación técnica dirigidos a los colaboradores responsables de la Seguridad Cibernética y de la Información; y,

d) La provisión de los recursos adecuados para apoyar la efectividad de los programas continuos de sensibilización de Seguridad Cibernética y de la Información;

**Artículo 19. Gestión de Activos de Información.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben desarrollar un esquema de gestión de activos de información que contemple los aspectos siguientes:

a) **Clasificación de Activos de Información:** La clasificación de los activos de información, se llevará a cabo de acuerdo con el nivel de confidencialidad y sensibilidad de la información que gestionan;

b) **Gestión de Documentos:** Los documentos deben ser manejados de una manera sistemática y estructurada, debiéndose cumplir con los requisitos de Seguridad Cibernética y de la Información durante el ciclo de vida del documento;

c) **Información Sensible en Formato Físico:** La información sensible en formato físico, debe protegerse contra la corrupción, la pérdida o la divulgación no autorizada; y,

d) **Registro de Activos de Información:** Los sistemas informáticos y equipos de la infraestructura tecnológica, deben ser registrados en un repositorio, el cual deberá permanecer actualizado.

**Artículo 20. Aplicaciones del Negocio.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben implementar controles de seguridad para las aplicaciones del negocio, que contemplen los aspectos siguientes:

a) **Protección de las Aplicaciones:** Deben utilizar funcionalidades de seguridad de la información alineadas a la infraestructura técnica de seguridad, que permitan el cumplimiento de los requerimientos de confidencialidad, integridad y disponibilidad de la información;

…/

b) **Protección de las Aplicaciones Basadas en Navegación:** Deben establecer controles específicos de seguridad cibernética sobre las aplicaciones y servicios transaccionales, tanto internos como externos que apoyen los servicios hacia internet, basados en el navegador y en los servidores en donde se ejecutan; y,

c) **Validación de la Información en las aplicaciones de negocio:** Deben incorporar controles de Seguridad Cibernética y de la Información, que protejan la confidencialidad e integridad de la información, cuando sean ingresadas, procesadas o extraídas de la aplicación.

**Artículo 21. Políticas de Privacidad de la Información.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben especificar en los contratos con sus clientes, las políticas relacionadas a la privacidad de la información y datos de carácter personal utilizados en sus productos y servicios, así como cualquier modificación a las mismas. Estas políticas deben contener el desglose del uso que la entidad receptora de información dará a cada tipo de información o dato recopilado y deberán ser divulgadas a través de medios físicos o electrónicos.

**Párrafo**: En el caso de los contratos vigentes aprobados por la Superintendencia de Bancos, se remitirá únicamente las nuevas cláusulas incluidas en los mismos.

**Artículo 22. Términos y Condiciones de Uso.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben mantener actualizados los términos y condiciones de uso previamente aprobados, cubriendo los aspectos de Seguridad Cibernética y de la Información. Asimismo, gestionarán el cumplimiento de dichos términos y condiciones de uso, de conformidad con los requerimientos de Seguridad Cibernética y de la Información de la entidad.

**Artículo 23. Trazabilidad de las Conexiones de los Clientes**. Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y

servicios conexos, deben identificar y registrar en un inventario de conexiones, los accesos de los clientes a los servicios de canales electrónicos o digitales. Este acceso de los clientes debe ser protegido mediante mecanismos de control y supervisión.

**Artículo 24. Gestión de Accesos de los Colaboradores.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben contemplar dentro de su Programa de Seguridad Cibernética y de la Información, la gestión de los accesos de los colaboradores a los sistemas de información e infraestructuras tecnológicas, considerando los aspectos siguientes:

a) **Control de Acceso:** Se deben establecer límites y controles para los accesos de los colaboradores a los sistemas de información e infraestructura tecnológica; y,

b) **Autorización a los Colaboradores:** Los accesos a los colaboradores sobre los sistemas de información e infraestructura tecnológica, deben ser autorizados previo a su otorgamiento.

**Artículo 25. Mecanismos de Control de Acceso.** El acceso a los sistemas de información e infraestructura tecnológica se limitará a las personas autorizadas, utilizando mecanismos apropiados de control de acceso contemplados en sus políticas internas y supervisado por el personal técnico de seguridad, contemplando los principios del menor privilegio y separación de funciones.

**Artículo 26. Gestión de Sistemas de Información.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer políticas y procedimientos para la gestión de los sistemas de información, considerando los aspectos siguientes:

a) **Sistemas Informáticos e Infraestructura Tecnológica:** Deben ser protegidos mediante controles de seguridad integrados;

b) **Configuración de los Servidores Físicos y Virtuales:** Deben estar configurados para evitar cambios o accesos no autorizados, previniendo la interrupción de los servicios como resultado de una sobrecarga del sistema u otros factores;

c) **Sistemas de Almacenamiento de Red:** Deben estar protegidos mediante controles de seguridad, procurando la confidencialidad, integridad y disponibilidad de la información que contienen;

d) **Gestión de Cambios:** Los cambios en los sistemas de la información e infraestructura tecnológica deben ser probados, revisados y aplicados mediante un proceso definido de gestión de cambios; y,

e) **Copias de Resguardo y su Retención:** Las copias de resguardo se deben realizar de forma regular, de acuerdo con un ciclo definido, con un esquema distribuido que incluya medios de resguardo no conectados a la red interna, fuera de línea y en formato digital. A saber:

   i. El resguardo de la información esencial deberá ser conservado de conformidad con el grado de utilidad de la misma para los fines de restauración. Dicha información deberá ser cifrada. El tiempo de retención para la información esencial de tipo transaccional, será de por lo menos 1 (un) año. Para la información esencial de tipo maestro, la entidad deberá resguardar en todo momento, la más actualizada de las versiones disponibles de dicha información; y,

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

**Artículo 27. Infraestructura Técnica de Seguridad.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben implementar plataformas y sistemas que faciliten la aplicabilidad de los controles de seguridad apropiados, contemplando los aspectos siguientes:

a) **Arquitectura de Seguridad Cibernética y de la Información:** El comité funcional de seguridad cibernética y de la información debe establecer la arquitectura de seguridad cibernética y de la información de la entidad, a fin de proporcionar un marco estándar para la aplicación de los controles;

b) **Gestión de Identidad:** Establecer un proceso de gestión de identidad, para proporcionar una administración de perfiles de usuarios eficaz y coherente con la identificación, autenticación y mecanismos de control de acceso;

c) **Sistemas de Información de Infraestructuras Críticas:** Los sistemas de información que apoyan las infraestructuras críticas, serán protegidos por políticas integrales de Seguridad Cibernética y de la Información, que incluyan la evaluación de riesgos, la selección de los controles de seguridad, la evidencia de su implementación y su monitoreo;

d) **Soluciones Criptográficas:** Utilizar soluciones criptográficas para proteger y preservar la confidencialidad e integridad de la información sensible en tránsito o almacenada, así como el canal de transmisión utilizado, tomando en cuenta lo siguiente:

   i. **Gestión de los Algoritmos de Cifrado:** La utilización de algoritmos de cifrado debe estar documentada y aprobada por el comité funcional de seguridad cibernética y de la información. Los algoritmos deben contar con respaldo internacional por su garantía a la confidencialidad e integridad de la información y los inseguros u obsoletos deben ser suspendidos o actualizados;

   ii. **Gestión de las Llaves Criptográficas:** Las llaves criptográficas deben ser manejadas de manera segura, de acuerdo con los estándares y procedimientos documentados, y deben ser protegidas contra el acceso o destrucción no autorizada; y,

   iii. **Infraestructura de Llaves Públicas (PKI, por sus siglas en inglés):** Cuando se utiliza una infraestructura de llave pública, deben ser establecidas por una o más entidades de certificación y autoridades de

registro y las llaves deben estar protegidas con los controles de seguridad necesarios.

e) **Protección Contra la Fuga de Información:** Se establecerán mecanismos de protección contra la fuga de información a los sistemas, infraestructura tecnológica y entornos locales que procesan, almacenan o transmiten información sensible; y,

f) **Gestión de los Derechos Digitales (DRM, por sus siglas en inglés):** La información sensible o las aplicaciones utilizadas fuera de la infraestructura tecnológica, se protegerán mediante el uso de un sistema de gestión de derechos digitales.

**Artículo 28. Gestión de la Red.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben implementar procesos y plataformas para la gestión segura de los componentes en las redes de información, tomando en consideración los aspectos siguientes:

a) **Configuración de Dispositivos de Red:** Los dispositivos de red deben ser configurados para funcionar de acuerdo con su rol y se establecerán controles de seguridad que eviten cambios no autorizados o incorrectos;

b) **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;

c) **Conexiones de Redes Externas:** Las conexiones de redes externas a los sistemas y redes informáticas deben ser identificadas, verificadas, registradas y aprobadas individualmente por el comité funcional de seguridad cibernética;

d) **Tráfico de Datos a Través de los Firewalls (Cortafuegos):** El tráfico de datos entre redes o subredes internas o externas interconectadas, será debidamente transmitido a través de firewalls, con las reglas de seguridad requeridas, previo a la concesión o restricción de acceso;



…/

e) **Mantenimiento Remoto:** El mantenimiento remoto de los sistemas y redes críticas debe restringirse al personal debidamente autorizado, confinado a sesiones individuales y sujeto a revisión;

f) **Acceso a Redes Inalámbricas:** El acceso desde y hacia redes inalámbricas, será limitado a los usuarios y dispositivos autenticados y autorizados. El canal de transmisión debe ser cifrado para salvaguardar la información sensible en tránsito;

g) **Redes de Voz sobre IP (VoIP, por sus siglas en inglés):** Las redes de VoIP deben ser protegidas por una combinación de controles de seguridad, tanto de la red como específicos del protocolo VoIP, para garantizar la disponibilidad de las mismas y proteger la confidencialidad e integridad de la información sensible en tránsito; y,

h) **Telefonía y Conferencia:** Las instalaciones de telefonía y conferencia deben protegerse con una combinación de controles de seguridad físicos y lógicos, monitoreo continuo y acceso restringido.

**Artículo 29. Conexiones con los Servicios de Entes Reguladores y Supervisores.** Las Superintendencias del sistema financiero y los órganos reguladores sub-sectoriales a cuyos regulados alcance este Reglamento, y que mantengan una conexión con los mismos, deben realizar revisiones periódicas a los modelos de conexión previamente establecidos con sus servicios, con el propósito de evaluar los controles de seguridad utilizados en los mismos, para determinar las mejoras necesarias que deben ser implementadas para garantizar la disponibilidad de los servicios.

**Artículo 30. Gestión de Vulnerabilidades y Amenazas Tecnológicas.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer un proceso de análisis, monitoreo y evaluación integral de las vulnerabilidades y amenazas tecnológicas a sus sistemas, infraestructuras y procesos tecnológicos, para minimizar la ocurrencia de incidentes

y eventos relacionados a la Seguridad Cibernética y de la Información, contemplando los aspectos siguientes:

a) **Actualizaciones de Seguridad de Sistemas:** Establecer un proceso para el despliegue recurrente de actualizaciones de seguridad del firmware, de los sistemas operativos y de las aplicaciones. En los casos en que la actualización esté a cargo de un proveedor externo y que, por cualquier causa y de manera definitiva, rescinda o descontinúe el servicio de soporte de actualizaciones de seguridad de firmware, sistemas operativos o aplicaciones, la entidad deberá sustituirlo;

b) **Inteligencia contra Amenazas:** Desarrollar capacidades de inteligencia contra amenazas mediante la implementación de procesos, plataformas de análisis y recolección de datos, apoyadas por un ciclo de inteligencia;

c) **Protección Contra el Software Malicioso:** Se debe implementar una solución tecnológica eficaz para el control y protección de software malicioso en los sistemas de información e Infraestructura Tecnológica. Esta solución estará configurada para recibir actualizaciones periódicas emitidas por el proveedor de la misma;

d) **Registro de Eventos de Seguridad Cibernética y de la Información:** Los acontecimientos potencialmente relacionados con incidentes de Seguridad Cibernética y de la Información deben ser registrados, almacenados de forma centralizada, protegidos contra la modificación no autorizada y analizados de manera regular. El tiempo de retención para estos registros no podrá ser menor a 3 (tres) años;

e) **Monitoreo de los Sistemas y la Infraestructura Tecnológica:** Los sistemas y la Infraestructura Tecnológica deben ser monitoreados y revisados continuamente para asegurar el rendimiento de los mismos, reducir la ocurrencia de sobrecargas~~,~~ identificar vulnerabilidades y detectar posibles intrusiones maliciosas;

f) **Prevención y Detección de Intrusos:** Implementar soluciones tecnológicas o mecanismos de prevención y detección de intrusos, a fin de proteger los sistemas y la infraestructura tecnológica.

**Artículo 31. Gestión de Incidentes de Seguridad Cibernética y de la Información.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer políticas y procedimientos para la gestión de los incidentes de Seguridad Cibernética y de la Información, con el fin de identificar, responder, remediar y documentar de manera efectiva los eventos o cadena de eventos que vulneren dicha seguridad, procurando minimizar su impacto y recuperarse del incidente en el menor plazo posible. A tales fines deben contemplar los aspectos siguientes:

a) **Medidas contra Ataques Cibernéticos e Incidentes de Seguridad de la Información:** Tomar medidas razonables y efectivas para procurar la protección de la información, los sistemas y la infraestructura tecnológica, frente a los ataques cibernéticos o incidentes relacionados con la seguridad de la información;

b) **Correctivos de Emergencia:** Establecer un método eficaz de prueba, revisión y aplicación de correctivos de emergencia a los sistemas de la información e infraestructura tecnológica, de acuerdo con los procedimientos previamente autorizados; y,

c) **Investigaciones Forenses:** Definir un proceso para realizar las investigaciones forenses relacionadas con incidentes de seguridad cibernética y de la información u otros eventos que lo requieran.

**Artículo 32. Entornos Locales de Operación.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben identificar los entornos locales de operación y establecer procesos de seguridad cibernética para estos ambientes, contemplando los aspectos siguientes:

a) **Perfil de Seguridad de Localidad Física:** Definir, documentar y actualizar los perfiles de seguridad de sus localidades físicas, los cuales deben contener detalles importantes de seguridad acerca de los colaboradores internos, los procesos, la información, la tecnología utilizada y la ubicación asociados a sus localidades físicas. La finalidad de los perfiles es la de servir de apoyo en la toma de decisiones basadas en el riesgo y relacionadas con la Seguridad Cibernética y de la Información, que involucren dichas localidades;

b) **Coordinación de la Seguridad Local:** Tomar medidas para coordinar las actividades de seguridad de la información en las unidades de negocio pertinentes; y,

c) **Equipos Electrónicos y Digitales:** Los equipos electrónicos y digitales que procesan, almacenan o transmiten información, deben ser protegidos y localizados en lugares físicamente seguros. El uso de dispositivos electrónicos que permitan el registro o la captación de contenido audiovisual en áreas restringidas debe ser controlado, así como los horarios de acceso a las mismas.

**Artículo 33. Aplicaciones de Estaciones de Trabajo.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer procesos para la gestión adecuada de la Seguridad Cibernética y de la Información de las aplicaciones instaladas en las estaciones de trabajo, contemplando los aspectos siguientes:

a) **Inventario de las Aplicaciones de Estaciones de Trabajo:** Las aplicaciones de estaciones de trabajo deberán estar registradas en un inventario o su equivalente;

b) **Protección de los Archivos con Información Confidencial:** Los archivos creados en aplicaciones de estaciones de trabajo, cuyo contenido sea información confidencial, deben ser protegidos mediante la validación de la entrada, aplicando mecanismos de control de acceso;

c) **Protección de las Bases de Datos:** Las bases de datos gestionadas con aplicaciones de estaciones de trabajo, deben ser protegidas mediante la

…/

validación de la entrada, la aplicación de controles de acceso y la restricción a colaboradores autorizados a las funcionalidades de alto privilegio; y,

d) **Desarrollo de Aplicaciones de Estaciones de Trabajo:** Debe ser llevado a cabo según la metodología de desarrollo seguro, adoptada por la entidad.

**Artículo 34. Dispositivos de Computación Móvil.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer mecanismos de seguridad para proteger la información intercambiada a través de los dispositivos de computación móvil utilizados por los colaboradores, tomando en consideración los aspectos siguientes:

a) **Acceso desde Entornos Remotos:** Los dispositivos utilizados por los colaboradores para acceder desde entornos remotos, deben estar sujetos a autorización según los estándares y procedimientos establecidos por el comité funcional de seguridad cibernética y de la información;

b) **Gestión Centralizada de Dispositivos Móviles:** Contar con mecanismos para la gestión centralizada de dispositivos móviles y se proveerá a los colaboradores autorizados, de información relevante relacionada a la protección de los dispositivos bajo su custodia;

c) **Protección de la Información en los Dispositivos Móviles:** Los dispositivos móviles deben ser protegidos contra la divulgación no autorizada de información, pérdida o hurto, mediante controles de acceso y cifrado de los mismos;

d) **Conectividad de los Dispositivos Móviles:** Los dispositivos móviles deben estar provistos de medios seguros de conexión a otros dispositivos y redes;

e) **Dispositivos Portátiles de Almacenamiento:** El uso de dispositivos portátiles de almacenamiento, debe ser objeto de aprobación con acceso restringido. El almacenamiento de información en este tipo de dispositivos, debe ser de forma cifrada; y,

f) **Dispositivos Personales:** El acceso a la red a través de dispositivos de computación móvil propiedad de los colaboradores, debe contar con la debida autorización y la implementación de controles técnicos, que contemplen los requerimientos de Seguridad Cibernética y de la Información.

**Artículo 35. Comunicaciones Electrónicas**: Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben asegurar las comunicaciones electrónicas, mediante controles y políticas de Seguridad Cibernética y de la Información, tomando en consideración los aspectos siguientes:

a) **Correo Electrónico:** Los sistemas de correo electrónico deben estar protegidos por una combinación de procesos, concienciación y controles técnicos de Seguridad Cibernética y de la Información; y,

b) **Mensajería Instantánea:** Los servicios de mensajería instantánea deben ser protegidos mediante el establecimiento de un proceso de gestión, la implementación de los controles y la configuración de los elementos de Seguridad Cibernética y de la Información;

c) **Plataformas de Colaboración:** Las plataformas de colaboración deben estar protegidas por políticas de gestión de configuración, controles de despliegue de aplicación y la realización de ajustes de seguridad en cada plataforma, asegurando su disponibilidad cuando se requieran y la protección de las informaciones en tránsito; y,

d) **Servicios de Comunicación de voz**: Los servicios de comunicación de voz deben ser aprobados y protegidos por una combinación de controles tecnológicos, los cuales deben monitorease regularmente y estar respaldados por restricciones en los accesos.

**Artículo 36. Gestión de Proveedores Externos de Productos o Servicios Tecnológicos.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, que contraigan obligaciones

contractuales con proveedores externos de productos o servicios tecnológicos, deben asegurar la integración de los requerimientos de Seguridad Cibernética y de la Información, tomando en consideración los aspectos siguientes:

a) **Tercerización:** Establecer un proceso para regir la selección y gestión de los proveedores externos, apoyado en contratos que especifiquen los requisitos de Seguridad Cibernética y de la Información;

b) **Requisitos de Seguridad a los Proveedores Externos:** El cumplimiento de los requisitos de Seguridad Cibernética y de la Información, debe considerarse y revisarse de manera periódica durante la relación con los proveedores externos, contemplando el análisis y la gestión adecuada de los riesgos;

c) **Adquisición o Arrendamiento de Equipos y Sistemas Tecnológicos:** El proceso de adquisición o arrendamiento de equipos y sistemas tecnológicos, debe basarse en guías de referencia para la selección y aprobación de proveedores de equipos, aplicaciones y servicios, y prever los requerimientos técnicos de seguridad aprobados por el comité funcional de seguridad cibernética y de la información, asegurando que estos brinden la funcionalidad requerida y no comprometan la seguridad de la información sensible de la entidad durante su ciclo de vida; y,

d) **Contratación de Servicios de Computación en la Nube:** Se debe documentar una política para el uso y contratación de servicios de computación en la nube, incluyendo el hospedaje de servicios web, que contemple el desarrollo de un análisis de riesgos de Seguridad Cibernética y de la Información de los servicios contratados, para determinar el uso de los mismos por parte de los colaboradores, la integridad de la información almacenada, así como los mecanismos de protección de la misma. Esta política debe ser comunicada a todos los colaboradores que puedan hacer uso de los mismos y los requerimientos de seguridad cibernética deben estar contenidos en dicha política.

**Artículo 37. Gestión de Desarrollo de Sistemas.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, que



…/

mantengan en su estructura orgánica un área de desarrollo de sistemas, deben establecer un proceso de gestión de desarrollo de sistemas, el cual contemplará las disposiciones siguientes:

a) **Metodología de Desarrollo de Sistemas:** Las actividades de desarrollo de sistemas deben llevarse a cabo de acuerdo con una metodología de desarrollo documentada y apegada a las mejores prácticas internacionales;

b) **Entornos de Desarrollo de Sistemas:** Las actividades de desarrollo de sistemas se deben realizar en los entornos de desarrollo especializados, los cuales deben estar separados de los ambientes de producción y preproducción, y protegidos contra el acceso no autorizado. La data de entornos productivos no debe ser utilizada o almacenada en los entornos de desarrollo. Deben establecerse mecanismos para asegurar la privacidad y protección de los datos de carácter personal en los ambientes de preproducción (aseguramiento de la calidad) y producción;

c) **Aseguramiento de la Calidad:** El desarrollo de los sistemas debe realizarse siguiendo normas y pruebas de calidad, que procuren que los controles y requisitos de Seguridad Cibernética y de la Información acordados, sean implementados durante el ciclo de desarrollo del mismo; y,

d) **Interfaces Programables de Aplicaciones (API, por sus siglas en inglés):** Los sistemas y aplicaciones que permitan la extensibilidad de funciones a través de interfaces de aplicaciones programables, deberán contar con controles de Seguridad Cibernética y de la Información que regulen la interacción con otros sistemas y aplicaciones, tanto internos como de terceros. Del mismo modo, las aplicaciones desarrolladas que interactúen con estas interfaces de aplicaciones programables, deberán cumplir con los requerimientos de seguridad establecidos por la entidad.

**Artículo 38. Ciclo de Vida del Desarrollo de Sistemas y Aplicaciones.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos que mantengan en su estructura orgánica un área de

desarrollo de sistemas, deben adoptar un ciclo de vida para el desarrollo seguro de sus sistemas y aplicaciones, de acuerdo a las disposiciones siguientes:

a) **Especificaciones de los Requerimientos:** Los requerimientos del negocio, incluidos los de Seguridad Cibernética y de la Información, deben ser contemplados durante la fase de especificación de requerimientos;

b) **Diseño de Sistemas y aplicaciones:** Los requisitos de Seguridad Cibernética y de la Información para los sistemas que se encuentran en el ciclo de desarrollo, deben ser considerados en el diseño de dichos sistemas y aplicaciones, a fin de minimizar las vulnerabilidades;

c) **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 las mejores prácticas de la industria, realizadas por el personal especializado en el desarrollo de sistemas y aplicaciones. Las actividades de compilación deben ser inspeccionadas para identificar modificaciones o cambios no autorizados;

d) **Prueba de Sistemas y aplicaciones:** Los sistemas y aplicaciones en desarrollo deben ser probados en una zona dedicada de pruebas que simule el entorno de producción, con la debida atención a la data de carácter personal utilizada, antes de que el sistema o aplicación sea colocado en el ambiente de producción;

e) **Pruebas de Seguridad:** Los sistemas y aplicaciones en desarrollo deben ser sometidos a pruebas de Seguridad Cibernética y de la Información en las fases requeridas dentro del ciclo de desarrollo, utilizando herramientas para la detección de vulnerabilidades, pruebas de penetración y pruebas de control de acceso, previo a su colocación en los ambientes de producción;

f) **Proceso de Instalación:** Los nuevos sistemas y aplicaciones se deben instalar en el entorno de producción, de acuerdo con un proceso documentado que contemple los requerimientos de Seguridad Cibernética y de la Información; y,

g) **Revisiones luego de las Implementaciones:** luego de la implementación, se deben realizar revisiones periódicas de acuerdo con procesos documentados, incluyendo la cobertura de la Seguridad Cibernética y de la Información.



…/

**Artículo 39. Seguridad Física y del Entorno.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben definir los mecanismos que provean las condiciones de seguridad física y del entorno adecuado de las instalaciones críticas.

**Párrafo:** Las instalaciones críticas, incluyendo lugares que albergan los sistemas informáticos, tales como los centros de datos, redes, equipos de telecomunicaciones, material físico sensible y otros activos importantes, deben ser protegidos contra accidentes, ataques y el acceso físico no autorizado; contra los cortes o fluctuaciones de energía, así como estar protegidos contra incendios, inundaciones y otras amenazas naturales.

**Artículo 40. Continuidad de las Operaciones Tecnológicas.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben definir los procesos que provean las capacidades necesarias que procuren garantizar la continuidad de las operaciones tecnológicas ante incidentes de Seguridad Cibernética y de la Información que puedan afectar significativamente las operaciones normales del negocio, contemplando las disposiciones siguientes:

a) **Esquema de Continuidad de las Operaciones Tecnológicas:** Se debe establecer un esquema de continuidad que incluya el desarrollo e implementación de sistemas e infraestructuras tecnológicas flexibles, creando una capacidad de gestión de crisis, así como la coordinación y el mantenimiento de los planes de continuidad y contingencia de las operaciones tecnológicas;

b) **Resiliencia:** Las aplicaciones críticas del negocio y la infraestructura tecnológica subyacente, se deben apoyar en equipos y sistemas robustos y confiables, con el apoyo de instalaciones alternativas o redundantes;

c) **Gestión de Crisis:** Establecer un proceso de gestión de crisis, con el soporte de una unidad de apoyo, que detalle las acciones que se deben tomar en caso de la

ocurrencia de un incidente de Seguridad Cibernética y de la Información, que afecten significantemente las operaciones normales del negocio;

d) **Planes de Continuidad y de Contingencia de las Operaciones Tecnológicas:** Los planes de continuidad de las operaciones tecnológicas deben ser desarrollados y documentados para apoyar los procesos críticos del negocio en la entidad. Para las operaciones tecnológicas que soportan los procesos no críticos, será suficiente con el desarrollo de un plan de contingencia;

e) **Planes de Recuperación ante Desastres:** Se deben establecer y documentar planes de recuperación ante desastres para las operaciones tecnológicas que soportan los procesos críticos del negocio y garantizar la disponibilidad de los mismos cuando sea necesario; y,

f) **Pruebas de Estrés:** Las pruebas de estrés relacionadas a la continuidad de las operaciones tecnológicas deben ser ejecutadas en intervalos de períodos no mayores a 1 (un) año, sin perjuicio del incremento de la frecuencia de las pruebas bajo circunstancias especiales o a requerimiento de los entes reguladores y supervisores. Debe existir un registro o constancia de la calidad y los resultados de las mismas.

## CAPÍTULO III
## MONITOREO Y EVALUACIÓN

**Artículo 41. Auditorías Internas.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer procesos de auditorías internas para garantizar la supervisión efectiva del Programa de Seguridad Cibernética y de la Información, contemplando los aspectos siguientes:

a) **Gestión de las Auditorías Internas de Seguridad Cibernética y de la Información:** El estado de Seguridad Cibernética y de la Información en los sistemas de la información y la infraestructura tecnológica, en adición a los procesos de evaluación a que hace referencia el Artículo 46 de este Reglamento, debe ser objeto de auditorías exhaustivas y periódicas, llevadas a cabo por la



…/

unidad interna de auditoría o a través de una firma de auditores externos, o bien, por un auditor externo que cuente con las competencias y certificaciones requeridas para el desarrollo de las mismas, según se defina en el instructivo correspondiente, registrados en la Superintendencia de Bancos y en cumplimiento con el proceso de auditoría interna de la entidad; y,

b) **Informes de Resultados de las Auditorías Internas de Seguridad Cibernética y de la Información:** Los resultados de las auditorías internas de Seguridad Cibernética y de la Información de los sistemas informáticos y la infraestructura tecnológica, deben contener la documentación y notificación a las partes interesadas de sus conclusiones y recomendaciones.

**Artículo 42. Desempeño de la Seguridad.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben establecer mecanismos que procuren asegurar un desempeño óptimo de la gestión de la Seguridad Cibernética y de la Información, contemplando los aspectos siguientes:

a) **Monitoreo de la Seguridad:** El Oficial de Seguridad Cibernética y de la Información debe monitorear permanentemente el estado de Seguridad Cibernética y de la Información; y,

b) **Informes sobre la Seguridad:** El Oficial de Seguridad Cibernética y de la Información debe elaborar informes periódicos y según necesidad, relativos a los riesgos de la Seguridad Cibernética y de la Información y los mismos serán presentados al comité funcional de seguridad cibernética y de la información en los tiempos establecidos por el mismo.

**Artículo 43. Cumplimiento del Monitoreo de la Seguridad.** Se debe establecer un procedimiento de gestión de cumplimiento de la Seguridad Cibernética y de la Información derivados de los lineamientos reglamentarios, jurídicos y de obligaciones contractuales.



## CAPÍTULO IV
## ESTÁNDARES INTERNACIONALES

…/

**Artículo 44. Estándares Internacionales.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, que de manera contractual accedan a los servicios prestados por entidades internacionales que habilitan la provisión de sus productos y servicios dentro de dicho sistema, deben cumplir, en cada caso en que aplique, con los objetivos siguientes:

a) Proteger los datos del cliente y facilitar la adopción de medidas de seguridad uniformes, apoyados en la Norma de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI-DSS, por sus siglas en inglés);

b) Asegurar la protección en la administración, procesamiento y transmisión, tanto en línea como fuera de línea, del Número de Identificación Personal (PIN, por sus siglas en inglés) del cliente, apoyados en los requerimientos de seguridad del PIN del grupo de estándares PCI – PTS;

c) Aplicar los requerimientos de seguridad y los procedimientos de evaluación de los proveedores de sistemas de aplicaciones de pago, apoyados en la Norma de Seguridad para las Aplicaciones de Pago (PA-DSS, por sus siglas en inglés); y,

d) Reforzar los controles de seguridad de los ambientes locales e infraestructuras relacionadas que interactúen con la red de SWIFT, apoyado en el Marco de Controles de Seguridad del Cliente (SWIFT – CSCF, por sus siglas en inglés).

**Artículo 45. Estándares Facilitadores del Cumplimiento de la Norma PCI-DSS.** A fin de facilitar el cumplimiento de la Norma PCI-DSS, las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y las entidades de apoyo y servicios conexos a quienes aplique a la adopción de la misma, debe cumplir con los objetivos siguientes:

a) Fortalecer la protección de los datos transmitidos desde el Punto de Interacción (PDI) hasta su destino final, apoyados en los requerimientos de soluciones para el cifrado punto a punto (P2PE) del estándar PCI – P2PE;

b) Reforzar los controles de seguridad física y lógica, en los procesos de producción y distribución de las tarjetas bancarias, apoyados en los requerimientos de seguridad para la producción y aprovisionamiento de tarjetas bancarias; y,

c) Robustecer los controles de seguridad para salvaguardar la integridad del entorno de datos del Token, tanto estáticos como dinámicos, apoyados en los estándares de seguridad para proveedores de servicios de Token (PCI – TSP).

**Párrafo**: En caso de que las entidades emisoras de tarjetas bancarias hayan tercerizado los servicios de producción de las mismas y los servicios de token estáticos y dinámicos, deben verificar el cumplimiento de los requerimientos que les apliquen a los citados terceros. Para los servicios de producción de tarjetas bancarias deberá tomarse en consideración lo establecido en los contratos de servicio suscritos con las marcas de tarjetas bancarias.

## CAPÍTULO V
## INFORMES DE CUMPLIMIENTO

**Artículo 46. Informes de Cumplimiento.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos que estén interconectadas con el SIPARD, deben cumplir con un procedimiento de autoevaluación a través de herramientas digitales, para la remisión de la información requerida, en los plazos y en la forma en que se determine mediante Instructivo. Las Superintendencias del sistema financiero, en coordinación con el Banco Central en su condición de Administrador del SIPARD, y los órganos reguladores sub-sectoriales a cuyos regulados alcance este Reglamento, implementarán dichas herramientas para la autoevaluación.

**Artículo 47. Requerimientos Adicionales de Información**. Las Superintendencias del sistema financiero y los órganos reguladores sub-sectoriales a cuyos regulados alcance este Reglamento, podrán requerir en cualquier momento, información adicional o complementaria a las entidades de intermediación financiera y las entidades públicas de intermediación financiera, respecto a la

…/

gestión del Programa de Seguridad Cibernética y de la Información. Del mismo modo, el Banco Central podrá requerir, en cualquier momento, información adicional o complementaria a los Administradores y Participantes del SIPARD y de los Sistemas de Pago y Liquidación de Valores que lo componen, a las Entidades de apoyo y servicios conexos, respecto a la gestión del Programa de Seguridad Cibernética y de la Información.

**Artículo 48. Verificación de los Entes Reguladores y Supervisores.** Las superintendencias del sistema financiero y los órganos reguladores sub-sectoriales a cuyos regulados alcance este Reglamento, así como el Banco Central, en su calidad de Administrador del SIPARD, podrán verificar la idoneidad del cumplimiento del Programa de Seguridad Cibernética y de la Información de sus entes regulados, así como de la evaluación independiente de la eficacia de dicha gestión.

## TÍTULO III
## COORDINACIÓN SECTORIAL DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNÉTICA

### CAPÍTULO I
### GOBERNANZA

**Artículo 49. Del Consejo Sectorial.** Se crea el Consejo Sectorial para la Respuesta a Incidentes de Seguridad Cibernética del sector financiero y estará integrado de la manera siguiente:

**Miembros permanentes con Voz y Voto:**

a) El Gobernador del Banco Central, quien lo Presidirá;

b) El Superintendente de Bancos;

c) El Superintendente del Mercado de Valores;

d) El Contralor del Banco Central;

e) El Subgerente de Sistemas e Innovación Tecnológica del Banco Central;

f) El Presidente de la Asociación de Bancos Comerciales de la República Dominicana, Inc. (ABA);

g) El Presidente de la Liga de Asociaciones de Ahorros y Préstamos Dominicana (LIDAAPI);

h) El Presidente de la Asociación de Bancos de Ahorro y Crédito y Corporaciones de Crédito, Inc. **(**ABANCORD**)**; y,

i) El Director del Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT por sus siglas en inglés) del sector financiero, habilitado de conformidad con este Reglamento, quien fungirá como Secretario, pero sólo con voz.

**Invitados permanentes con Voz:**

a) El Director de Seguridad Operativa del Banco Central;

b) El Director del Departamento de Sistemas y Tecnología del Banco Central;

c) El Director del Departamento del Sistema de Pagos del Banco Central;

d) El Director del Departamento de Seguridad Interna del Banco Central;

e) El Responsable de la Oficina de Gestión de Riesgos y Continuidad del Banco Central;

f) El Director del Departamento de Tecnología y Operaciones de la Superintendencia de Bancos;

g) El Director de Riesgos y Estudios de la Superintendencia de Bancos;

h) Un representante de alta jerarquía de la Superintendencia del Mercado de Valores; y,

i) Un representante de alta jerarquía de la Superintendencia de Pensiones.

**Párrafo I:** Los miembros permanentes de este Consejo Sectorial podrán delegar su representación en un funcionario de alta jerarquía.

**Párrafo II:** Los invitados permanentes de este Consejo Sectorial no podrán delegar su representación.

**Párrafo III**: El Consejo Sectorial podrá invitar otras entidades relacionadas al sector financiero a reuniones puntuales por requerimiento de 3 (tres) o más de sus miembros.

**Artículo 50. Facultades.** El Consejo Sectorial tendrá de manera enunciativa, pero no limitativa, las facultades siguientes:

a) Definir las prioridades y lineamientos para la coordinación del Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés;

b) Dar seguimiento a las actividades del Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés) y al funcionamiento de sus programas;

c) Coordinar los esfuerzos de cooperación entre las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, para la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad cibernética;

d) Realizar las recomendaciones de lugar para la consecución de los objetivos estratégicos del Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés);

e) Definir el marco de cooperación y comunicación del Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés) con las áreas funcionales de seguridad cibernética de las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y las entidades de apoyo y servicios conexos;

f) Definir el marco de cooperación y comunicación con otras comisiones de similar naturaleza y con aquellas definidas por Ley;

g) Definir los protocolos de comunicación hacia los demás sectores económicos y sociales de la República Dominicana; y,

h) Cualquier otra facultad atribuida por la Junta Monetaria.

**Artículo 51. Funcionamiento.** El Consejo Sectorial deberá reunirse de manera ordinaria previa convocatoria de su Presidente, quien establecerá el orden del día y sesionará válidamente con la presencia de al menos de 4 (cuatro) de sus miembros permanentes y el secretario de dicho Consejo, con una frecuencia de por lo menos 1 (una) vez por trimestre. El Presidente, podrá convocar extraordinariamente a tantas sesiones de trabajo como sean necesarias.

## CAPÍTULO II
## DEL MECANISMO SECTORIAL DE RESPUESTA A INCIDENTES DE SEGURIDAD CIBERNÉTICA

**Artículo 52. Creación del Mecanismo.** Se crea el Equipo de Respuesta a Incidentes de Seguridad Cibernética para el Sector Financiero (CSIRT, por sus siglas en inglés), bajo la dependencia administrativa del Banco Central y funcional del Consejo Sectorial, con la finalidad de definir acciones inmediatas para la prevención, detección, contención, erradicación y recuperación frente a incidentes de seguridad cibernética que afecten las entidades definidas en el objeto y ámbito de este Reglamento;

**Párrafo:** El presupuesto requerido, así como las modalidades de ejecución del mismo, para la puesta en funcionamiento y mantenimiento de las operaciones del

Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés), será determinado por la Junta Monetaria.

**Artículo 53. Responsabilidades.** El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés) debe cumplir con los deberes y responsabilidades que le sean otorgadas por el Consejo Sectorial.

**Artículo 54. Estructura.** El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés) debe contar con una estructura orgánica que facilite el cumplimiento de sus deberes y responsabilidades.

**Artículo 55. Dirección.** El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés), estará dirigido por un profesional designado por el Banco Central, en virtud de sus competencias administrativas y capacidad requerida para la dirección de equipos de respuesta de esta naturaleza.

**Artículo 56. Instalaciones.** El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés), operará en un lugar aislado, asegurado y sus sistemas de información e infraestructura tecnológica, deben estar implementados tomando en consideración la protección de la información sensible recibida y almacenada en sus sistemas de información. Asimismo, deberá contar con controles de seguridad físicos y lógicos de manera permanente.

**Párrafo I:** Las instalaciones de dicho Equipo estarán en un área restringida con el fin de evitar el acceso no autorizado a los recursos y a la información.

**Párrafo II:** Los servidores, los equipos de comunicaciones, los dispositivos de seguridad lógica y los repositorios de datos, deben permanecer en las instalaciones del Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés) o en un centro de datos autorizado por el Consejo Sectorial, donde el acceso físico y lógico se regirá por un estricto control de acceso, según lo definido en las políticas de acceso a ser elaboradas para esos fines.

**Artículo 57. Definición de Políticas.** El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés) debe contar con políticas que deben ser seguidas por su personal en la realización de sus operaciones acorde

a los lineamientos definidos por este Reglamento y por las disposiciones del Consejo Sectorial.

**Artículo 58. Establecimiento de los Servicios.** El Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés), debe establecer servicios de seguridad cibernética, a fin de dar apoyo a las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, en sus procesos de respuesta a incidentes de seguridad cibernética.

## TÍTULO IV
## DISPOSICIONES FINALES

### CAPÍTULO I
### RÉGIMEN SANCIONATORIO Y MEDIDAS PRECAUTORIAS

**Artículo 59. Sanciones.** Las entidades de intermediación financiera y las entidades públicas de intermediación financiera que infrinjan cualesquiera de las disposiciones contenidas en este Reglamento y en los instructivos que fueren creados para su implementación, serán pasibles de la aplicación de las sanciones establecidas en la Ley Monetaria y Financiera y en el Reglamento de Sanciones.

**Artículo 60. Medidas Precautorias.** Cuando los administradores y participantes del SIPARD previstos en este Reglamento, así como las entidades de apoyo y servicios conexos que mantengan una interconexión o intercambio de información con el SIPARD, y sus administradores y participantes, incumplan alguna de las disposiciones contenidas en este Reglamento y en los instructivos que fueren creados para su implementación, el Banco Central podrá suspender temporalmente su participación en el SIPARD, como medida precautoria y para minimizar el riesgo sistémico. De verificarse el incumplimiento continuo de las disposiciones enunciadas, podrá ser gestionado en coordinación con el organismo regulador correspondiente, la exclusión definitiva del Sistema de Pagos y Liquidación de Valores.

### CAPÍTULO II
### OTRAS DISPOSICIONES

**Artículo 61. Elaboración de Instructivos y Circulares.** El Banco Central y la Superintendencia de Bancos, deberán elaborar los instructivos y circulares con los lineamientos que consideren necesarios para la aplicación de este Reglamento.

**Artículo 62. Plazo de Adecuación.** Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben ajustarse a las disposiciones contenidas en este Reglamento en el plazo de 1 (un) año contado a partir de la fecha de entrada en vigencia de este Reglamento.'

2. Esta Resolución deberá ser publicada en uno o más diarios de amplia circulación nacional, en virtud de las disposiciones del literal g) del Artículo 4 de la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002**.**"

Publicado: 27 nov, 2018

**-END-**