SE
SECRETARÍA DE ECONOMÍA

CONAMER
COMISIÓN NACIONAL DE MEJORA REGULATORIA

COORDINACIÓN GENERAL DE MEJORA REGULATORIA SECTORIAL

ACUSE

SH SUBSECRETARIA DE INGRESOS
CP
20 NOV 2018
COORD. DE CONTROL DE GESTION
HORA 14:33 REC

Oficio No. COFEME/18/4350

Asunto: Se emite Dictamen Final, respecto del anteproyecto denominado ***Resolución que modifica las Disposiciones de carácter general aplicables a las instituciones de crédito.***

Ciudad de México, a 16 de noviembre de 2018

DR. ALBERTO TORRES GARCÍA
Subsecretario de Ingresos
Secretaría de Hacienda y Crédito Público
P r e s e n t e

Me refiero al anteproyecto denominado ***Resolución que modifica las Disposiciones de carácter general aplicables a las instituciones de crédito***, así como a su respectivo formulario de Análisis de Impacto Regulatorio (AIR), ambos instrumentos remitidos por la Secretaría de Hacienda y Crédito Público (SHCP) y recibidos por la Comisión Nacional de Mejora Regulatoria (CONAMER) el 8 de noviembre de 2018, a través del sistema informático correspondiente[1]. Asimismo, no se omite hacer mención de sus versiones previas del 15 y 23 de octubre del presente año.

Sobre el particular, con fundamento en los artículos Tercero, fracción II y Cuarto del *Acuerdo que fija los lineamientos que deberán ser observados por las dependencias y organismos descentralizados de la Administración Pública Federal, en cuanto a la emisión de los actos administrativos de carácter general a los que les resulta aplicable el artículo 69-H de la Ley Federal de Procedimiento Administrativo* (Acuerdo Presidencial) se le informa que procede el supuesto de calidad aludido (i.e. que la dependencia u organismo descentralizado cumpla con una obligación establecida en ley, así como en reglamento, decreto, acuerdo u otra disposición de carácter general expedidos por el Titular del Ejecutivo Federal); ello, en virtud de que el artículo 96 Bis de la *Ley de Instituciones de Crédito*[2] (LIC) establece que la Comisión Nacional Bancaria y de Valores (CNBV) emitirá disposiciones generales de carácter, para preservar la solvencia, liquidez y estabilidad de las instituciones de crédito, así como para mantener el sano y equilibrado desarrollo de las operaciones que realicen dichos intermediarios financieros, como es el caso del anteproyecto en comento.

Por otra parte, con fundamento en los artículos Tercero, fracción V, y Cuarto del Acuerdo Presidencial, le informo que también procede el supuesto de excepción aludido por la SHCP (i.e. los beneficios aportados por el acto administrativo de carácter general, en términos de competitividad y funcionamiento eficiente de los mercados, entre otros, sean superiores a los costos de su cumplimiento por parte de los particulares) ello, toda vez que conforme a la información presentada por esa Dependencia en la AIR, es posible advertir que los beneficios que generará la propuesta para los sujetos regulados serán superiores a los costos de cumplimiento, como se detallará más adelante en el presente oficio.

[1] http://cofemersimir.gob.mx/
[2] Publicada en el Diario Oficial de la Federación (DOF el 18 de julio de 1990 y modificada por última vez el 9 de marzo de 2018.

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México, Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

En este sentido, el anteproyecto y su AIR correspondiente quedaron sujetos al procedimiento de mejora regulatoria previsto en el Capítulo III de la *Ley General de Mejora Regulatoria*[3] (LGMR), por lo que con fundamento en lo dispuesto en sus artículos 25, fracción II, 26, 27, 71, cuarto párrafo y 75, este órgano desconcentrado tiene a bien emitir el siguiente:

DICTAMEN FINAL

I. Consideraciones respecto al requerimiento de simplificación regulatoria

En relación con los requerimientos de simplificación regulatoria previstos en los artículos 78 de la LGMR y Quinto del Acuerdo Presidencial, esta Comisión observa que a través del AIR correspondiente, así como de su documento anexo denominado *20181022185437_46225_Acuerdo 1X1 (22-oct-18).docx*, la SHCP solicitó que se tome en consideración la acción de simplificación descrita en el cuadro siguiente:

Cuadro 1. Flexibilizaciones realizadas para dar cumplimiento al artículo 78 de la Ley.

Trámite / Acción Regulatoria del anteproyecto	*Flexibilizaciones*
Nombre del Trámite: *Notificación de contingencias operativas.* ***Artículo aplicable:*** *164 Bis, fracción III de las Disposiciones.*	***Flexibilización:*** *Se reforman los artículos transitorios Cuarto, fracción III, segundo párrafo y Quinto, primero y tercero párrafos de la de la "Resolución modificatoria a las Disposiciones de carácter general aplicables a las instituciones de crédito", publicada en el Diario Oficial de la Federación el 6 de enero de 2017.* ***Acción:*** *se amplía el plazo con el que cuentan las instituciones de crédito para que tengan constituido el 100 % del monto de las estimaciones preventivas para riesgos crediticios que corresponden a las carteras crediticias de consumo no revolvente, hipotecaria de vivienda y microcréditos, conforme a la utilización de la nueva metodología aplicable, al tiempo de precisar cuándo deberán revelar dicha información en sus estados financieros, así como en cualquier comunicado público de información financiera. Lo anterior, con la finalidad de otorgar a las instituciones de crédito el tiempo adecuado para el cumplimiento de las obligaciones previstas en el marco regulatorio.* ***AHORRO:*** *$4,177,000,000.00, el cual ya fue dictaminado por CONAMER en la exención de AIR con número de folio 42732, que se encuentra bajo el expediente número 05/0067/300517.*
Acción regulatoria: *Conservación de registro de accesos y actividades de los usuarios de la infraestructura tecnológica.* ***Artículo aplicable:*** *168 Bis 11, fracción VIII, último párrafo de las Disposiciones.*	
Nombre del trámite: *Notificación de conclusiones de pruebas de penetración.* ***Artículos aplicables:*** *168 Bis 12, fracción IV, último párrafo de las Disposiciones*	
Nombre del trámite: *Notificación de planes de remediación sobre vulnerabilidades en componentes y sistemas críticos.* ***Artículos aplicables:*** *168 Bis 12, fracción VI, segundo párrafo de las Disposiciones.*	
Nombre del trámite: *Notificación de incidentes de seguridad de la Información.* ***Artículos aplicables:*** *168 Bis 16, fracción I de las Disposiciones*	
Acción regulatoria: *Conservación de registro de los incidentes de seguridad de la información no reportados.* ***Artículo aplicable:*** *168 Bis 16, fracción I, último párrafo de las Disposiciones.*	
Nombre del trámite: *Notificación de plan de trabajo para eliminar o mitigar riesgos y vulnerabilidades que generen incidentes de seguridad de la información.* ***Artículo aplicable:*** *168 Bis 16, fracción II de las Disposiciones.*	
Acción regulatoria: *Conservación de registro en bases de datos de incidentes, fallas o vulnerabilidades en la infraestructura tecnológica.* ***Artículo aplicable:*** *168 Bis 17 de las Disposiciones.*	
Acción regulatoria: *Obligaciones del director general en materia de seguridad de la información.* ***Artículos aplicables:*** *168 Bis 11, 168 Bis 12 y 168 Bis 13, primer párrafo de las Disposiciones.*	

[3] Publicada en el DOF el 18 de mayo de 2018.

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México, Tel. (01 55) 56 29 95 00 ext. 22637 | contacto@conamer.gob.mx

Trámite / Acción Regulatoria del anteproyecto	*Flexibilizaciones*
Acción regulatoria: *Designación, obligaciones y funciones del oficial en jefe de seguridad de la información (CISO por sus siglas en inglés Chief Information Security Officer).* ***Artículos aplicables:*** *168 Bis 13 y 168 Bis 14, así como Anexo 72 de las Disposiciones.*	
Acción regulatoria: *Funciones de los oficiales operativos de seguridad de la información.* ***Artículo aplicable:*** *168 Bis 15 de las Disposiciones.*	
Acción regulatoria: *Certificaciones PCI (Peripheral Component Interconnect) y EMV (Europay MasterCard Visa), en materia de banca electrónica.* ***Artículos aplicables:*** *316 Bis 10, fracción V de las Disposiciones.*	
Costo total: ***$152, 859, 896.00*** *pesos.*	*Ahorros:* ***$4,177,000, 000.00*** *pesos.*

Fuente: Elaboración propia con información de la SHCP.

En referencia a lo anterior, esta Comisión observa que efectivamente en el expediente referido en el cuadro precedente, esa Secretaría solicitó que los ahorros generados por su implementación, fueran tomados en cuenta para la emisión de futuras regulaciones. Por tales motivos esta CONAMER toma nota de las acciones y sus correspondientes ahorros, mismos que serán utilizadas para el cumplimiento del artículo 78 de la LGMR para el presente anteproyecto regulatorio.

En este sentido, respecto a la cuantificación que permita evidenciar que los ahorros que se generarán con la simplificación de las cargas regulatorias antes señaladas, se observa lo siguiente:

Cuadro 2. Costos vs. Ahorros

Nuevos costos de cumplimiento aproximados (Total).	Ahorros que se generarán a partir de las flexibilizaciones (Total).
$152,859,896.00 pesos	*$4, 177, 000, 000.00 pesos*

Fuente: Elaboración propia con datos de SHCP.

Bajo tales premisas, se observa que hay obligaciones regulatorias que se hacen más flexibles en su cumplimiento para los particulares, generando ahorros de hasta ***$4,177,000,000 pesos en una única ocasión***, mientras que los costos de cumplimiento del anteproyecto serán de aproximadamente ***$152,859,896 pesos anual***, tal y como se detallará en la sección *V. Impacto de la regulación* del presente dictamen. Al respecto, es factible prever que si dichos ahorros tuvieran que ser cuantificados de manera anual, la relación con los costos sería positiva por al menos por 27 años.

Asimismo, este órgano desconcentrado observa que esa Secretaría en los "Considerandos" del anteproyecto hizo referencia expresa a las acciones de simplificación regulatoria que llevó a cabo, a efecto de dar cumplimiento a lo establecido en el artículo 78 de la LGMR y primer párrafo del Artículo Quinto del citado Acuerdo, como se detalla a continuación:

> *"Que en atención al artículo 78 de la Ley General de Mejora Regulatoria y con la finalidad de reducir el costo de cumplimiento de las presentes disposiciones, la Comisión Nacional Bancaria y de Valores, mediante resolución publicada en el Diario Oficial de la Federación el 26 de junio de 2017, reformó la "Resolución modificatoria a las Disposiciones de carácter general aplicables a las instituciones de crédito" publicada en el mismo medio de difusión el 6 de enero de 2017, con el objetivo de ampliar el*

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22007 | contacto@conamer.gob.mx

plazo con el que cuentan las instituciones de crédito para que tengan constituido el 100 % del monto de las estimaciones preventivas para riesgos crediticios que corresponden a las carteras crediticias de consumo no revolvente, hipotecaria de vivienda y microcréditos, conforme a la utilización de la nueva metodología aplicable, al tiempo de precisar cuándo deberán revelar dicha información en sus estados financieros, así como en cualquier comunicado público de información financiera".

Por lo antes indicado, se advierte que los beneficios que se generarán con la simplificación, flexibilización, derogación o abrogación de las obligaciones regulatorias son superiores a los costos de cumplimiento del anteproyecto; ello, de conformidad con lo que se explicará más adelante en el apartado *V. Impacto de la regulación* del presente escrito.

En este sentido, esta Comisión estima que con dicha justificación se atiende lo previsto en el artículo 78 de la LGMR y al artículo Quinto del Acuerdo Presidencial.

II. Consideraciones generales

La regulación del sistema financiero es fundamental para garantizar su correcto funcionamiento, ya que un adecuado marco jurídico genera mayor certidumbre sobre las operaciones que realizan las instituciones que lo conforman, con lo cual se incentiva el aumento de la actividad económica a través de canalizar el ahorro de los diversos agentes al financiamiento a proyectos de inversión, con lo cual se coadyuva a la asignación eficiente de los recursos y al crecimiento de los países.

En este tenor, de acuerdo con la perspectiva desarrollada por Joseph Stiglitz[4], para que la regulación de los mercados financieros sea exitosa debe contener los siguientes propósitos:

a) Mantener la seguridad y solidez.
b) Promover la competencia entre los oferentes.
c) Proteger a los consumidores.
d) Asegurar que los grupos menos favorecidos tengan algún grado de acceso al capital.

Por consiguiente, a efecto de cumplir con el inciso a) es necesario proteger la infraestructura tecnológica que soporta la operación interna y externa de las instituciones de crédito y, en general, al sistema financiero de agresiones que vulneren su integridad, dado que el 70% de los ataques cibernéticos en el mundo está dirigido al sector financiero y México es el décimo lugar con más número de ofensivas a nivel global[5].

Al respecto, el Banco de México en su comunicado sobre la *Situación Actual del Sistema de Pagos Electrónicos Interbancarios* (SPEI) indica que *"reducir el riego a cero es una labor prácticamente imposible y, precisamente, en el margen de riesgo que queda sin cubrir es donde pueden presentarse las vulnerabilidades que afecten de manera irremediable a las instituciones de crédito. Tal es el caso de los acontecimientos que recientemente tuvieron lugar en el sistema bancario mexicano en donde se presentaron vulneraciones a la denominada Ciberseguridad, entendiendo por esta la preservación de la confidencialidad, integridad y disponibilidad de la información a través de infraestructuras tecnológicas interconectadas con personas, procesos o datos".*

---

[4] Premio Nobel de Economía 2001.
[5] Información disponible en la siguiente liga electrónica: https://www.eleconomista.com.mx/sectorfinanciero/CNBV-Ante-ciberataques-habra-medidas-de-seguridad-adicionales-20181029-0021.html (consultado el 15 de noviembre de 2018).

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22607. contacto@conamer.gob.mx

Asimismo, precisó que "*los ataques perpetrados han sido dirigidos hacia los bancos, casas de bolsa y otros participantes del sistema de pagos, enfocándose en los sistemas de los participantes con los que se conectan al Sistema de Pagos Electrónicos Interbancarios (SPEI). En resumen y con la información disponible, el Banco de México estima que los montos involucrados en envíos irregulares y sujetos a revisión son de aproximadamente 300 millones de pesos*[6]."

Por lo anterior, es necesario destacar que la infraestructura tecnológica es el activo más importante que tienen las instituciones de crédito, dado que, contiene la información financiera de sus clientes, por lo que deben existir medidas que la mantenga segura en las plataformas electrónicas.

En este sentido, el artículo 316 Bis 10 de las *Disposiciones de carácter general aplicables a las instituciones de crédito* (Disposiciones vigentes) establece que *"las instituciones que utilicen medios electrónicos para la celebración de operaciones y prestación de servicios, deberán implementar medidas o mecanismos de seguridad en la transmisión, almacenamiento y procesamiento de la información a través de dichos medios electrónicos, a fin de evitar que sea conocida por terceros".*

Bajo dichas consideraciones, para fortalecer el sistema financiero nacional se requiere que las instituciones de crédito consideren la seguridad de la información como un aspecto prioritario y además, conozcan las técnicas para prevenir los riesgos asociados a la misma, como es la finalidad de la propuesta regulatoria.

En este sentido, esta Comisión considera adecuada la expedición del presente anteproyecto, pues constituye un instrumento regulatorio alineado al marco jurídico vigente, que propicia el óptimo funcionamiento del sistema financiero, promoviendo las mejores prácticas en materia de los servicios de seguridad de la información dentro de las instituciones créditos supervisadas por la CNBV.

III. Objetivos regulatorios y problemática

En lo referente al presente apartado, de acuerdo con la información presentada por la SHCP, la propuesta regulatoria tiene los siguientes objetivos:

- *Proteger los activos de información, como elementos fundamentales de la Seguridad de la Información. En este sentido, se propone fortalecer la protección sobre lo siguiente: i) la información, que es el objeto de mayor valor para la institución de crédito, ii) los equipos, tales como software, hardware y la propia institución de crédito y iii) los usuarios, es decir, las personas que usan la tecnología de la institución de crédito.*
- *Llevar a cabo el análisis de los riesgos a que está expuesta la institución de crédito en el entorno que comprende la seguridad de la información, a fin de mejorar los procesos de las actividades siguientes:*

[6] Publicado en mayo de 2018 y véase: http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf (consultado el 15 de noviembre de 2018).

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

a) *Restricción del acceso a los programas y a los archivos más importantes, por parte de las personas que laboran en la institución de crédito.*

b) *Asegurar que los empleados y operadores de la infraestructura tecnológica pueden realizar su trabajo, pero sin realizar modificaciones que no sean necesarias en los programas ni archivos.*

c) *Salvaguardar la utilización de los datos, archivos y los programas correctos en los procedimientos elegidos.*

d) *Proteger la información transmitida, es decir, que esta sea la misma que sea reciba por el destinatario.*

e) *Prever que existen diferentes sistemas en caso de emergencia y que estos estén distribuidos por toda la institución de crédito.*

f) *Organizar a todos los empleados y otorgarles distintas claves, que sean intransferibles.*

g) *Actualizar de forma constante todas las contraseñas de acceso a la infraestructura tecnológica.*

- *Robustecer la política de seguridad de la información, a través de establecer medidas más estrictas a los derechos de acceso a los datos y a los recursos con los que cuenta la institución de crédito, así como fortaleciendo las herramientas de control y los mecanismos de identificación. De conformidad con lo anterior, es inminente que el cuerpo normativo en vigor debe actualizarse, para las instituciones de crédito puedan:*

a) *Ofrecer sus productos y servicios bajo un marco jurídico transparente y sólido que les otorgue seguridad y certeza jurídica en beneficio propio y de sus clientes, y*

b) *Incorporar las mejores prácticas nacionales e internacionales que conduzcan a una sana operación, incentiven las operaciones y servicios del mercado bancario, transparenten las operaciones, preserven y fomenten la confianza de los inversionistas, al tiempo de proteger su información y recursos, así como que cuenten con regulación equiparable. Lo anterior, redundaría en un sistema financiero con reglas equitativas en beneficio de quienes participan en el mercado de financiero, a través de las instituciones de crédito.*

En este sentido, esa Secretaría mencionó que la emisión de la propuesta regulatoria se deriva que en el país se han presentado vulneraciones a la ciberseguridad de las instituciones de crédito y, que el Banco de México estima que los montos involucrados en envíos irregulares y sujetos a revisión son de aproximadamente 300 millones de pesos.

Por lo anterior, esa Dependencia señaló la relevancia de realizar actualizaciones al marco regulatorio vigente a efecto de reducir los riesgos derivados de las innovaciones tecnológicas que se presentado, a fin de tener con entidades financieras competitivas que cuenten con niveles de seguridad similares a nivel internacional.

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22657 | contacto@conamer.gob.mx

Al respecto, esta CONAMER observa que a través de las adecuaciones propuestas al contenido de las Disposiciones vigentes, se contribuirá a proteger los activos de información robusteciendo la política de seguridad de la información para las diversas entidades financieras y personas sujetas a la supervisión de la CNBV.

Por lo anterior, esta Comisión considera justificados los objetivos y situación que da origen a la regulación propuesta toda vez que los mismos se encuentran alineados a la resolución de la problemática identificada en la presente sección, de conformidad con los principios de mejora regulatoria plasmados en el LGMR.

IV. Alternativas a la regulación

En lo referente a este apartado, la SHCP consideró que la propuesta regulatoria representa la mejor alternativa para atender la problemática señalada, toda vez que con su emisión se tendrán los siguientes beneficios:

- *Un solo instrumento normativo, que permitiría su fácil consulta, al igual que la localización de la normatividad que deben observar las instituciones de crédito.*

- *Reglas claras y transparentes en materia de seguridad de la información, lo que otorgaría certeza jurídica a las instituciones de crédito y al público usuario en la realización de sus actividades.*

- *Que las instituciones de crédito sean más competitivas, dado que se realizan diversos ajustes a las Disposiciones conforme a los realizados a la normatividad que deben observar otros intermediarios del sistema financiero, así como a las nuevas realidades operativas, y sanas prácticas nacionales e internacionales en materia de Seguridad de la Información.*

Sin perjuicio de lo anterior, esa Secretaría indicó que evaluó las diversas alternativas regulatorias y no regulatorias que pudieron haber sido utilizadas para atender la problemática:

- **No emitir regulación alguna**. Al respecto, esta alternativa fue descartada por esa Secretaría ya que al considerar que "*los destinatarios de la norma no tendrían un cuerpo normativo actualizado que atienda las necesidades del sector bancario, por lo que seguirían en desventaja con sus similares a nivel nacional e internacional. Asimismo, rezagaría el crecimiento y seguridad cibernética del mercado financiero en México, limitaría la presencia de una mayor diversidad de productos, inhibiría la competencia y resultaría en mayores costos de intermediación*".

- **Esquemas de voluntarios**. En referencia a tal mecanismo, la autoridad indicó que no consideró esta opción en razón que "*se generarían reglas diferenciadas y no se permitiría igualdad de circunstancias al operar en el sistema bancario. Además, estos esquemas generarían que existan dos normas aplicables: por un lado, las disposiciones vigentes, que no estarían actualizadas y adecuadas a lo que exige el dinamismo del mercado financiero, así como el esquema voluntario, lo que generaría incertidumbre jurídica para los destinatarios de la norma, al igual que para los ahorradores y usuarios de servicios bancarios, quienes se verían afectados*

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 20 95 00 ext. 22607 | contacto@conamer.gob.mx

al no tener seguridad respecto de la aplicación de un solo estándar que dé certeza a sus operaciones".

- **Incentivos económicos**. La SHCP señaló que descartó esta alternativa debido a que "*el objeto de la presente propuesta regulatoria no podría instrumentarse a través de incentivos económicos ya que, de acuerdo a lo previsto por la LCNBV y las leyes aplicables al sector bancario, esta autoridad no dispone de recursos para la implementación de dichos esquemas respecto al tema que versa la Propuesta Regulatoria; asimismo, el mercado financiero se vería distorsionado por la entrega de estos incentivos, generando competencia desleal, además de que dejaría en duda los objetivos que persigue la regulación*".

- **Esquemas de autorregulación**. En referencia a dicha opción, esa Secretaría mencionó que no era beneficiosa para el sistema financiero, dado que: "*(i) no se tendría un marco integral; (ii) no se atenderían las situaciones que dan origen a la intervención gubernamental, y (iii) no permitiría la estandarización de las normas aplicables a las instituciones de crédito. Adicionalmente, entorpecería las labores de supervisión de la CNBV, ya que se tendrían esquemas desiguales de aplicación de los aspectos que se regulan en la presente Propuesta Regulatoria, lo cual generaría un mercado desordenado e inseguro, en detrimento del patrimonio e intereses de los inversionistas*".

- **Otro tipo de regulación**. Esa Dependencia no consideró adecuada la emisión de otro tipo de regulación, dado que "*las materias sobre las que recae la presente propuesta regulatoria deben regularse a través de disposiciones de carácter general emitidas por la CNBV de acuerdo a lo establecido en la LIC. Por otra parte, ya existe un cimiento en las Disposiciones que regula algunos de los temas que toca la presente Propuesta Regulatoria; por lo cual, es deseable que dichas normas se sigan conteniendo en un solo ordenamiento jurídico como son las Disposiciones, a fin de tener instrumentos normativos auto contenidos que eviten distorsiones, confusión entre los destinatarios y desorden en el mercado financiero*".

En este sentido, la CONAMER considera que esa Secretaría analizó las distintas alternativas de política pública que pueden atender a la problemática y objetivos antes descritos, dando así cumplimiento al requerimiento de esta Comisión en materia de evaluación de alternativas regulatorias.

V. Impacto de la regulación

1. Creación, modificación y/o eliminación de trámites

Respecto al presente apartado, de acuerdo con la información contenida en el AIR correspondiente, la autoridad indicó que como consecuencia de la implementación de la presente propuesta regulatoria, se crearán los siguientes trámites:

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

Cuadro 3: Trámites identificados y justificados por la SHCP

No.	Nombre	Justificación	Información respecto al apartado 6 del formulario de AIR.
1	Notificación de contingencias operativas.	*(Artículo 164 Bis, fracción III de las Disposiciones) Con el fin de que las instituciones de crédito cuenten con más medios de contacto con la CNBV, se habilita un correo electrónico a efecto de que las instituciones hagan del conocimiento de manera más pronta una contingencia operativa que presente la institución de crédito de que se trate. Por otro lado, con la modificación de los requerimientos para considerar un evento como contingencia operativa a la afectación de componentes críticos de la infraestructura tecnológica o la afectación al treinta por ciento de sucursales, cajeros automáticos, terminales punto de venta o puntos de atención de sus comisionistas, se amplía el abanico de aquellos supuesto que pueden calificarse "contingencia operativa" a fin de hacer frente a los avances tecnológicos en materia de seguridad de la información.*	***Acción:*** *Modifica.* ***Tipo:*** *Obligación.* ***Vigencia:*** *Indefinida.* ***Medio de presentación:*** *dirección electrónica contingencias@cnbv.gob.mx u otros medios que disponga la CNBV al efecto.* ***Requisitos:*** *Fecha y hora de inicio de la contingencia operativa; indicación de si continúa o, en su caso, si ha concluido, fecha y hora de conclusión y su duración total; procesos, sistemas y canales afectados; una descripción del evento que se haya registrado y una evaluación inicial del impacto o gravedad.* ***Ficta:*** *No aplica.* ***Plazo:*** *No aplica.*
2	Notificación de conclusiones de pruebas de penetración.	*(Artículo 168 Bis 12, fracción IV, último párrafo de las Disposiciones) Con el fin de preservar la estabilidad financiera de las instituciones de crédito, así como el patrimonio e información de estas y de sus clientes, al igual que para detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga en riesgo la información y patrimonio de los clientes y de las instituciones de crédito, al igual que para verificar la integridad de los componentes de hardware y software que permitan detectar alteraciones de estos, es necesario que la CNBV tenga conocimiento de las pruebas de penetración realizadas en los sistemas y aplicativos de las instituciones de crédito y, por ende, de las vulnerabilidades detectadas en estos.*	***Acción:*** *crea.* ***Tipo:*** *Obligación.* ***Vigencia:*** *Indefinida.* ***Medio de presentación:*** *Escrito libre presentado ante la oficialía de partes de la CNBV.* ***Requisitos:*** *Conclusiones de las pruebas de penetración en los sistemas y aplicativos de la institución.* ***Ficta:*** *No aplica.* ***Plazo:*** *La notificación se deberá efectuar dentro de los siguientes veinte días hábiles de haberse finalizado las pruebas.*
3	Notificación de planes de remediación sobre vulnerabilidades en componentes y sistemas críticos.	*(Artículo 168 Bis 12, fracción VI, segundo párrafo de las Disposiciones). Con el fin de preservar la estabilidad financiera y operativa de las instituciones de crédito, estas deberán enviar a la CNBV planes de remediación respecto de las vulnerabilidades que las instituciones de crédito hayan detectado en sus sistemas y componentes críticos previa la realización de escaneos y pruebas de penetración.*	***Acción:*** *crea.* ***Tipo:*** *Obligación.* ***Vigencia:*** *Indefinida.* ***Medio de presentación:*** *Escrito libre presentado ante la oficialía de partes de la CNBV.* ***Requisitos:*** *Indicar el personal responsable de la implementación y ejecución de los planes de remediación, los plazos en que se realizarán, las actividades realizadas y por realizar, así como los recursos técnicos, materiales y humanos que serán empleados.* ***Ficta:*** *No aplica.* ***Plazo:*** *No aplica.*
4	Notificación de incidentes de seguridad de la Información.	*(Artículo 168 Bis 16, fracción I y Anexos 64 y 64 Bis de las Disposiciones) Con el fin de asegurar que la CNBV tenga conocimiento de los incidentes de seguridad de la información que se presenten en las instituciones de crédito, se establece la obligación de notificarle de manera inmediata cuando dichas contingencias tengan lugar y que como consecuencia de ello: i) se genere una pérdida económica. de información o interrupción de los servicios de la institución; ii) su modo de operación, incluyendo las vulnerabilidades explotadas, se pueda replicar a otras instituciones de crédito; iii) pueda representar una afectación a los clientes de la institución, la estabilidad del sistema financiero o de pagos, o bien, a los sistemas centrales de pagos, cámaras de compensación o a los depositarios*	***Acción:*** *crea.* ***Tipo:*** *Obligación.* ***Vigencia:*** *Indefinida.* ***Medio de presentación:*** *A la dirección electrónica Ciberseguridad_CNBV@cnbv.gob.mx u otros medios que disponga la CNBV al efecto.* ***Requisitos:*** *Que los incidentes de seguridad de la información se presenten en: i) los componentes de la infraestructura tecnológica; ii) los canales de atención a clientes, tales como medios electrónicos, oficinas bancarias o comisionistas de la*

2

Boulevard Adolfo López Mateos 3025, piso 10. Col. San Jerónimo Aculco. La Magdalena Contreras.
C.P. 10400. Ciudad de México. Tel: (01 55) 56 20 95 00 e t. 22607 | contacto@conamer.gob.mx

No.	Nombre	Justificación	Información respecto al apartado 6 del formulario de AIR.
		centrales de valores, y iv) cualquier otro que considere grave a juicio de la institución. Con los mismos objetivos de mantener informada a la CNBV, las instituciones de crédito deberán enviarle por escrito, dentro de los cinco días naturales siguientes al incidente de seguridad de la información de que se trate, la información que contienen los Anexos 64 y 64 Bis de las Disposiciones. Al respecto, cabe destacar que las instituciones de crédito ya están obligadas a presentar el señalado Anexo 64 y, con el fin de disminuir las cargas administrativas, en el Propuesta Regulatoria se pretende sustituir el contenido actual de dicho anexo para eliminar que las instituciones de crédito deberán reportar cualquier evento de pérdida de información administrada a través de medios electrónicos, conservando solamente la obligación de reportar los incidentes de seguridad de la información que se presenten en los componentes de la infraestructura tecnológica o en la operación de las referidas instituciones de crédito. Finalmente y con el objetivo de información antes indicado, las instituciones de crédito también deberán enviar a la CNBV el resultado de la investigación y el plan de trabajo, que debe elaborar el director general, incorporando las causas que generaron el incidente de seguridad de la información y estableciendo en el referido plan de trabajo las acciones a implementar para eliminar o mitigar los riesgos y vulnerabilidades que propiciaron el incidente.	*institución de crédito; iii) la infraestructura tecnológica de cualquier tercero que afecte la operación o la infraestructura tecnológica de las instituciones de crédito. Estos incidentes deben notificarse de manera inmediata.* ***Ficta:*** *No aplica.* ***Plazo:*** *No aplica.*
7	*Notificación de plan de trabajo para eliminar o mitigar riesgos y vulnerabilidades que generen incidentes de seguridad de la información.*	*(Artículo 168 Bis 16, fracción II de las Disposiciones) Con el fin de preservar la estabilidad financiera de las instituciones de crédito, así como el patrimonio e información de estas y de sus clientes, las instituciones de crédito, al generarse un incidente de seguridad de la información, deberán elaborar un plan de trabajo en el que se detallen acciones a tomar por parte de las instituciones afectadas a efecto de mitigar o eliminar los riesgos o vulnerabilidades que hayan dado margen al incidente de seguridad de la información.*	***Acción:*** *crea.* ***Tipo:*** *Obligación.* ***Vigencia:*** *No aplica.* ***Medio de presentación:*** *Escrito libre presentado ante la oficialía de partes de la CNBV.* ***Requisitos:*** *Indicar, al menos, el personal responsable del diseño del plan del trabajo, implementación, ejecución y seguimiento, plazos para su ejecución, así como los recursos técnicos, materiales y humanos que se emplearán al efecto.* ***Ficta:*** *No aplica.* ***Plazo:*** *No aplica.*

Al respecto, esta CONAMER observa que esa SHCP identificó los trámites que se crearán como consecuencia de la emisión de la propuesta regulatoria, así como la información a la que se refiere el artículo 46 de la LGMR. Por lo anterior, este órgano desconcentrado le conmina a revisar los argumentos vertidos en el apartado *VI. Comentarios respecto a los trámites del anteproyecto* del presente escrito.

2. *Disposiciones, obligaciones y/o acciones regulatorias distintas a los trámites*

Respecto del presente apartado y derivado de la revisión efectuada sobre el AIR correspondiente al anteproyecto, esta CONAMER da cuenta de que la SHCP detalló que con la emisión de la propuesta regulatoria se establecerán obligaciones para los sujetos regulados, las cuales han sido identificadas conforme a lo siguiente:

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco La Magdalena Contreras,
C.P. 10400 Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

Cuadro 4: Acciones regulatorias del anteproyecto

Núm.	Artículo aplicable	Justificación
1	*Artículo 160, fracción XIV*	*Es necesario que, un área de la institución que goce de independencia operativa en la gestión de incidentes de seguridad de la información, realice una evaluación de estos procesos, de esta manera esta obligación recaerá en el área de auditoria interna de las instituciones de crédito, garantizando así la imparcialidad en la evaluación de estos incidentes, lo que deriva en un proceso más seguro y confiable para los usuarios de la infraestructura tecnológica.*
2	*Artículo 168 Bis 11, fracción VIII, último párrafo*	*Conservación de registro de accesos y actividades de los usuarios de la infraestructura tecnológica, con el fin de asegurar que la CNBV tenga conocimiento y pueda ejercer su facultad de vigilancia de los accesos o intentos de acceso y las actividades efectuadas por los usuarios de la infraestructura tecnológica de las instituciones de crédito, estas estarán obligadas a conservar el registro de los registros de auditoría que incluyan los accesos o intentos de acceso y la operación de los usuarios de la infraestructura cuando dichos registros se refieran a actividades realizadas sobre componentes que procesen o almacenen información considerada como crítica por la institución, durante al menos tres años, tratándose de otros accesos la conservación se realizará por al menos seis meses.*
3	*Artículos 168 Bis 11, 168 Bis 12 y 168 Bis 13, primer párrafo.*	*Las modificaciones que se plantean en la Propuesta Regulatoria en materia de las obligaciones que el director general tienes respecto a la seguridad de la información tiene como fin de robustecer los controles internos con los que deberán contar las instituciones de crédito. Al respecto, se está proponiendo fortalecer principalmente algunas de las funciones que ya tiene respecto de la infraestructura tecnológica, y adicionando las que, debido a la importancia de salvaguardar la confidencialidad, integridad y disponibilidad de la información de los usuarios de la infraestructura tecnológica contenida en aplicativos y sistemas y que repercute en la estabilidad financiera de la institución, así como de sus clientes. Con lo anterior, se persigue evitar la fuga de información y el fortalecimiento de los activos tecnológicos. En este sentido las obligaciones del director general son del tenor siguiente: (i) Implementar el sistema de control interno en materia de seguridad de la información que procure su confidencialidad, integridad y disponibilidad; (ii) Aprobar el denominado "Plan Director de Seguridad", así como definir y priorizar los proyectos en materia de seguridad de la información, e informar al consejo de administración de la institución de crédito el contenido del mencionado plan, y contar con evidencia de su implementación; (iii) Llevar a cabo revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la Infraestructura Tecnológica; (iv) Elaborar un calendario anual para la realización de pruebas de escaneo de vulnerabilidades de los componentes de la Infraestructura Tecnológica; (v) Contratar a un tercero independiente, con personal que cuente con capacidad técnica comprobable mediante certificaciones especializadas de la industria en la materia, para la realización de pruebas de penetración en los diferentes sistemas y aplicativos de la institución de crédito con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los clientes y de la propia institución; (vi) Clasificar las vulnerabilidades detectadas de acuerdo con la metodología aprobada por el comité de riesgos; (vii) Elaborar planes de remediación respecto de los hallazgos de las revisiones y pruebas a que se refieren los incisos iii, iv y v anteriores; (viii) Implementar procesos de seguimiento al cumplimiento de los planes de remediación referidos; (ix) Implementar los programas anuales de capacitación a los que se refiere la en materia de administración integral de riesgos, así como los de concientización en materia de seguridad de la información, dirigidos a todo el personal y a los clientes incluyendo, en su caso, a terceros que le presten servicios; (x) Realizar, de manera proactiva e iterativa, la búsqueda de alertas de fraude, así como de amenazas que pudieran afectar a la seguridad de la información del público usuario, al igual que acciones para su protección considerando; (xi) Implementar controles que permitan a la institución de crédito asegurar la confidencialidad, integridad y disponibilidad de la información del público usuario y de la propia Institución o el acceso a la Infraestructura Tecnológica, por parte de sus empleados o personal que tengan acceso a ella, y (xii) Designar*

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México, Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

Núm.	Artículo aplicable	Justificación
		al oficial en jefe de seguridad de la información (CISO por sus siglas en inglés Chief Information Security Officer).
4	*Artículo 168 Bis 13 y 168 Bis 14, así como Anexo 72.*	*Es menester que exista una figura que vele por la seguridad de la información de las instituciones de crédito y que asuma un rol activo en la búsqueda de vulnerabilidades en los sistemas para la detección de fallas, errores o vulnerabilidades en la infraestructura tecnológica que permita su identificación para crear medidas y procedimientos para evitar la materialización de un incidente de seguridad de la información y de esta forma preservar la estabilidad financiera de las instituciones y de sus clientes, todo ello utilizando al efecto los lineamientos y criterios establecido en el Anexo 72 de las Propuesta Regulatoria. Cabe destacar que, el CISO puede ser designado como tal para varias entidades financieras que formen parte de consorcios o grupos empresariales.*
5	*Artículo 168 Bis 15.*	*Dado que se establece la figura del oficial en jefe de seguridad de la información (CISO) para dar cumplimiento a las disposiciones en materia de seguridad de la información, se habilita a las instituciones para que puedan apoyarse de personal existente en las instituciones que tendrán como funciones el apoyo al oficial en jefe, lo anterior para que este último esté en aptitud de poder cumplir con sus funciones, y así se logre un monitoreo en el avance de la estrategia de seguridad de la información a efecto de garantizar el ciclo de mejora continua dentro de los controles de las instituciones.*
6	*Artículo 168 Bis 16, fracción I, último párrafo*	*Conservación de registro de los incidentes de seguridad de la información no reportados, con el fin de asegurar que, en el momento que así lo requiera, la CNBV tenga conocimiento de los incidentes de seguridad de la información que se presenten en las instituciones de crédito, estas estarán obligadas a conservar por diez años el registro de los incidentes que se hayan presentado y que, por no estar obligadas, no hayan sido reportados a la CNBV.*
7	*Artículo 168 Bis 17*	*Conservación de registro en bases de datos de incidentes, fallas o vulnerabilidades en la infraestructura tecnológica, con el fin de asegurar que, en el momento que así lo requiera, la CNBV tenga conocimiento de los incidentes, fallas o vulnerabilidades detectadas en la infraestructura tecnológica, las instituciones de crédito estarán obligadas a conservar un registro de bases de datos de todos estos eventos, así como de las medidas correctivas que hayan implementado en razón de los incidentes, fallas o vulnerabilidades detectadas.*
8	*Artículo 316 Bis 10, fracción V.*	*Cumplir con las certificaciones PCI (Peripheral Component Interconnect) y EMV (Europay MasterCard Visa), en la industria de pagos garantiza que las instituciones de crédito conozcan e implementen los estándares que han sido establecidos y probados para preservar la estabilidad financiera de cada uno de los usuarios, incluyendo comercios, procesadores de pagos, las propias instituciones de crédito y, por ende, en la seguridad financiera del público usuario.*
9	*Artículo 160, fracción XIV.*	*Es necesario que, un área de la institución que goce de independencia operativa en la gestión de incidentes de seguridad de la información, realice una evaluación de estos procesos, de esta manera esta obligación recaerá en el área de auditoria interna de las instituciones de crédito, garantizando así la imparcialidad en la evaluación de estos incidentes, lo que deriva en un proceso más seguro y confiable para los usuarios de la infraestructura tecnológica.*
10	*Artículo 51 Bis 3, segundo párrafo.*	*Se establece la obligación para las instituciones de crédito de adoptar un mecanismo con un orden para capturar huellas dactilares, ya que es necesario para garantizar que las instituciones de crédito cuenten con una base de datos de sus empleados, directivos y funcionarios, y que de esta manera estas puedan ser plenamente identificados y separados de las huellas de sus clientes y así, evitando con esta medida, la materialización de incidentes de seguridad de la información.*
11	*Artículo 1, fracciones XIII, XXXIX, LXXVI, LXXXII, LXXXIII, CXXXVI y CXCII; 11; 12, fracción III; 15, fracción V; 51 Bis 3, fracción I y último párrafo; 51 Bis 5, fracción I; 51 Bis 9, fracción I; 71, fracción IX; inciso b); 86, fracción III,*	*Los cambios propuestos no representan una acción regulatoria en sí y, por tanto, no generan costo alguno en las instituciones de crédito; sin embargo, para que la CONAMER cuente con toda la información soporte para su análisis respecto la Propuesta Regulatoria, le manifestamos que se realizaron los siguientes cambios que consisten en ajustes de redacción, referencias, términos definidos o re-numeración del articulado: 1. Ajustes de redacción a fin de: i) Cambiar el término "infraestructura tecnológica" por el de "Infraestructura Tecnológica" como el definido en el artículo 1, fracción LXXXIII de la Propuesta Regulatoria;*

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 [illegible] contacto@conamer.gob.mx

Nota	Artículo aplicable	Justificación
	inciso b); 141, fracción III; 160, fracción III; 164, fracción IV, incisos f) y h); 166, fracción III y 316 Bis 14, primer párrafo.	*ii) adicionar en el concepto "Autenticación" a los usuarios que utilizan u operan con la infraestructura tecnológica; iii) eliminar del concepto "Información Sensible" las palabras "de los Usuarios" para que este tipo de información también comprenda a la de cualquier persona que contrata operaciones y servicios con una institución de crédito, y iv) ajustar verbos. Todo ello con el fin de contar con reglas claras y adecuadas que permitan su fácil observancia al modificar su redacción. 2. Incorporación de dos nuevos términos que se citan en el proyecto de la Sección Octava Bis del Capítulo IV del Título Segundo que se presenta en la Propuesta Regulatoria, con el fin de facilitar a las instituciones de crédito el cumplimiento de las obligaciones que tienen que realizar en términos de la mencionada sección. 3. Re-numeración de fracciones que, por la inclusión de otras, fue necesario recorrerse en su orden, así como la actualización de su referencia en otros preceptos. 4. Para mejor comprensión del texto, se realizan ajustes en la forma en la que estos se presentan.*

Fuente: Elaboración propia con datos de la SHCP.

Por lo anterior, esta Comisión considera que la SHCP identificó y justificó las acciones regulatorias que se desprenderán de la emisión de la propuesta regulatoria.

3. Costos

En lo referente al presente apartado, esa Dependencia indicó que derivado de la emisión del anteproyecto en comento, se generarán costos para los sujetos obligados derivados de los trámites señalados en el apartado anterior, como se indica a continuación:

Cuadro 5: Costos relacionados con trámites identificados por la SHCP

Concepto	Justificación
Trámite: Notificación de contingencias operativas.	*Este trámite no representa costo alguno, al contrario, se trata una flexibilización al trámite en el sentido de que la contingencia operativa de que se trate, podrá ser avisada a la CNBV a través de un correo electrónico, mediante los equipos de cómputo con los que ya cuentan las instituciones de crédito.*
Notificación de conclusiones de pruebas de penetración.	A fin de notificar a la CNBV las conclusiones de las pruebas de penetración es necesario utilizar un servicio de pruebas de penetración para que lleve a cabo dichas pruebas y elabore las conclusiones que correspondan. Al efecto, las instituciones de crédito de deberán contratar dos especialistas en pruebas de penetración denominadas *Pentest* con duración de 4 semanas, cuyo costo asciende a $ 321,600.00, lo que multiplicado por las cincuenta entidades que conforman el sector, equivale a un gasto aproximado de $16'080,000.00. **Total Costos: $16'080,000.00**
Notificación de planes de remediación sobre vulnerabilidades en componentes y sistemas críticos.	A fin de notificar a la CNBV los planes de remediación, es menester que la institución de crédito contrate dos especialistas que los elaboren, cuyo sueldo mensual asciende a $26,000.00 por cada uno, lo que arroja un gasto mensual de $2'600,000.00 por las cincuenta instituciones de crédito que conforman el sector, erogación que solo se realizará cuando se requiera elaborar los planes de que se trata. **Total Costos: $2'600,000.00**
Notificación de incidentes de seguridad de la Información.	Con el propósito de notificar incidentes de seguridad de la información, es necesario que la institución de crédito encomiende dicha tarea a los mismos especialistas que tienen la finalidad de realizar los planes de remediación contemplados en el numeral 4 del presente cuadro, cuyo sueldo mensual asciende a $26,000.00 por cada uno, lo que arroja un gasto mensual de $2'600,000.00 por las cincuenta instituciones de crédito que conforman el sector, erogación que solo se realizará cuando se requiera elaborar los planes de que se trata. **Total Costos: $2'6000,000.00**
Notificación de plan de trabajo para eliminar o mitigar riesgos y vulnerabilidades que generen incidentes de seguridad de la información.	Para llevar a cabo una investigación sobre la causa que generó el incidente de seguridad de la información, establecer un plan de trabajo de las acciones a implementar y notificar a la CNBV el citado plan, se requiere de atención especializada por como la descrita en el numeral 4 del presente cuadro, quienes devengan un sueldo mensual de alrededor de $26,000.00 por cada uno, lo que arroja un gasto mensual de $2'600,000.00 por las cincuenta instituciones de crédito que conforman el sector, erogación que solo se realizará cuando se requiera elaborar los planes de que se trata. **Total Costos : $2'600,000.00**

Fuente: Elaboración propia con datos de la SHCP.

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 45 00 ext. 22607 | contacto@conamer.gob.mx

Asimismo, de acuerdo con la información contenida en el AIR y derivado del análisis del anteproyecto, se observa que tras su emisión, se establecerán obligaciones para los particulares regulados, las cuales fueron cuantificadas por esa Secretaría, conforme a lo siguiente:

Cuadro 6: Costos identificados por la SHCP

Acción Regulatoria	Justificación
Obligaciones del director general en materia de seguridad de la información.	1. ***Asegurarse que la infraestructura tecnológica se apegue a los requerimientos indicados en el artículo 168 Bis 11 de la Propuesta Regulatoria*** *Para este objetivo, las instituciones de crédito deben implementar un software denominado "Configuration Management Data Base (CMDB por su acrónimo en inglés), cuyo costo asciende a $17,016.30, representando un gasto por las cincuenta instituciones que conforman el sector de $850,815.00.* *De igual forma, deberán implementar un sistema de prevención como la denominada Consultoría de Hardening comprende alrededor de 450 equipos con un servicio de dos días al mes, lo que representa un gasto por $71,696.00 que deriva en un costo total para el sector de $3'584,800.00.* *De la misma forma, las instituciones deberán realizar un gasto por la implementación de una solución informática conocida como DLP (Data Loss Prevention), que en el mercado especializado oscila entre $982,003.00, lo que resulta un gasto por el total del sector de $49'100,150.00.* ***Subtotal 9.1: $53, 535, 765.00*** 2. ***Contar con un Plan Director de Seguridad e informar al consejo de dicho plan*** *Al respecto, las instituciones de crédito deberán contratar una consultoría para la generación de estrategia de seguridad, la cual proporcionará servicios profesionales para llevar acabo la evaluación de la administración integral de riesgos, cuyos servicios tienen un costo promedio de $231,168.62, resultando por el sector un gasto de $11'558,431.00.* ***Subtotal 9.2: $11, 558, 431.00*** 3. ***Efectuar revisiones de seguridad*** *Para esta finalidad las instituciones de crédito deberán de contratar los servicios de dos especialistas que lleven a cabo las revisiones de seguridad correspondientes, servicios que tienen un costo promedio de $231,168.62, resultando por el sector un gasto de $11'558,431.00.* ***Subtotal 9.3: $11, 558, 431.00*** ***(se subsume en el numeral 9.2 anterior)*** 4. ***Realizar pruebas de escaneo de vulnerabilidades*** *Para atender la obligación descrita, las instituciones de crédito requieren el servicio de escaneo de vulnerabilidades por un periodo de 4 trimestres con un alcance de 100 equipos, gasto que asciende a $611,664.00, resultando un costo para las cincuenta instituciones que conforman el sector de $30'583,200.00.* ***Subtotal 9.4: $30, 583, 200.00*** 5. ***Obligaciones adicionales del director general en materia de seguridad de la información, tales como: (i) Programas anuales de capacitación y concientización en materia de***

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México, Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

Acción Regulatoria	Justificación
	seguridad de la información; (ii) Realizar la búsqueda de alertas de fraude así como de amenazas considerando al menos la continua investigación y análisis de información, la implementación de procesos para proteger la información o recursos de clientes y que se cuente con procedimientos de comunicación para clientes afectados, esta obligación tiene que documentarse en manuales y políticas de procedimientos *Para cumplir con las obligaciones descritas, las destinatarias de la norma deben implementar la denominada "Consultoría de concientización de seguridad interno y clientes. Plataforma Knowbe4" con alcance de 12 meses por 2,000 licencias Silver la cual, en el mercado especializado, asciende a $166,500.00 por cada institución de crédito, derivando en un gasto para el sector de $8'325,000.00.* ***Total : $104, 002, 396.00** pesos*
Designación, obligaciones y funciones del oficial en jefe de seguridad de la información (CISO por sus siglas en inglés Chief Information Security Officer).	*Para contar con una figura que vele por la seguridad de la información, las instituciones de crédito deberán contratar un profesionista denominado CISO, con rango de sueldo mensual de $141,000.00, lo que multiplicado por las cincuenta entidades que conforman el sector, resulta un gasto de $7'050,000.00.* ***Total: $7,050, 000.00** pesos*
Funciones de los oficiales operativos de seguridad de la información.	*Al igual que en numeral inmediato anterior, para contar con personal que velen por la seguridad de la información en cada una de las áreas de la institución de crédito de que se trate, las instituciones de crédito deberán contratar en promedio dos profesionistas denominados CISO, con rango de sueldo mensual de $70,500.00, lo que multiplicado por las cincuenta entidades que conforman el sector, resulta un gasto de $7, 050, 000.00.* *Es importante destacar que esta esta función puede ser desarrollada por personal de las áreas de negocio, por lo que este costo es opcional.* ***Total: $7, 050, 000.00** pesos*
Certificaciones en materia de banca electrónica (PCI y EMV).	*Obtener las certificaciones denominadas PCI (*Peripheral Component Interconnect*) y EMV (Europay MasterCard Visa), representa un costo para cada institución de crédito de $104,550.00, lo que multiplicado cincuenta instituciones que conforman el sector, resulta un costo de $5'227,500.00.* ***Total: $5, 227, 500.00** pesos*
Conservación de registro de accesos y actividades de los usuarios de la infraestructura tecnológica.	*Para la conservación de que se trata, las instituciones de crédito deberán adquirir un sistema de conservación conocido como NAS (Network Attached Storage) o servidor de almacenamiento, el cual tiene en el mercado especializados un costo de alrededor de $217,000.00 por cada ochenta TB, que es la cantidad que se estima necesaria para almacena la información de que se trata por el periodo solicitado de tres años, por lo cual el costo aproximado por sector ascendería a $10'850,000.00 a razón de un equipo por cincuenta instituciones que lo conforman.* ***Total Costos: $10'850,000.00 pesos***
Conservación de registro de los incidentes de seguridad de la información no reportados.	Para la conservación de que se trata, las instituciones de crédito deberán adquirir un SIEM o servidor de almacenamiento, los cuales tiene en el mercado especializados un costo de alrededor de $217,000.00 por cada ochenta TB, por lo cual el costo aproximado por sector ascendería a $10'850,000.00, a razón de un equipo por cincuenta instituciones que lo conforman. ***Total Costos: $10, 850, 000.00 pesos***
Conservación de registro en bases de datos de incidentes, fallas o	*Para la conservación de que se trata, las instituciones de crédito deberán adquirir un SIEM o servidor de almacenamiento, los cuales tiene en el mercado especializados un costo de alrededor de $217,000.00 por cada ochenta TB, por*

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras,
C.P. 10400, Ciudad de México, Tel. (01 55) 56 29 95 00 ext. 22607 | **contacto@conamer.gob.mx**

Acción Regulatoria	Justificación
vulnerabilidades en la infraestructura tecnológica.	*lo cual el costo aproximado por sector ascendería a $$10'850,000.00, a razón de un equipo por cincuenta instituciones que lo conforman.*
	Total Costos 8: $10, 850, 000.00 pesos

Bajo tales consideraciones, el costo total asociado a la emisión de la propuesta regulatoria asciende a ***$152,859,896.00 pesos*** totales anuales.

4. Beneficios

En lo referente a la presente sección, la SHCP mencionó que con la emisión de la regulación propuesta se busca "*establecer, mantener y demostrar el cumplimiento del estándar de la Industria de Pagos PCI es un beneficio para todos los miembros de la red de tarjetas de pago, incluyendo a los comercios, procesadores, instituciones bancarias, así como las empresas que almacenan, procesas o transmiten los datos de los consumidores de tarjetas de débito y crédito y/o datos confidenciales de autenticación de los clientes, toda vez que se reduce la información a la que se tiene acceso por personas no autorizadas, así como el aumento de controles en materia seguridad información atendiendo los puntos de revisión del estándar*".

En este sentido, esa Secretaría señaló que "*de no atender la mitigación de riesgos en materia de seguridad de la información, se presentaría una brecha que se refleja en pérdidas económicas como las ocurridas con el denominado Caso SPEI con una pérdida total para cinco instituciones de crédito de $300'000,000.00, esto es un promedio de $60, 000, 000.00 por institución. En tal sentido, si las cincuenta instituciones de crédito que conforman el sector tuvieran afectaciones de esta naturaleza, las pérdidas ascenderían a **$3,000,000,000.00** pesos por lo cual implementar medidas en materia de seguridad de la información representaría un ahorro de dicho monto*".

Bajo tales consideraciones, es posible advertir que los beneficios de la presente propuesta regulatoria son notoriamente superiores a los costos de cumplimiento para los particulares, como lo muestra el cuadro siguiente:

Cuadro 7: Costos *vs.* Beneficios

Costos	Beneficios
$152'859,896.00 pesos	$3,000'000,000.00 pesos

Fuente: Elaboración propia con información de CNBV.

En consecuencia y conforme a la información presentada por la SHCP, se aprecia que la regulación cumple con los objetivos de mejora regulatoria, en términos de transparencia en elaboración y aplicación y que éstas generen mayores beneficios que costos de cumplimiento para los particulares.

VI. Comentarios sobre los trámites del anteproyecto

Conforme lo señalado en el apartado *V. Impacto de la regulación, sección 1. Creación, modificación o eliminación de trámites*, del presente escrito, se advierte que derivado del análisis realizado a las disposiciones del anteproyecto, tras su emisión se crearán diversos trámites.

2

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras, C.P. 10400, Ciudad de México, Tel. (01 55) 56 29 95 00 ext. 22607 | contacto@conamer.gob.mx

En este sentido, conforme lo dispuesto por el artículo 47 de la LGMR, se comunica a la SHCP que deberá proporcionar a la CONAMER la información prevista en el artículo 46 de ese ordenamiento legal, respecto a todos los trámites indicados en la sección correspondiente del presente escrito, dentro de los 10 días hábiles siguientes a que se publique en el Diario Oficial de la Federación (DOF) el anteproyecto en comento, a fin de que se realicen las adecuaciones correspondientes a la información inscrita en el Registro Federal de Trámites y Servicios a cargo de esta Comisión.

VII. Consulta pública

En lo que respecta al presente apartado, tal y como se señaló con anterioridad, el anteproyecto y su AIR fueron recibidos por esta CONAMER por primera ocasión el 15 de octubre de 2018, por lo que a la fecha del presente escrito se ha cumplido con al menos veinte días de consulta pública que prevé para tal efecto el segundo párrafo del artículo 73 de la LGMR. Asimismo, se observa que la Asociación de Bancos de México el 16 de octubre del año en curso se pronunció a favor de la emisión del presente anteproyecto, indicando que fortalecerá el marco normativo sobre la seguridad de sus sistemas e infraestructuras tecnológicas y robustecerá los controles internos en la materia de la Banca en México.

Dicho comentario se puede encontrar en la siguiente liga electrónica para su consulta:

http://www.cofemersimir.gob.mx/portales/resumen/46349

Por todo lo expresado con antelación, la CONAMER resuelve emitir el presente **Dictamen Final** respecto a lo previsto en el artículo 75 de la LGMR, por lo que la SHCP puede continuar con las formalidades necesarias para la publicación del referido anteproyecto en el DOF, en términos del artículo 76 de esa Ley.

Lo anterior, se emite con fundamento en los preceptos jurídicos antes mencionados, en los artículos Séptimo Transitorio y Décimo Transitorio de la LGMR, en los artículos 7, fracción I, 9, fracciones XI y XXXVIII, penúltimo párrafo, y 10, fracción VI, del *Reglamento Interior de la Comisión Federal de Mejora Regulatoria*[7], así como Primero, fracción I, del *Acuerdo por el que se delegan facultades del Titular de la Comisión Federal de Mejora Regulatoria a los servidores públicos que se indican* y en el *Anexo Único del Acuerdo por el que se fijan plazos para que la Comisión Federal de Mejora Regulatoria resuelva sobre anteproyectos y se da a conocer el Manual de la Manifestación de Impacto Regulatorio*[8].

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

Atentamente
El Coordinador General

JULIO CÉSAR ROCHA LÓPEZ

CFP/ORM

[7] Publicado en el DOF el 28 de enero de 2004, con su última modificación publicada el 9 de octubre de 2015.
[8] Publicado en el DOF el 26 de julio de 2010.

Boulevard Adolfo López Mateos 3025, piso 10, Col. San Jerónimo Aculco, La Magdalena Contreras.
C.P. 10400, Ciudad de México. Tel. (01 55) 56 29 95 00 ext. 22907 | contacto@conamer.gob.mx

COMISIÓN NACIONAL DE
MEJORA REGULATORIA
RECURSOS MATERIALES
16 NOV. 2018
RECIBIDO
RÚBRICA 14:40