OBSERVACIONES DE ABA AL PROYECTO DE REGLAMENTO DE SEGURIDAD CIBERNÉTICA Y DE LA INFORMACIÓN PUESTO EN CONSULTA PÚBLICA MEDIANTE LA 3RA. RESOLUCIÓN DE LA JUNTA MONETARIA DEL 12 DE ABRIL DEL 2018 (14 de junio del 2018).

Las observaciones y recomendaciones de ABA al Proyecto de Reglamento de Seguridad Cibernética y de la Información puesto en consulta pública mediante la 3ra. Resolución de la Junta Monetaria del 12 de abril del 2018 son:

1). El literal **gg) Incidente,** establece lo siguiente: *''Ocurrencia que potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de la información o la información que el sistema procesa, almacena, o transmite, o que constituye una violación o amenaza inminente de violación de políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.''* (el subrayado es nuestro).

ABA entiende que debería eliminarse en esta definición la palabra ''potencialmente'' y la frase de ''amenaza inminente de violación'' para que quede conceptualmente y de forma específica alineada a lo que es un Incidente. En consecuencia proponemos la siguiente redacción:

gg) **Incidente:** Ocurrencia que pone en peligro la confidencialidad, integridad o disponibilidad de la información o la información que el sistema procesa, almacena, o transmite, o que constituye una violación de políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

2). **El Párrafo IV del Artículo 7** establece: *''Dicha estructura deberá ser revisada periódicamente por el Consejo u órgano societario equivalente, para verificar su idoneidad e independencia de las áreas de negocios, tecnologías de la información y operaciones, a medida que cambien las estrategias y/o estructura de las entidades de intermediación financiera, administradoras y participantes del SIPARD, entidades públicas mixtas de intermediación financiera y , las entidades de apoyo y servicios conexos.''* (el subrayado es nuestro).

Dado que las estructuras organizativas de las entidades financieras se mantienen en el corto plazo estables, con cambios en el mediano o largo plazo, por lo que proponemos eliminar lo referente a revisiones periódicas y sustituir por ''supervisada''. Por otra parte, vemos que lo referente a *''independencia de las áreas de negocios, tecnologías de la información y operaciones''* pueden generar contradicciones, si de forma lógica, dicha área funcional de ciberseguridad queda incorporada al Comité de Riesgos, como bien establecen los Párrafos I y II de dicho Artículo.

Por lo anterior se propone la siguiente redacción al párrafo IV del Artículo 7:

Dicha estructura deberá ser **supervisada** por el Consejo u órgano societario equivalente, para verificar su idoneidad, a medida que cambien las estrategias y/o estructura de las entidades de intermediación financiera, administradoras y participantes del SIPARD, entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos.

3). **El Artículo 11, Literal d)** establece: '' *Llevar a cabo las acciones para el tratamiento del riesgo tecnológico en coordinación con las áreas pertinentes de negocio, previa aprobación del comité funcional de seguridad cibernética y de la información.''* (el subrayado es nuestro).

Se propone sustituir la frase ''llevar a cabo'' por ''gestionar'', para que quede más claro según las actividades funcionales que quedan asignadas al oficial de seguridad de información. Por lo que se propone la siguiente redacción al literal d) del Artículo 11:

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

4). **El literal e) del Artículo 26** establece lo siguiente: ''*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. 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.'' (El subrayo es nuestro).

Se propone que las copias de resguardo puedan ser realizadas fuera de línea y en formato digital, por lo que proponemos la siguiente redacción:

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**.

Adicionalmente, en lo referente a lo establecido para las copias de resguardo de las **pistas de auditoría**, proponemos que el **tiempo de retención sea de 90 días** para tener consistencia con normativas internacionales que regulan la actividad.

5). En el literal c) del Artículo 30 establece lo siguiente: *''Registro de Eventos de Seguridad Cibernética y de la Información: Los acontecimientos relacionados con la Seguridad Cibernética y de la Información serán 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;''* (el subrayado es nuestro)

Se propone sustituir el término de ''acontecimiento'' por el de ''incidentes'' para estandarizar y acotar a este tipo de situaciones. Además, que la retención de estos registros pueda realizarse fuera de línea. En ese sentido proponemos la siguiente redacción del literal c) del Artículo 30:

Los acontecimientos relacionados con **incidentes** de Seguridad Cibernética y de la Información serán 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, **fuera de línea**;

6). El literal b) del Artículo 37 establece lo siguiente: "*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. Dentro de estos entornos de desarrollo deben de ser establecidos mecanismos para asegurar la privacidad y protección de los datos de carácter personal;"* (el subrayado es nuestro).

Los entornos de desarrollo de sistemas requieren de una mayor flexibilidad en la gestión de accesos, ya que el personal que labora en estos medios y con las funciones de Desarrollo de Sistemas, necesitan realizar tareas que requieren niveles de accesos superiores a los usuarios finales y similares a los administradores. De esta manera, "asegurar la privacidad y protección de los datos" en estos ambientes requerirá de asumir altos riesgos o hacer poco efectiva la función hasta el punto de no ser factible. Sin

embargo, utilizando data no-productiva en estos entornos hace que pierda todo su valor y hace inútil el robo de la misma.

Adicionalmente, facilita a que el personal con las funciones de Desarrollo de Sistemas pueda realizar las tareas que necesita con eficiencia y también facilita la distribución o tercerización de estas funciones cuando aplique. Mientras tanto, la data de valor se mantiene debidamente protegida en ambientes productivos.

En este sentido ABA propone la siguiente redacción del literal b) del Artículo 37:

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 no-productivos.**

7). En el Párrafo del Artículo 45 se establece lo siguiente: '' *En caso de que las entidades hayan tercerizado los servicios de producción de tarjetas bancarias y servicios de token estáticos y dinámicos, las mismas deberán verificar el cumplimiento de los requerimientos definidos en estos estándares internacionales.''*

ABA considera que las entidades deben cumplir con los estándares internacionales que les aplique de acuerdo al requerimiento de sus contratos de servicios con marcas internacionales. En este sentido proponemos la siguiente redacción:

En caso de que las entidades hayan tercerizado los servicios de producción de tarjetas bancarias y servicios de token estáticos y dinámicos, las mismas deberán verificar el cumplimiento de los requerimientos **que les aplique de acuerdo al requerimiento de sus contratos de servicios con marcas internacionales.**

8). En el Artículo 62 referente al Plazo de Adecuación se establece que: *''Las entidades de intermediación financiera, los administradores y participantes del SIPARD, las entidades públicas mixtas de intermediación financiera y, las entidades de apoyo y servicios conexos, deben ajustarse a las disposiciones contenidas en este Reglamento dentro de un plazo de 1 (un) año contado a partir de la fecha de entrada en vigencia de este Reglamento.''* (el subrayado es nuestro).

Con respecto al plazo de implementación de este Reglamento, consideramos que no es suficiente debido a que se requerirán realizar: adecuaciones de estructura y procesos; capacitación del personal; implementación de herramientas tecnológicas que obligan a la identificación de soluciones, pruebas pilotos o demostraciones, procesos de licitación y adquisición, planes de proyecto de implementación y presupuestos.

Por lo anterior ABA solicita que el plazo para la implementación sea en base a un programa escalonado o desarrollado por etapas, sujeto a evaluaciones para determinar el avance, y que deberá ser establecido por el Consejo Sectorial posteriormente a la fecha de entrada en vigencia de este Reglamento.

9). En referencia al literal e) del Artículo 49 se propone que quien figure como miembro permanente con voz y voto sea el Presidente de la Asociación de Bancos Comerciales de la República Dominicana en vez del Presidente del Comité de Seguridad de la Asociación de Bancos Comerciales de la República Dominicana, por lo que se propone la siguiente redacción al literal c) del Artículo 49:

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

Por otro lado, debido a la importancia que tiene la banca múltiple en el sistema financiero y sistema de pagos, consideramos que es necesario tener una mayor representación de técnicos de alto nivel en este tipo de actuación en el Consejo Sectorial. Por lo que proponemos como invitados permanentes con voz, los siguientes miembros de ABA: el Presidente del Comité de Riesgos, el Presidente del Comité de Seguridad y el Presidente del Comité de Operaciones.

ABA
14 de junio 2018