Vigente		Propuesta
	Sin correlativo	**Anexos 1 a 12-D**
	Sin correlativo	**Anexo 12-E Lineamientos mínimos para el Plan de gestión para la prevención del fraude.**
	Sin correlativo	**Anexo 12-F De la información que las instituciones deberán poner a disposición del Usuario o la Comisión derivado de Reclamaciones Monetarias.**
	Sin correlativo	**Anexos 13 a 73.**
1	Artículo 1.- Para efectos de las presentes disposiciones, se entenderá por: I. a XXXVII. . . .	Artículo 1.- . . . I. a XXXVII. . . . **XXXVII Bis. Conductas observables para la gestión del fraude: En singular o plural, las conductas Internas o Externas que, para efectos del cumplimiento de estas disposiciones, son aquellos comportamientos o conjunto de acciones realizadas por una persona o conjunto de personas en contra del Público Usuario con la finalidad de obtener un lucro indebido para sí o para tercera persona; así como aquellas acciones tendientes a:** **i. Suplantar o usurpar la identidad del Usuario.** **ii. Robar datos personales e información financiera del Usuario.** **iii. Suplantar la identidad de la propia institución.** **iv. Usar información privilegiada de los Usuarios por empleados de las Instituciones.** **v. Comprometer los Medios Electrónicos empleados por el Usuario con el objetivo de instalar un código malicioso capaz de alterar la realización de Operaciones Monetarias.** **vi. Alterar cheques y emitir cheques falsos.** **Para efecto de estas disposiciones y de las gestiones que las Instituciones deben realizar ante la probable presencia de dichas conductas, las Instituciones considerarán que son:** **a) Internas: Cuando las conductas sean realizadas por al menos un empleado, personal que ostente algún cargo, mandato o comisión o cualquier otra designación que las propias Instituciones hayan otorgado para la realización de sus Operaciones, en contra del Público Usuario, cuando las conductas sean contrarias a la normativa de las instituciones.** **b) Externas: Cuando las conductas sean realizadas exclusivamente por parte de uno o varios terceros, distintos a las personas señaladas en el inciso anterior, en contra de sus Usuarios.** XXXVIII. a CXV Bis. . . .

Vigente		Propuesta
		CXV Bis 1. Monto Transaccional del Usuario: Monto de referencia de las Operaciones Monetarias realizadas por Usuarios que sean personas físicas o personas físicas con actividad empresarial a través de los servicios de Banca por Internet, Banca Telefónica Voz a Voz, Banca Telefónica Audio Respuesta y Banca Móvil, definido por dicho Usuario o, en su defecto, estimado por la Institución de conformidad con el historial de las Operaciones Monetarias del usuario, utilizado para los fines específicos de las presentes disposiciones. **CXV Bis 2. NIF C-16: a la Norma de Información Financiera "Deterioro de Instrumentos financieros por cobrar" publicada por el Consejo Mexicano de Normas de Información Financiera, A.C., la cual converge con la Norma Internacional de Información Financiera 9 "Instrumentos financieros" emitida por el Consejo de Normas Internacionales de Contabilidad.** CXVI. a CXXXV. . . . **CXXXVI. Personas en Situación de Vulnerabilidad: Al grupo de personas que declaran de forma libre y voluntaria a las Instituciones, conforme a las presentes disposiciones, pertenecer de manera enunciativa, mas no limitativa, a las personas adultas mayores, personas con discapacidad, personas pertenecientes a alguna etnia, pueblo o comunidad indígena.** **CXXXVI Bis. Plan de gestión para la prevención del fraude: Es el documento que contiene el conjunto de lineamientos, metodologías de análisis y acciones mínimas que establecen la estrategia, procesos operativos y los proyectos de las Instituciones para llevar a cabo la identificación, medición, monitoreo, y atención a las Conductas observables para la gestión del fraude, así como a la prevención, detección, respuesta oportuna y resarcimiento monetario del daño al Público Usuario derivados de estas.** **CXXXVI Bis 1. Plan Director de Seguridad: al documento que establece la estrategia de seguridad de una Institución para procurar una correcta gestión de la seguridad de la información y evitar la materialización de Incidentes de Seguridad de la Información que podrían afectar de forma negativa a la Institución.** CXXXVII. a CXLVIII. . . . **CXLVIII Bis. Reclamación Monetaria: En singular o plural, a todas aquellas Operaciones Monetarias no reconocidas por el usuario y que han sido comunicadas a la Institución por cualquier canal o medio puesto a disposición del usuario.** CXLIX. a CXCVII. . . .

Vigente	Propuesta
Artículo 51 Bis 1.- Las Instituciones, en la realización de operaciones de retiros de efectivo y de transferencias de recursos que se realicen a cargo de Cuentas Bancarias Nivel 4, que se lleven a cabo de manera presencial, deberán observar lo siguiente:	Artículo 51 Bis 1.- . . .
I. Si son por montos iguales o menores al equivalente en moneda nacional a 1,500 UDIs, deberán requerir a los clientes que presenten como medio de identificación cualquiera de los documentos mencionados en la disposición 4ª, fracción I, inciso b), subinciso (i) de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito emitidas por la Secretaría o las que las sustituyan.	I. a III. . . .
II. Si son por montos mayores al equivalente en moneda nacional a 1,500 UDIs y menores al equivalente en moneda nacional a 2,800 UDIs, excepto que se trate de transferencias a otras cuentas de las que el cliente también sea el titular en la misma Institución, deberán solicitar la credencial para votar vigente expedida por el Instituto Nacional Electoral en el país o a través de las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, o el pasaporte mexicano vigente expedido por la Secretaría de Relaciones Exteriores en el país o a través de sus oficinas consulares en el extranjero, o la matrícula consular vigente expedida por las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, y realizar las correspondientes acciones de verificación previstas en el Artículo 51 Bis 4, fracciones I, II y V de las presentes disposiciones, según corresponda. En caso de que la persona que se presente no cuente con ningún documento de los señalados en el párrafo anterior, las Instituciones deberán requerir dos de las demás identificaciones mencionadas en la disposición 4ª, fracción I, inciso b), subinciso (i) de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito emitidas por la Secretaría o las que las sustituyan, y realizar las acciones de verificación previstas en el Artículo 51 Bis 4, fracción IV de estas disposiciones. Para el caso de personas físicas de nacionalidad extranjera, las Instituciones únicamente estarán obligadas a requerir el original del pasaporte o tarjeta pasaporte vigente, o los documentos migratorios expedidos por el Instituto Nacional de Migración que se encuentren vigentes, con los que acrediten su internación o condición de estancia en el país, o bien la tarjeta de acreditación que expida la Secretaría de Relaciones Exteriores a cuerpos diplomáticos o consulares, la cual deberá estar vigente, debiendo realizar las acciones de verificación previstas en el Artículo 51 Bis 4, fracción III de las presentes disposiciones. No serán aplicables las acciones de verificación respecto de la credencial para votar expedida por el Instituto Nacional Electoral en el país o a través de las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, el pasaporte mexicano vigente expedido por la Secretaría de	

Vigente	Propuesta
Relaciones Exteriores en el país o a través de sus oficinas consulares en el extranjero, o la matrícula consular vigente expedida por las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, cuando las Instituciones: a) Requieran al cliente que presente su Tarjeta Bancaria con Circuito Integrado correspondiente a su Cuenta Bancaria Nivel 4 o aquella emitida al amparo de un contrato de crédito en cuenta corriente con la propia Institución, e ingrese el NIP asociado a la tarjeta de que se trate en los dispositivos electrónicos que obtengan la información de la tarjeta a través del circuito integrado, siempre que en la entrega de la Tarjeta Bancaria con Circuito Integrado o al momento de que el cliente establezca su NIP por primera vez, se hubiere realizado la verificación de los datos de la credencial para votar vigente del cliente expedida por el Instituto Nacional Electoral en el país o a través de las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, del pasaporte mexicano vigente expedido por la Secretaría de Relaciones Exteriores en el país o a través de sus oficinas consulares en el extranjero, o de la matrícula consular vigente expedida por las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, conforme al Artículo 51 Bis 4, fracciones I, II o V de estas disposiciones, y b) Requieran al cliente cualquiera de las identificaciones mencionadas en la disposición 4ª, fracción I, inciso b), subinciso (i) de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito emitidas por la Secretaría o las que las sustituyan. III. Si son por montos iguales o mayores al equivalente en moneda nacional a 2,800 UDIs, excepto que se trate de transferencias a otras cuentas de las que el cliente también sea el titular en la misma Institución, deberán solicitar la credencial para votar vigente expedida por el Instituto Nacional Electoral en el país o a través de las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero, el pasaporte mexicano vigente expedido por la Secretaría de Relaciones Exteriores en el país o a través sus oficinas consulares en el extranjero, o la matrícula consular vigente expedida por las oficinas consulares de la Secretaría de Relaciones Exteriores en el extranjero y realizar las acciones de verificación previstas en el Artículo 51 Bis 4, fracciones I, II o V del de las presentes disposiciones, según corresponda. A falta de estos documentos de identificación, las Instituciones deberán: a) Requerir dos de las demás identificaciones mencionadas en la disposición 4ª, fracción I, inciso b), subinciso (i) de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito emitidas por la Secretaría o las que las sustituyan, y realizar las acciones de verificación previstas en el Artículo 51 Bis 4, fracción IV de estas disposiciones, o bien tratándose de personas de nacionalidad extranjera, su pasaporte o tarjeta pasaporte vigente, o los documentos	

Vigente	Propuesta
migratorios con los que acrediten su condición de estancia en el país expedidos por el Instituto Nacional de Migración, o bien la tarjeta de acreditación que expida la Secretaría de Relaciones Exteriores a cuerpos diplomáticos o consulares, los cuales deberán estar vigentes, debiendo realizar las acciones de verificación previstas en el Artículo 51 Bis 4, fracción III de las presentes disposiciones. b) Contar con la autorización del gerente o encargado de la Oficina Bancaria, o bien del funcionario facultado para ello, para proceder a la realización de la operación de que se trate. c) Conservar evidencia de la realización de las acciones descritas en los incisos anteriores. Cuando las Instituciones obtengan la aprobación de la Comisión para utilizar documentos de identificación distintos de los señalados en la disposición 4ª, fracción I, inciso b), subinciso (i) de las Disposiciones de carácter general a que se refiere el artículo 115 de la Ley de Instituciones de Crédito emitidas por la Secretaría o las que las sustituyan, podrán aceptarlos para la realización de operaciones en los términos y condiciones que la propia Comisión les haya señalado. Para efectos de lo previsto en este artículo, las Instituciones tomarán el valor de la UDI que corresponda al primer día de enero del año en curso. Las Instituciones podrán no realizar las acciones de verificación descritas en este artículo, cuando pacten con sus clientes en los respectivos contratos de Cuentas Bancarias Nivel 4, así como de contratos de apertura de crédito en cuenta corriente, que aquellas se obligan a asumir los riesgos y, por lo tanto, los costos de las operaciones que no sean reconocidas por sus clientes, obligándose además a que los montos de las ~~reclamaciones~~ de dichas operaciones serán abonadas a estos, a más tardar, cuarenta y ocho horas posteriores a la ~~reclamación~~ que haga el ~~cliente~~. Las Instituciones deberán avisar a la Comisión cuando decidan optar por lo previsto en el presente párrafo a más tardar a los diez días hábiles posteriores a dicha determinación, indicando las operaciones a las cuales les será aplicable.	. . . . . . Las Instituciones podrán no realizar las acciones de verificación descritas en este artículo, cuando pacten con sus clientes en los respectivos contratos de Cuentas Bancarias Nivel 4, así como en contratos de apertura de crédito en cuenta corriente, que aquellas se obligan a asumir los riesgos y, por lo tanto, los costos de las operaciones que no sean reconocidas por sus clientes, obligándose además a que los montos de las **Reclamaciones Monetarias** de dichas operaciones serán abonadas a estos, a más tardar, cuarenta y ocho horas posteriores a la **Reclamación Monetaria** que haga el **Usuario**. Las Instituciones deberán avisar a la Comisión cuando decidan optar por lo previsto en el presente párrafo a más tardar a los diez días hábiles posteriores a dicha determinación, indicando las operaciones a las cuales les será aplicable.
Artículo 142.- El Consejo, una vez aprobados los objetivos del Sistema de Control Interno y los lineamientos para su implementación, deberá en el ámbito de su competencia: I. Aprobar, al menos, hasta el segundo nivel jerárquico la estructura orgánica de la Institución, presentada por el director general, así como las eventuales modificaciones hasta ese nivel, habiendo escuchado el Consejo previamente la opinión del comité de recursos humanos y desarrollo institucional, en el caso de las instituciones de banca de desarrollo.	Artículo 142.- El Consejo, una vez aprobados los objetivos del Sistema de Control Interno y los lineamientos para su implementación deberá, en el ámbito de su competencia: I. y II. . . .

Vigente	Propuesta
II. Analizar mediante reportes elaborados al efecto por la Dirección General y el Comité de Auditoría, que el Sistema de Control Interno esté funcionando adecuadamente.	
III. Aprobar, en su caso, el código de conducta de la Institución, así como promover su divulgación y aplicación en coordinación con la Dirección General.	III. . . .
El código de conducta deberá contener normas acordes con la legislación vigente y demás disposiciones legales aplicables, con las sanas prácticas y usos bancarios. Adicionalmente, deberá incorporar lineamientos que detallen las obligaciones relativas a la confidencialidad de la información de la Institución, otras entidades o ~~su clientela~~.	El código de conducta deberá contener normas acordes con la legislación vigente y demás disposiciones legales aplicables, con las sanas prácticas y usos bancarios. Adicionalmente, deberá incorporar lineamientos que detallen las obligaciones relativas a la confidencialidad de la información de la Institución, otras entidades, o **sus usuarios, así como las Conductas observables para la gestión del fraude internas y sus sanciones correspondientes aplicadas por la Institución, especificando que estas últimas son independientes de aquellas impuestas por las autoridades judiciales correspondientes**.
Para el caso de las instituciones de banca de desarrollo, el código de ética de la Administración Pública Federal a que se refiere el Artículo 49 de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, hará las veces del código de conducta a que se refiere la presente fracción. Sólo en el caso de que dicho código de ética no resultare suficiente para regular los aspectos relacionados con la correcta operación del banco, conforme a los citados usos y prácticas, deberán elaborarse, utilizando como base dicho código, las normas de conducta que resulten convenientes para tal efecto.	. . .
IV. Designar, a propuesta del Comité de Auditoría al auditor interno de la Institución.”	IV. a VII. . . .
V. Revisar, por lo menos anualmente, los objetivos del Sistema de Control Interno y los lineamientos para su implementación, así como evaluar las funciones del Comité de Auditoría y de la Dirección General al respecto.	
VI. Determinar las acciones que correspondan a fin de subsanar las irregularidades que sean de su conocimiento e implementar las medidas correctivas correspondientes.	
VII. Aprobar el Plan de Continuidad de Negocio, así como sus modificaciones, que le presente el Comité de Auditoría.	
La totalidad de los asuntos que conforme al presente capítulo deben ser autorizados por el Consejo, serán presentados para tal efecto directamente por el Comité de Auditoría de las Instituciones.	. . .
Artículo 160.- El área de Auditoría Interna tendrá, entre otras, las funciones siguientes:	Artículo 160.- . . .

Vigente		Propuesta
	I. Evaluar con base en el programa anual de trabajo a que se refiere la fracción XI del presente artículo, mediante pruebas sustantivas, procedimentales y de cumplimiento, el funcionamiento operativo de las distintas unidades de la Institución, así como su apego al Sistema de Control Interno, incluyendo la observancia del código de conducta. II. Revisar que los mecanismos de control implementados, conlleven la adecuada protección de los activos de la Institución. (259) III. Verificar que la Infraestructura Tecnológica que soporta la operación y procesos internos de la Institución, incluyendo los sistemas contables, operacionales de cartera crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, que eviten su alteración y cumplan con los objetivos para los cuales fueron implementados o diseñados, en términos del Artículo 168 Bis 11 de estas disposiciones. Asimismo, vigilar periódicamente la Infraestructura Tecnológica a fin de identificar fallas potenciales y verificar que esta genere información suficiente, consistente y que fluya adecuadamente. En todo caso, deberá revisarse que la Institución cuente con planes de contingencia y medidas necesarias para evitar pérdidas de información, así como para, en su caso, su recuperación o rescate. IV. Cerciorarse de la calidad, suficiencia y oportunidad de la información financiera, así como que sea confiable para la adecuada toma de decisiones, y tal información se proporcione en forma correcta y oportuna a las autoridades competentes. V. Valorar la eficacia de los procedimientos de control interno para prevenir y detectar actos u operaciones con recursos, derechos o bienes, que procedan o representen el producto de un probable delito, así como comunicar los resultados a las instancias competentes dentro de la Institución. VI. Facilitar a las autoridades financieras competentes la información necesaria de que dispongan con motivo de sus funciones, a fin de que estas determinen la oportunidad y alcance de los procedimientos seguidos por la propia área de Auditoría Interna y puedan efectuar su análisis para los efectos que correspondan. VII. Verificar la estructura organizacional autorizada por el Consejo, en relación con la independencia de las distintas funciones que lo requieran, así como la efectiva segregación de funciones y ejercicio de facultades atribuidas a cada unidad de la Institución. Segundo párrafo.- Derogado. VIII. Verificar el procedimiento mediante el cual la unidad para la Administración Integral de Riesgos, dé seguimiento al cumplimiento de los	I. a XIV. . . .

Vigente		Propuesta
	límites en la asunción de riesgos al celebrar operaciones, así como a los niveles de tolerancia definidos, en el caso de los riesgos no discrecionales, acorde con las disposiciones legales aplicables, así como con las políticas establecidas por la Institución. IX. Proporcionar al Comité de Auditoría los elementos que le permitan cumplir con lo establecido en la fracción VI del Artículo 156 de las presentes disposiciones. X. Dar seguimiento a las deficiencias o desviaciones relevantes detectadas en relación con la operación de la Institución, con el fin de que sean subsanadas oportunamente, informando al respecto al Comité de Auditoría, para lo cual deberán elaborar un informe específico. XI. Presentar para aprobación del Comité de Auditoría, el programa anual de trabajo correspondiente a lo establecido por las presentes disposiciones. XII. Proporcionar, en su caso, al Comité de Auditoría los informes de gestión elaborados por el o los responsables de las Funciones de Contraloría Interna a que hace referencia el último párrafo del Artículo 167 de las presentes disposiciones. XIII. Valorar, al menos anualmente, la eficacia de los criterios, medidas y procedimientos para la verificación y actualización de los datos de identificación proporcionados por los clientes, conforme a lo previsto en los Artículos 51 Bis a 51 Bis 6, 51 Bis 8 y 51 Bis 10 de las presentes disposiciones, para lo cual deberá considerarse la información del registro a que se refiere el Artículo 51 Bis 12 de estas disposiciones, entre otros aspectos. Lo previsto en esta fracción podrá ser realizado por un tercero especializado Independiente. XIV. Evaluar con base en el programa anual de trabajo a que se refiere la fracción XI del presente artículo, el proceso de gestión de Incidentes de Seguridad de la Información al que alude el Artículo 168 Bis 14 de estas disposiciones. Penúltimo párrafo.- Derogado	**XV. Evaluar, al menos una vez cada dos años, y de manera alternada con la auditoría externa de conformidad con el último párrafo del Anexo 12-E de las presentes disposiciones, la efectividad y debilidades del Plan de gestión para la prevención del fraude, estableciendo recomendaciones para su mejora continua, tomando en cuenta los hechos identificados que representaron la comisión del delito de fraude, realizando el seguimiento de las acciones correctivas implementadas por las áreas o funciones responsables de atender dichas recomendaciones. Los hallazgos de cada auditoría formarán parte del anexo de la siguiente entrega del Plan de gestión para la prevención del fraude a la Comisión.** . . .

Vigente		Propuesta
	Las Instituciones, en la elaboración del programa anual a que se refiere la fracción XI anterior, deberán incorporar las observaciones que la Comisión hubiere formulado en ejercicio de sus facultades de inspección y vigilancia. Dicho programa, una vez aprobado, deberá entregarse al director general y presentarse a la Comisión a más tardar durante el primer trimestre del año de su aplicación.	. . .
	Artículo 164.- La Dirección General será la responsable de la debida implementación del Sistema de Control Interno**; lo anterior, en el ámbito de las funciones que correspondan a dicha dirección**. En la implementación deberá procurarse que su funcionamiento sea acorde con las estrategias y fines de la Institución, aplicando las medidas preventivas y correctivas necesarias para subsanar cualquier deficiencia detectada. Al efecto, a la Dirección General, en adición a lo señalado en estas disposiciones, le corresponderá llevar a cabo las actividades siguientes: I. Elaborar, revisar y, en su caso, actualizar o proponer la actualización, para someter a la consideración del Comité de Auditoría y posterior presentación al Consejo, por lo menos una vez al año o con frecuencia mayor de acuerdo a lo determinado al efecto por el propio Consejo, los objetivos y lineamientos del Sistema de Control Interno, el código de conducta de la Institución, así como el Plan de Continuidad de Negocio. II. Elaborar, revisar y, en su caso, actualizar o proponer la actualización de los manuales de la Institución, definiendo las áreas o personal responsable de las actividades respectivas. III. Identificar y evaluar los factores internos y externos que puedan afectar la consecución de las estrategias y fines que la propia Institución haya establecido. IV. Prever las medidas que se estimen necesarias para que las transacciones u operaciones de la Institución y el Sistema de Control Interno, sean congruentes entre sí, adoptando, entre otras, las medidas siguientes: a) Diseñar para aprobación del Consejo, la estructura organizacional de la Institución y sus modificaciones, observando para ello las políticas generales en la materia elaboradas por el director general y sujetas a la consideración del Comité de Auditoría, a que hace referencia la fracción I del Artículo 154 de las presentes disposiciones. Al efecto, dicha estructura deberá contemplar, cuando menos, los aspectos siguientes: 1. Las facultades generales o específicas otorgadas al personal, preservando una adecuada segregación y delegación de funciones, por línea de producto, tipo de operación, monto, nivel jerárquico,	Artículo 164.- La Dirección General**, en el ámbito de las funciones que le correspondan,** será la responsable de la debida implementación del Sistema de Control Interno. . . . . . . I. a III. . . . IV. . . . a) y b) . . .

Vigente	Propuesta
áreas, unidades de negocios o administrativas y comités, entre otros criterios de clasificación, así como sus restricciones. 2. La definición de áreas y niveles jerárquicos del personal de la Institución, asegurándose que sus responsabilidades sean acordes con sus facultades. 3. La delimitación de facultades entre el personal que autorice, ejecute, vigile, evalúe, registre y contabilice las transacciones, evitando su concentración en una misma persona y un posible conflicto de interés. 4. La descripción general de las funciones de Contraloría Interna a que se refiere el Artículo 166 de estas disposiciones, indicando la estructura y las características generales para el desarrollo de las mismas, así como las medidas establecidas para evitar se presenten conflictos de interés en su desempeño. Tratándose de instituciones de banca de desarrollo, el Consejo deberá oír, para el diseño de la estructura organizacional, la opinión del comité de recursos humanos y desarrollo institucional. b) Diseñar los canales de comunicación y de flujo de información entre las distintas unidades y áreas de la Institución, que tengan por objeto, al menos, lo siguiente: 1. Generar información financiera, económica, contable, jurídica y administrativa de la Institución, así como la relativa al seguimiento de los mercados financieros, relevante para la toma de decisiones. Dicha información deberá formularse de manera tal que facilite su uso y permanente actualización. 2. Proporcionar información en forma oportuna al personal que corresponda conforme a su nivel jerárquico y facultades. 3. Procesar, utilizar y conservar información relativa a cada transacción, con grado de detalle suficiente; utilizando mecanismos de seguridad que permitan su consulta sólo al personal autorizado y que limiten su modificación. 4. Proporcionar en tiempo y forma, información a las autoridades financieras competentes, conforme a lo establecido en las disposiciones legales aplicables. c) ~~Proveer~~ mecanismos para que las diversas actividades en la Institución se lleven a cabo por personal ~~que cuente~~ con la calidad técnica ~~y~~ experiencia necesaria~~s, así como con~~ honorabilidad, para lo cual deberá efectuar una evaluación **del personal, periódicamente**.	c) **Implementar y hacer del conocimiento del Consejo los** mecanismos para que las diversas actividades en la Institución se lleven a cabo**, únicamente** por el personal **definido previamente, y, en su caso, autorizado de conformidad con la estructura organizacional de cada Institución referida en el inciso a) de la presente fracción, para lo cual deberán contar** con la calidad

Vigente	Propuesta
	técnica**, la** experiencia necesaria y honorabilidad para lo cual deberá**n** efectuar una evaluación**, al menos una vez cada tres años, la cual debe estar documentada y disponible en todo momento para la Comisión por al menos cinco años**.
d) Proveer a todas las áreas de la Institución de los objetivos del Sistema de Control Interno y los lineamientos para su implementación y de los manuales de acuerdo a su ámbito de competencia, así como difundirlos oportunamente. e) Contar con programas de verificación del cumplimiento del Sistema de Control Interno, así como de las políticas y procedimientos en materia de control interno establecidos en los distintos manuales. f) Proteger la integridad y adecuado mantenimiento de la Infraestructura Tecnológica, incluidos los sistemas automatizados de procesamiento de datos y redes de telecomunicaciones a que se refiere el Artículo 52 de la Ley, así como la integridad, confidencialidad y disponibilidad de la información recibida, generada, procesada, almacenada y transmitida por estos, en términos del Artículo 168 Bis 11 de las presentes disposiciones. Adicionalmente, se deberán establecer procedimientos para que los clientes puedan reportar el robo o extravío de cualquiera de sus Factores de Autenticación, incluso cuando las Instituciones operen a través de sus comisionistas. g) Proponer medidas para evitar que terceros o personal de la Institución, utilicen a esta última para la comisión de actos ilícitos o irregularidades. h) Asegurar que se observen procedimientos, estructuras organizacionales y políticas de seguridad de la información acordes con la Institución. i) Verificar que en las ofertas públicas restringidas únicamente participen inversionistas institucionales o calificados para girar instrucciones a la mesa.	d) a i) . . .
V. Derogada.	V. a IX. . . .
VI. Implementar, en su caso, los mecanismos necesarios para dar cumplimiento a lo autorizado al amparo del Artículo 46 Bis de la Ley, sin poner en riesgo el valor económico de la Institución, la confidencialidad de la información y la continuidad de sus operaciones. VII. Cumplir las medidas correctivas y preventivas determinadas por el Consejo o el Comité de Auditoría, relacionadas con las deficiencias o desviaciones del Sistema de Control Interno, debiendo circunstanciar en un registro especial los actos y hechos que motiven dichas medidas.	

Vigente		Propuesta
	VIII. Dictar las medidas necesarias para que en el manejo de la información relativa a los clientes de la Institución, se observe lo relativo al secreto bancario y fiduciario. IX. Establecer los mecanismos necesarios para efectuar las acciones de verificación a que se refieren los Artículos 51 Bis a 51 Bis 6, 51 Bis 8 y 51 Bis 10 de estas disposiciones, así como para llevar el registro a que alude el Artículo 51 Bis 12 de las presentes disposiciones. Asimismo, el director general de las instituciones de banca múltiple, será el encargado de elaborar y presentar al Consejo para su aprobación, las políticas para el adecuado empleo y aprovechamiento de los recursos humanos y materiales del banco, en atención a lo dispuesto por el Artículo 21, tercer párrafo de la Ley. Tratándose de instituciones de banca de desarrollo, adicionalmente se escuchará la opinión del comité de recursos humanos y desarrollo institucional en el ámbito de su competencia, conforme a lo señalado en el Artículo 42, fracción XVIII de la Ley y en las presentes disposiciones. El director general informará por escrito, al menos anualmente, al Consejo y al Comité de Auditoría, sobre el desempeño de las actividades a que se refiere el presente Artículo, así como del funcionamiento del Sistema de Control Interno en su conjunto.	**X. Aprobar el Plan de gestión para la prevención del fraude. La persona titular de la dirección general deberá informar al Consejo el contenido de dicho plan, y contar con evidencia de su implementación desde su preparación y elaboración.** . . . . . .
		Artículo 164 Bis 1.- **El Plan de gestión para la prevención del fraude deberá contener los lineamientos, procesos, políticas y criterios para la prevención, detección y respuesta oportuna de las Conductas observables para la gestión del fraude. Asimismo, por cada proyecto que se defina dentro de dicho plan, se deberá señalar al menos: nombre del proyecto, objetivo y estrategias definidas para lograrlo, alcance, fechas de inicio y conclusión, plazos y periodicidad para su ejecución, áreas involucradas y una especificación detallada de las responsabilidades de cada área involucrada en cada proyecto definido, inversión proyectada, el detalle de las acciones y actividades realizadas y por realizar, los recursos técnicos, materiales y humanos empleados; verificando que en la elaboración del plan al que se refiere este artículo se dé cumplimiento a los lineamientos mínimos descritos en el Anexo 12-E de las presentes disposiciones.** **La persona titular de la dirección general podrá designar en algún funcionario de los dos niveles jerárquicos inferiores a éste, y que no pertenezcan al área de negocios o auditoria, o bien al área responsable**

Vigente		Propuesta
		de prevención de fraudes, la facultad de elaborar el Plan de gestión para la prevención del fraude, documentando dicha designación. El Plan de gestión para la prevención del fraude se ejecutará por una estructura administrativa específica. **El acta o la certificación emitida por el secretario o prosecretario en los que conste la presentación del Plan de gestión para la prevención del fraude al Consejo, para su conocimiento, deberá incluirse como anexo del documento que se envíe a la Comisión. Una vez hecho del conocimiento el Plan de gestión para la prevención del fraude al Consejo, la Institución deberá remitirlo a la vicepresidencia de la Comisión encargada de su supervisión, a más tardar, el último día hábil de enero de cada año. La Comisión podrá solicitar ajustes al Plan de gestión para la prevención del fraude derivado de la revisión referida en el presente párrafo. Sin perjuicio de lo anterior, las Instituciones deberán ejecutar el plan desde su aprobación por el director general.** **Las Instituciones deberán contar con evidencia documentada de la implementación de cada proyecto que conforma el Plan de gestión para la prevención del fraude, la cual debe ser conservada y estar disponible para la Comisión por un periodo de al menos cinco años.**
	Artículo 166.- Las Instituciones deberán desarrollar permanentemente las funciones de Contraloría Interna que consistirán, por lo menos, en el desempeño cotidiano y permanente de las actividades relacionadas con el diseño, establecimiento y actualización de medidas y controles que: I. Propicien el cumplimiento de la normatividad interna y externa aplicable a la Institución en la realización de sus operaciones. II. Permitan que la concertación, documentación, registro y liquidación diaria de operaciones, se realicen conforme a las políticas y procedimientos establecidos en los manuales de la Institución y en apego a las disposiciones legales aplicables. III. Propicien el correcto funcionamiento de la Infraestructura Tecnológica conforme a las medidas de seguridad a que se refiere el Artículo 168 Bis 11 de las presentes disposiciones, auxiliándose para tal efecto del oficial en jefe de seguridad de la información a que se refiere el Artículo 168 Bis 14 de estas disposiciones, así como la elaboración de información completa, correcta, precisa, íntegra, confiable y oportuna, incluyendo aquella que deba proporcionarse a las autoridades competentes, y que coadyuve a la adecuada toma de decisiones. IV. Tengan como finalidad el verificar que los procesos de conciliación entre los sistemas de operación y contables sean adecuados. V. Derogada.	Artículo 166.- . . . I. a VI. . . .

Vigente	Propuesta
VI. Permitan verificar que las casas de bolsa con las que operen cumplen con el deber de mejor ejecución, en términos de las Disposiciones de carácter general aplicables a las casas de bolsa, publicadas en el Diario Oficial de la Federación el 6 de septiembre de 2004 y sus respectivas modificaciones.	
Sin correlativo	**VII. Verificar y revisar que los aspectos básicos de dictaminación de Reclamaciones Monetarias, y alertamiento por posibles eventos de Conductas observables para la gestión del fraude, se realicen con un nivel mínimo de calidad, lo que será determinado en los manuales, políticas y procedimientos internos de la Institución, por parte de las áreas responsables involucradas en cada proceso de dictaminación, así como dar cumplimiento a lo que se establece en dicha materia en los Anexos 12-E y 12-F de las presentes disposiciones.** **VIII. Dar seguimiento y propiciar el cumplimiento de los proyectos contenidos en el Plan de gestión para la prevención del fraude, debiendo contar con evidencia documentada la cual debe ser conservada y estar disponible para la Comisión por un periodo de al menos cinco años.**
Último párrafo.- Derogado	. . .
Artículo 168 Bis 11.- El director general de la Institución será responsable de la implementación del Sistema de Control Interno en materia de seguridad de la información que procure su confidencialidad, integridad y disponibilidad. El marco de gestión a que se refiere este párrafo, deberá asegurar que la Infraestructura Tecnológica, propia o provista por terceros, se apegue a los requerimientos siguientes: I.Que cada uno de sus componentes realice las funciones para las que fue diseñado, desarrollado o adquirido. II. Que sus procesos, funcionalidades y configuraciones, incluyendo su metodología de desarrollo o adquisición, así como el registro de sus cambios, actualizaciones y el inventario detallado de cada componente de la Infraestructura Tecnológica, estén documentados. III. Que se hayan considerado aspectos de seguridad de la información en la definición de proyectos para adquirir o desarrollar cada uno de sus componentes, debiendo incluirlos durante las diversas etapas del ciclo de vida. Este comprenderá la elaboración de requerimientos, diseño, desarrollo o adquisición, pruebas de implementación, pruebas de aceptación por parte de los Usuarios de la Infraestructura Tecnológica, procesos de liberación incluyendo pruebas de vulnerabilidades y análisis de código previos a su puesta en producción, pruebas periódicas, gestión de cambios, reemplazo y destrucción de información.	Artículo 168 Bis 11.- La persona titular de la Dirección General de la Institución será responsable de la implementación del Sistema de Control Interno en materia de seguridad de la información que procure su confidencialidad, integridad y disponibilidad. El marco de gestión a que se refiere este artículo deberá asegurar que la Infraestructura Tecnológica, propia o provista por terceros, se apegue a los requerimientos siguientes: I a XV. . . .

Vigente		Propuesta
	Tratándose de componentes de comunicaciones y de cómputo, los aspectos de seguridad deberán incluir, al menos, lo siguiente: a) Segregación lógica, o lógica y física de las diferentes redes en distintos dominios y sub redes, dependiendo de la función que desarrollen o el tipo de datos que se transmitan, incluyendo segregación de los ambientes productivos de los de desarrollo y pruebas, así como componentes de seguridad perimetral y de redes que aseguren que solamente el tráfico autorizado es permitido. En particular, en aquellos segmentos con enlaces al exterior, tales como Internet, proveedores, autoridades, otras redes de la Institución o matriz y otros terceros, todo ello referido a servicios críticos, ya sean sistemas de pagos, equipos de cifrado, autorizadores de operaciones, entre otros, considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (DMZ por sus siglas en inglés). b) Configuración segura de acuerdo con el tipo de componente, considerando al menos, puertos y servicios, permisos otorgados bajo el principio de mínimo privilegio, uso de medios extraíbles de almacenamiento, listas de acceso, actualizaciones del fabricante y reconfiguración de parámetros de fábrica. Se entenderá como principio de mínimo privilegio a la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo de las funciones propias de cada Usuario de la Infraestructura Tecnológica. IV. Que cada uno de sus componentes sea probado antes de ser implementado o modificado, utilizando mecanismos de control de calidad que eviten que en dichas pruebas se utilicen datos reales del ambiente de producción, se revele información confidencial o de seguridad, o se introduzca cualquier funcionalidad no reconocida para dicho componente. V. Que cuente con las licencias o autorizaciones de uso, en su caso. VI. Que cuente con medidas de seguridad para su protección, así como para el acceso y uso de la información que sea recibida, generada, transmitida, almacenada y procesada en la propia Infraestructura Tecnológica, contando al menos con lo siguiente: a) Mecanismos de identificación y Autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio. Para lo anterior, se deberán incluir controles pertinentes para aquellos Usuarios de la Infraestructura Tecnológica con mayores privilegios, derivados de sus funciones, tales como, la de administración de bases de datos y de sistemas operativos. Asimismo, se deberán prever políticas y procedimientos para las autorizaciones de accesos por excepción, tales como usuarios de ambientes de desarrollo con acceso a ambientes de producción y con acceso por eventos	

Vigente		Propuesta
	de contingencia, entre otros. Dichas políticas y procedimientos deberán ser aprobados por el oficial en jefe de seguridad de la información. b) Cifrado de la información conforme al grado de sensibilidad o clasificación que la Institución determine y establezca en sus políticas, cuando dicha información sea transmitida, intercambiada y comunicada entre componentes, o almacenada en la Infraestructura Tecnológica o se acceda de forma remota. c) Claves de acceso con características de composición que eviten accesos no autorizados, considerando procesos que aseguren que solo el Usuario de la Infraestructura Tecnológica sea quien las conozca, así como medidas de seguridad, cifrado en su almacenamiento y mecanismos para cambiar las claves de acceso cada 90 días o menos. En el caso de los Usuarios de la Infraestructura Tecnológica asignados a aplicativos o componentes para autenticarse entre ellos, el cambio a que alude este inciso deberá realizarse al menos una vez al año. En el evento de que algún Usuario de la Infraestructura Tecnológica tenga conocimiento de las claves de acceso y deje de prestar sus servicios a la Institución, estas deberán modificarse de manera inmediata. d) Controles para terminar automáticamente sesiones no atendidas, así como para evitar sesiones simultáneas no permitidas con un mismo identificador de Usuario de la Infraestructura Tecnológica. e) Mecanismos de seguridad, tanto de acceso físico, como de controles ambientales y de energía eléctrica, que protejan la Infraestructura Tecnológica y permitan la operación conforme a las especificaciones del proveedor, fabricante o desarrollador. f) Medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la Infraestructura Tecnológica, considerando, al menos lo siguiente: 1. La veracidad e integridad de la información. 2. La Autenticación entre componentes de la Infraestructura Tecnológica, que aseguren que se ejecutan solo las solicitudes de servicio legítimas desde su origen y hasta su ejecución y registro. 3. Los protocolos de mensajería, comunicaciones y cifrado, los cuales deben procurar la integridad y confidencialidad de la información. 4. La identificación de transacciones atípicas, previendo que las aplicaciones cuenten con medidas de alerta automática para su atención de las áreas operativas correspondientes. 5. La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados al proceso de ejecución de transacciones. Las medidas a que alude este inciso deberán	

Vigente		Propuesta
	establecerse acorde con el grado de riesgo que las Instituciones definan para cada tipo de transacción. VII. Que cuente con mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación, en concordancia con lo dispuesto en el Artículo 164 Bis de las presentes disposiciones. VIII. Que mantenga registros de auditoría íntegros, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por los Usuarios de la Infraestructura Tecnológica, lo anterior, con independencia del nivel de privilegios con el que estos cuenten para el acceso, generación o modificación de la información que reciban, generen, almacenen o transmitan en cada componente de la Infraestructura Tecnológica, incluyendo actividad de procesos automatizados, así como los procedimientos para la revisión periódica de dichos registros. Las Instituciones deberán conservar los registros de auditoría a que se refiere esta fracción por un periodo de tres años cuando dichos registros se refieran a actividades realizadas sobre componentes que procesen o almacenen información considerada como crítica de conformidad con la clasificación señalada en el Artículo 86, fracción III, inciso b), numeral 3 de las presentes disposiciones. En caso contrario, el periodo de conservación de los registros será mínimo de seis meses. IX. Que para la atención de los Incidentes de Seguridad de la Información se cuente con procesos de gestión que aseguren la detección, clasificación, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, reporte a niveles jerárquicos competentes, solución, seguimiento y comunicación a autoridades, clientes y contrapartes de dichos incidentes. (260) Para la detección y respuesta de Incidentes de Seguridad de la Información a que hace referencia el párrafo anterior, el director general deberá designar un equipo que incorpore a personal de las diferentes áreas de la Institución para participar en cada actividad del proceso de gestión antes señalado del que, en todo caso, deberá formar parte el oficial en jefe de seguridad de la información de conformidad con la fracción VII del Artículo 168 Bis 14 de estas disposiciones. En caso de que se detecte la existencia de vulnerabilidades y deficiencias en la Infraestructura Tecnológica, deberán tomarse las acciones correctivas o controles compensatorios de acuerdo al nivel de riesgo de que se trate, previniendo que los Usuarios de la Infraestructura Tecnológica o la Institución puedan verse afectados. X. Que sea sometida a la realización de ejercicios de planeación y revisión anuales que permitan medir su capacidad para soportar su operación, garantizando que se atiendan oportunamente las necesidades de incremento de capacidad detectadas como resultado de dichos ejercicios.	

Vigente		Propuesta
	Asimismo, la Institución deberá evaluar la obsolescencia de los componentes de la Infraestructura Tecnológica, debiendo contar con un plan para su actualización. XI. Que cuente con controles automatizados o, en ausencia de estos, que se realicen controles compensatorios, tales como doble verificación, que previo o posteriormente a la realización de la operación de que se trate, minimicen el riesgo de eliminación, exposición, alteración o modificación de información, que se deriven de procesos manuales o semi-automatizados realizados por el personal de la Institución, con el objetivo de prevenir errores, omisiones, sustracción o manipulación de información. XII. Que tenga controles que permitan detectar la alteración o falsificación de libros, registros y documentos digitales relativos a las operaciones activas, pasivas y de servicios de la Institución. XIII. Que cuente con procesos para medir y asegurar los niveles de disponibilidad y tiempos de respuesta, que garanticen la ejecución de las operaciones y servicios realizados; lo anterior incluyendo los supuestos en que las Instituciones contraten la prestación de servicios por parte de proveedores externos para el procesamiento y almacenamiento de información. XIV. Que cuente con dispositivos o mecanismos automatizados para detectar y prevenir eventos e Incidentes de Seguridad de la Información, así como para evitar conexiones y flujos de datos entrantes o salientes no autorizados y fuga de información, considerando entre otros, medios de almacenamiento removibles. Las Instituciones deberán correlacionar los datos obtenidos de los dispositivos o mecanismos automatizados a que alude el párrafo anterior con los datos de otras fuentes, tales como registros de actividad o de Incidentes de Seguridad de la Información. Adicionalmente, a lo señalado en el párrafo anterior, las Instituciones deberán mantener controles que eviten la filtración de la información correspondiente a la configuración de la Infraestructura Tecnológica, tales como direcciones IP, reglas de los cortafuegos, así como versiones de hardware y software. XV. Que para la prestación de servicios de tecnologías de información a los Usuarios de la Infraestructura Tecnológica, en sus fases de estrategia, diseño, transición, operación y mejora continua se proteja la integridad de la Infraestructura Tecnológica así como la integridad, confidencialidad y disponibilidad de la información recibida, generada, procesada, almacenada y transmitida por esta. **Sin correlativo**.	**XVI. Definir en los respectivos manuales de políticas y procedimientos, los roles y responsabilidades del personal de la Infraestructura Tecnológica en materia de seguridad de la información de la Institución.**

Vigente		Propuesta
	El director general será responsable de documentar en políticas y procedimientos lo previsto en este artículo.	. . .
	Artículo 168 Bis 12.- El director general de la Institución será responsable del cumplimiento de las siguientes obligaciones en relación con la Infraestructura Tecnológica: I. Aprobar el Plan Director de Seguridad, el cual debe estar alineado con la estrategia de negocio de la Institución, así como definir y priorizar los proyectos en materia de seguridad de la información, con el objetivo de reducir la exposición a los riesgos tecnológicos y la materialización de Incidentes de Seguridad de la Información hasta niveles aceptables en los términos que defina el Consejo, a partir de un análisis de la situación actual. Para la aprobación de dicho plan, el director general deberá verificar que contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes y podrá contemplar los controles requeridos conforme a las disposiciones aplicables. El director general deberá informar al Consejo el contenido del Plan Director de Seguridad, y contar con evidencia de su implementación. II. Llevar a cabo revisiones de seguridad, enfocadas a verificar la suficiencia en los controles aplicables a la Infraestructura Tecnológica. Estas revisiones deberán comprender al menos lo siguiente: a) Mecanismos de Autenticación de los Usuarios de la Infraestructura Tecnológica. b) Configuración y controles de acceso a la Infraestructura Tecnológica. c) Actualizaciones requeridas para los sistemas operativos y software en general, previo a su implementación y una vez implementados. d) Identificación de posibles modificaciones no autorizadas al software original. e) Dispositivos, redes de comunicaciones, sistemas y procesos asociados a los Medios Electrónicos y canales de atención al público, a fin de verificar que no existan vulnerabilidades o se cuente con herramientas o procedimientos que permitan conocer las credenciales de Autenticación de los Usuarios de la Infraestructura Tecnológica, así como cualquier información que de manera directa o indirecta pudiera dar acceso a la Infraestructura Tecnológica en nombre del Usuario de la Infraestructura Tecnológica. Las revisiones a que se refiere esta fracción deberán realizarse, por lo menos, una vez al año o antes si se presentan cambios significativos en la Infraestructura Tecnológica. Para determinar si se trata de un cambio	Artículo 168 Bis 12.- . . . I. a VII. . . .

Vigente		Propuesta
	significativo deberá obtenerse, al efecto, la opinión del oficial en jefe de seguridad de la información. III. Elaborar un calendario anual para la realización de pruebas de escaneo de vulnerabilidades de los componentes de la Infraestructura Tecnológica que almacenen, procesen o transmitan información, priorizándolos de acuerdo al resultado del ejercicio de clasificación de información a que se refiere el artículo 86, fracción III, inciso b), numeral 3. El calendario deberá prever la revisión trimestral de algunos de los componentes de la Infraestructura Tecnológica de manera que a la conclusión del año se hayan revisado la totalidad de los componentes que almacenen, procesen o transmitan información catalogada como crítica, además de los que la Institución considere necesarios. El director general será responsable de vigilar que dichas pruebas se lleven a cabo ya sea a través de la propia Institución o de un tercero contratado al efecto. Adicionalmente, cuando se incorporen nuevos componentes de la Infraestructura Tecnológica, el director general será responsable de vigilar que se realice la prueba de escaneo de vulnerabilidades, previo a su puesta en producción. IV. 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 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. Tal revisión deberá incluir la verificación de la integridad de los componentes de hardware y software que permitan detectar alteraciones a estos. Dichas pruebas deberán considerar, al menos lo siguiente: a) Su alcance y metodología, debiendo ser validados por el oficial en jefe de seguridad de la información. b) Ser realizadas al menos dos al año sobre sistemas y aplicativos distintos, o bien, cuando lo ordene la Comisión habiendo detectado factores que puedan afectar los sistemas y aplicativos o la información recibida, generada, procesada, almacenada o transmitida en estos. En este último caso, la Comisión determinará el alcance de las pruebas, así como los plazos para realizarlas. Se podrán efectuar pruebas adicionales a juicio del director general, con opinión del oficial en jefe de seguridad de la información, cuando existan cambios significativos en los sistemas y aplicativos, o realizarlas sobre sistemas y aplicativos previamente revisados cuando existan vulnerabilidades críticas.	

Vigente	Propuesta
El director general de la Institución deberá enviar a la Comisión, dentro de los 20 días hábiles de haber sido finalizadas las pruebas, un informe con las conclusiones de estas. En el envío que se realice, se deberá procurar el uso de mecanismos que impidan el acceso al contenido de este informe por personal no autorizado. V. Clasificar las vulnerabilidades detectadas de acuerdo con la metodología aprobada por el comité de riesgos. VI. Elaborar planes de remediación respecto de los hallazgos de las revisiones y pruebas a que se refieren las fracciones II, III y IV anteriores, considerando la clasificación de la fracción V del presente artículo, así como implementar mecanismos de defensa que prevengan el acceso y uso no autorizado de la Infraestructura Tecnológica. Los planes de remediación a que se refiere el párrafo anterior deberán ser validados por el oficial en jefe de seguridad de la información. Asimismo, dichos planes deberán contener, al menos, la indicación del personal responsable de su implementación y ejecución, así como los plazos para esta, detalle de las actividades realizadas y por realizar, al igual que los recursos técnicos, materiales y humanos empleados. Los referidos planes de remediación deben ser elaborados una vez que se identifiquen las vulnerabilidades y ser enviados a la Comisión en un plazo de 10 días hábiles. En adición a lo señalado en el párrafo anterior, en caso de tratarse proyectos de corto, mediano o largo plazo en los planes de remediación, deberán incorporarse al Plan Director de Seguridad. VII. Implementar procesos de seguimiento al cumplimiento de los planes de remediación referidos, lo que deberá ser verificado por el oficial en jefe de seguridad de la información.	
VIII. Implementar los programas anuales de capacitación a los que se refiere ~~la fracción V del~~ Artículo 69 de estas disposiciones, 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, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de la Infraestructura Tecnológica tengan al respecto.	VIII. Implementar **y evaluar mediante auditoría interna,** los programas anuales de capacitación a los que se refiere **el** Artículo 69**, fracción V** de estas disposiciones, así como los de concientización en materia de seguridad de la información, dirigidos a todo el personal y **al Usuario** incluyendo, en su caso, a terceros que le presten servicios **relacionados con los medios a través de los cuales se pueden cometer Conductas observables para la gestión del fraude**, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de la Infraestructura Tecnológica tengan al respecto.
IX. Realizar, de manera proactiva e iterativa, la búsqueda de alertas de fraude, así como de amenazas, tales como campañas de correos fraudulentos, sitios de Internet falsos, divulgación de bases de datos con información del Público Usuario, alteración de cajeros automáticos o terminales punto de venta y	IX. y X. . . .

Vigente		Propuesta
	suplantación de identidad, entre otros, que pudieran afectar a la seguridad de la información del Público Usuario, al igual que acciones para su protección considerando, al menos, lo siguiente: a) La continua investigación, recopilación, procesamiento y análisis de información que provenga de cualquier fuente relacionada con los productos y servicios que ofrezca la Institución, que pueda constituir indicios o evidencias de que se han evadido los controles de seguridad, representando una amenaza para la información o recursos del Público Usuario. Los indicios o evidencias a que se refiere el párrafo anterior, se mantendrán en un registro el cual deberá contenerse en la base de datos a que se refiere el primer párrafo del Artículo 168 Bis 17 de estas disposiciones. b) La implementación de procesos proactivos para proteger la información o recursos de los clientes cuando se presenten los indicios o evidencias señaladas en el inciso a) anterior, tales como bloqueo y reposición de medios de disposición, cambio de datos de autenticación y notificaciones, entre otros. c) Que cuente con procedimientos de comunicación y recomendaciones de seguridad con los clientes afectados, para informarles sobre los procesos de remediación que la Institución llevará a cabo y, en su caso, las medidas que el propio cliente debe adoptar, tales como cambio de contraseñas, verificación de saldos y movimientos, instalación de antivirus, instalación de software de detección de programas maliciosos, revisión de dispositivos y reinstalación de aplicaciones, entre otros. Los términos y condiciones para realizar los procesos mediante los cuales se realicen las actividades señaladas en la presente fracción, deberán documentarse en los respectivos manuales de políticas y procedimientos, en los cuales deberá preverse que la Institución mantendrá evidencia de la realización de dichas actividades. X. Implementar controles que permitan a la Institución 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, que garanticen que dicha información e Infraestructura Tecnológica no sean alterados o causen una afectación a la Institución o a los recursos de sus clientes. Dichos controles deberán implementarse desde la contratación respectiva y hasta su terminación.	
	Sin correlativo.	**Artículo 171 Bis 1.- Las Instituciones deberán contar con procesos que evalúen la efectividad de la resolución de Reclamaciones Monetarias. Asimismo, deberán garantizar la transparencia en dichos procesos para lo cual deberán ajustarse a lo señalado en el Anexo 12-F de las presentes disposiciones.**

Vigente	Propuesta
Artículo 207.- Las Instituciones deberán proporcionar a la Comisión, con la periodicidad establecida en los artículos siguientes, la información que se adjunta a las presentes disposiciones como Anexo 36, la cual se identifica con las series y reportes que a continuación se relacionan: Serie R01 Catálogo mínimo A-0111 Catálogo mínimo Serie R03 Inversiones en valores E-0304 Asignaciones E-0305 Órdenes Serie R04 Cartera de crédito Situación financiera A-0411 Cartera por tipo de crédito, saldo promedio, intereses y comisiones A-0417 Calificación de la cartera de crédito y estimación preventiva para riesgos crediticios A-0419 Movimientos en la estimación preventiva para riesgos crediticios A-0420 Movimientos en cartera con riesgo de crédito etapa 3 A-0424 Movimientos en cartera con riesgo de crédito etapas 1 y 2 Cartera comercial Información detallada (Metodología de calificación de cartera Anexos 18 a 22) C-0430 Alta de créditos comerciales a cargo de entidades federativas y municipios, entidades financieras, personas morales y físicas con actividad empresarial, gobierno federal, organismos descentralizados federales, estatales y municipales, empresas productivas del estado y créditos otorgados a proyectos de inversión o activos con fuente de pago propia C-0431 Seguimiento de créditos comerciales a cargo de entidades federativas y municipios, entidades financieras, personas morales y físicas con actividad empresarial, gobierno federal, organismos descentralizados federales, estatales y municipales, empresas productivas del estado y créditos otorgados a proyectos de inversión o activos con fuente de pago propia C-0432 Baja de créditos comerciales a cargo de entidades federativas y municipios, entidades financieras, personas morales y físicas con actividad empresarial, gobierno federal organismos descentralizados federales, estatales y municipales, empresas productivas	Artículo 207.- . . . Serie R01 Catálogo mínimo a Serie R26 Información por comisionistas

Vigente		Propuesta
	C-0433 Reservas de créditos comerciales a cargo de entidades federativas y municipios, entidades financieras, personas morales y físicas con actividad empresarial, gobierno federal, organismos descentralizados federales, estatales y municipales y empresas productivas del Estado C-0434 Severidad de la Pérdida de créditos comerciales a cargo de entidades federativas y municipios, entidades financieras, personas morales y físicas con actividad empresarial, gobierno federal, organismos descentralizados federales, estatales y municipales y empresas productivas del Estado C-0435 Probabilidad de Incumplimiento de créditos comerciales a cargo de entidades federativas y municipios C-0436 Probabilidad de Incumplimiento de créditos comerciales a cargo de entidades financieras C-0437 Probabilidad de Incumplimiento de créditos comerciales a cargo de personas morales y físicas con actividad empresarial, del gobierno federal, organismos descentralizados federales, estatales y municipales y empresas productivas del estado con Ventas Netas o Ingresos Netos anuales menores a 14 millones de UDIS, distintas a entidades federativas, municipios y entidades financieras C-0438 Probabilidad de Incumplimiento de créditos comerciales a cargo de personas morales y físicas con actividad empresarial, del gobierno federal, organismos descentralizados federales, estatales y municipales y empresas productivas del estado con Ventas Netas o Ingresos Netos anuales mayores o iguales a 14 millones de UDIS, distintas a entidades federativas, municipios y entidades financieras C-0439 Método de calificación y provisionamiento aplicable a los créditos comerciales para proyectos de inversión o activos con fuente de pago propia (Anexo 19) C-0440 Garantías de créditos comerciales (328)3 Información detallada de garantías de segundo piso C-0447 Seguimiento de garantías Cartera a la vivienda H-0491 Altas de créditos a la vivienda H-0492 Seguimiento de créditos a la vivienda H-0493 Baja de créditos a la vivienda H-0494 Reservas de créditos a la vivienda Serie R06 Bienes adjudicados	

Vigente		Propuesta
	Serie R08 Captación A-0811 Captación tradicional y préstamos interbancarios y de otros organismos A-0815 Préstamos interbancarios y de otros organismos, estratificados por plazos al vencimiento A-0816 Depósitos de exigibilidad inmediata y préstamos interbancarios y de otros organismos, estratificados por montos A-0819 Captación integral estratificada por montos Serie R10 Reclasificaciones A-1011 Reclasificaciones en el estado de situación financiera A-1012 Reclasificaciones en el estado de resultado integral Serie R12 Consolidación A-1219 Consolidación del estado de situación financiera de la institución de crédito con sus subsidiarias A-1220 Consolidación del estado de resultado integral de la institución de crédito con sus subsidiarias B-1230 Desagregado de inversiones permanentes en acciones Serie R13 Estados financieros A-1311 Estado de cambios en el capital contable A-1316 Estado de flujos de efectivo B-1321 Estado de situación financiera B-1322 Estado de resultado integral Serie R14 Información cualitativa A-1411 Integración accionaria A-1412 Funcionarios, empleados, jubilados, personal por honorarios y sucursales Serie R15 Operaciones por servicio B-1522 Usuarios no clientes de los medios electrónicos de la institución B-1523 Operaciones de clientes por servicios de Banca Electrónica	

Vigente	Propuesta
B-1524 Clientes por servicio de Banca Electrónica Serie R16 Riesgos A-1611 Brechas de repreciación A-1612 Brechas de vencimiento B-1621 Portafolio global de juicios Serie R24 Información operativa B-2421 Información de Operaciones referentes a productos de captación B-2422 Información de Operaciones referentes a sucursales, tarjetas de crédito y otras variables operativas B-2423 Titulares garantizados por el IPAB C-2431 Información de Operaciones con partes relacionadas D-2441 Información general sobre el uso de servicios financieros D-2442 Información de frecuencia de uso de servicios financieros D-2443 Información de ubicación de los puntos de transacciones de servicios financieros E-2450 Número de clientes de cada producto o servicio por tipo de persona E-2451 Número de Operaciones de cada producto o servicio por tipo de moneda E-2452 Número de Operaciones de cada producto o servicio por zona geográfica Serie R26 Información por comisionistas A-2610 Altas y bajas de Administradores de Comisionistas A-2611 Altas y bajas de comisionistas B-2612 Altas y bajas de módulos o establecimientos de comisionistas C-2613 Seguimiento de Operaciones de comisionistas Serie R27 Reclamaciones	

Vigente	Propuesta
A-2701 Reclamaciones Serie R28 Información de Riesgo Operacional A-2811 Eventos de pérdida por Riesgo Operacional A-2812 Estimación de niveles de Riesgo Operacional A-2813 Actualización de eventos de pérdida por Riesgo Operacional A-2815 Asignación del Método del Indicador de Negocio para Riesgo Operacional Serie R29 Aseguramientos, transferencias y desbloqueos de cuentas A-2911 Aseguramientos, transferencias y desbloqueos de cuentas Serie R32 Conciliaciones A-3211 Conciliación contable fiscal Serie 34 Razón de Apalancamiento A-3401 Cálculo de la Razón de Apalancamiento Serie R35 Grandes Exposiciones A-3511 Operaciones de Grandes Exposiciones Serie R36 Derogada A-3601 Derogado	Serie R27 Reclamaciones **Monetarias** A-2701 Reclamaciones **Monetarias** Serie R28 a Serie R36 . . .
Las Instituciones requerirán de la previa autorización de la Comisión para la apertura de nuevos conceptos o niveles que no se encuentren contemplados en las series que correspondan exclusivamente para el envío de información de las nuevas operaciones que les sean autorizadas al efecto por la Secretaría, en términos de la legislación relativa, para lo cual solicitarán la referida autorización mediante escrito libre dentro de los quince días hábiles siguientes a la autorización hecha por la Secretaría.	. . .
Asimismo, en caso de que por cambios en la normativa aplicable se requiera establecer conceptos o niveles adicionales a los previstos en las presentes disposiciones, la Comisión hará del conocimiento de las Instituciones la apertura de los nuevos conceptos o niveles respectivos. En los dos casos previstos en el párrafo anterior la Comisión, a través del SITI, notificará a la Institución el mecanismo de registro y envío de la información correspondiente.	. . .

Vigente	Propuesta
Artículo 208.- Las Instituciones presentarán la información a que se refiere el Artículo 207, con la periodicidad que a continuación se indica:	Artículo 208.- . . .
I. Diariamente, la información relativa a la serie R03, de la siguiente forma:	I. . . .
a) Por lo que se refiere al reporte E-0304, en la fecha de liquidación de las operaciones con valores efectuadas en los sistemas electrónicos de negociación de las Bolsas.	
b) Por lo que se refiere al reporte E-0305, las Órdenes derivadas de las instrucciones que reciban de sus clientes en el mismo día en que ingresaron dichas Órdenes al Sistema de Recepción y Asignación de las Instituciones.	
II. Mensualmente:	II. . . .
a) La información relativa a la serie R29 deberá proporcionarse dentro de los 10 días del mes inmediato siguiente al de su fecha.	a) a e) . . .
b) La información relativa a la serie R04, exclusivamente por lo que se refiere a los reportes C0430, C-0431, C-0432, H-0491, H-0492, H-0493 y H-0494 deberá proporcionarse dentro de los 12 días del mes inmediato siguiente al de su fecha.	
c) La información relativa al reporte A-2815 de la serie R28, deberá proporcionarse, a más tardar, dentro de los 15 días hábiles siguientes al cierre del mes a que corresponda la información.	
d) La información relativa a las series R01; R04, exclusivamente por lo que se refiere a los reportes A-0411, A-0417, A-0419, A-0420 y A-0424, C-0433, C-0434, C-0435, C-0436, C-0437, C0438, C-0439 y C-0440; R08; R10; R12; y R13, únicamente por lo que se refiere a los reportes B-1321 y B-1322, deberá proporcionarse, a más tardar, el día 20 del mes inmediato siguiente al de su fecha. Con independencia del envío electrónico, los reportes B-1321 y B-1322 de la serie R13, deberán remitirse a la Comisión, debidamente suscritos por los directivos y personas a que se refiere el Artículo 179 de las presentes disposiciones.	
e) La información relativa a las series R04, exclusivamente por lo que se refiere al reporte C0447, R06 y R07, dentro de los 25 días del mes inmediato siguiente al de su fecha.	
f) La información relativa a la serie R16, exclusivamente por lo que se refiere a los reportes A1611 y A-1612, la serie R24, únicamente los reportes B-2421, B-2422, C-2431, D-2441 y D-2442, la correspondiente a la serie R26~~, así como la serie R35, por lo que se refiere al reporte A-~~	f) La información relativa a la serie R16, exclusivamente por lo que se refiere a los reportes A-1611 y A-1612, la serie R24, únicamente los reportes B-2421, B-2422, C-2431, D-2441 y D-2442, así como la correspondiente a la serie R26, R27 y R35 por lo que se refiere al

Vigente	Propuesta
~~3511,~~ deberá enviarse~~,~~ a más tardar~~,~~ el último día del mes inmediato siguiente al de su fecha.	reporte A-3511, deberá enviarse a más tardar el último día del mes inmediato siguiente al de su fecha.
g) La información del reporte B-2423 correspondiente a la serie R24, deberá ser enviada, a más tardar, a los 45 días siguientes de la fecha de cierre que se reporta.	g) a h) . . .
h) La información relativa a la serie R34 deberá proporcionarse, a más tardar, el último día hábil del mes inmediato siguiente al del mes cuyas cifras se utilicen para el cálculo de la Razón de Apalancamiento	
III. Trimestralmente, la información de las series R14, R15, ~~R27~~ y R32 deberá enviarse dentro del mes inmediato siguiente al de su fecha.	III. Trimestralmente, la información de las series R14, R15, y R32 deberá enviarse dentro del mes inmediato siguiente al de su fecha.
De igual forma, en el plazo mencionado en el párrafo anterior, la relativa a las series R16, R24 y R28, exclusivamente por lo que se refiere a los reportes B-1621, D-2443, E-2450, E-2451, E-2452, A2811 y A-2813 de dichas series.4	. . .
La información de los reportes A-1311 y A-1316 correspondientes a la serie R13, deberá proporcionarse dentro de los veinte días naturales siguientes al de su fecha.	. . .
IV. Anualmente:	IV. . . .
a) La información relativa a la serie R28, exclusivamente por lo que se refiere al reporte A-2812, deberá proporcionarse, con cifras a diciembre de cada año, dentro del mes inmediato siguiente al de su fecha.	
b) La información relativa a las series y reportes que resulte necesario reenviar a fin de guardar consistencia con los estados financieros básicos consolidados anuales dictaminados con cifras al mes de diciembre de cada año referidos en el Artículo 180 de las presentes Disposiciones, deberá proporcionarse dentro de los 90 días naturales siguientes al cierre del ejercicio respectivo.	
Tratándose de instituciones de banca de desarrollo cuyos estados financieros no hubieren sido aprobados por el Consejo dentro de los plazos referidos en las presentes disposiciones como consecuencia del impedimento para sesionar mencionado en el tercer párrafo del Artículo 178, y por lo tanto aún no estuvieren dictaminados, deberán entregarlos a la Comisión, en el plazo a que se refiere el inciso b) de la presente fracción, indicando en todo caso tal circunstancia, eliminando la anotación de que fueron aprobados por el consejo. Lo anterior, sin perjuicio de que deberán remitirlos nuevamente dentro de los 5 días naturales siguientes a la fecha de la sesión del consejo en que tal aprobación se produzca.	. . .
Sin correlativo.	**Artículo 287 Bis.- El Monto Transaccional del Usuario podrá ser definido por el Usuario en la celebración del contrato para apertura de cualquier cuenta, producto o servicio del que se trate O en cualquier momento a**

Vigente		Propuesta
		través del servicio de Banca Electrónica posterior a la contratación de apertura de cuenta, producto o servicio. La Institución deberá proveer lo necesario para que sus Usuarios establezcan el Monto Transaccional del Usuario, empleando cualquier Factor de Autenticación determinado por la Institución, si se realiza en Medios Electrónicos o mediante firma en Oficinas Bancarias, previa identificación del cliente. **En el caso de que el Usuario no establezca su Monto Transaccional del Usuario para los servicios del párrafo anterior, este deberá ser estimado por la Institución de conformidad con el historial de Operaciones Monetarias del Usuario, en un plazo no mayor a seis meses a partir de la celebración del contrato referido. Una vez determinado el Monto Transaccional del Usuario, deberá ser enviado al Usuario para su conocimiento a través de un medio que permita comprobar su recepción, y surtirá sus efectos al día siguiente de su notificación. La metodología y procedimiento para su determinación deberá estar documentado en el Plan de gestión para la prevención del fraude.** **Las Instituciones deberán permitir a sus Usuarios modificar el Monto Transaccional del Usuario mediante Medios Electrónicos de manera no presencial o mediante firma en Oficinas Bancarias. Cuando la modificación se realice mediante Medios Electrónicos de manera no presencial, dicha modificación requerirá al menos dos Factores de Autenticación de los referidos en el artículo 310 de las presentes disposiciones, los cuales deberán ser de categoría distinta. Una vez modificado el Monto Transaccional del Usuario, surtirá sus efectos una vez que la Institución envíe un alertamiento al Usuario de la modificación señalada en el presente párrafo a través de mensajería instantánea con protocolos de Cifrado, vía telefónica o correo electrónico, y este último confirme la acción referida.** **Las Instituciones podrán utilizar el Monto Transaccional del Usuario como insumo para la detección y prevención de eventos que se aparten de los parámetros de uso habitual de sus Usuarios a través de Medios Electrónicos a los que se refiere el Artículo 316 Bis 13 de las presentes disposiciones.**
	Sin correlativo.	**Artículo 287 Bis 1.- Cuando el monto de una Operación Monetaria realizada a través de los servicios de Banca por Internet, Banca Telefónica Voz a Voz, Banca Telefónica Audio Respuesta y Banca Móvil sea mayor al Monto Transaccional del Usuario, las Instituciones deberán requerir un Factor de Autenticación adicional a los establecidos en las presentes disposiciones para la Operación Monetaria de que se trate, de los referidos en el Artículo 310 de las presentes disposiciones, solicitado a través de mensajería instantánea con protocolos de Cifrado, vía telefónica o correo electrónico con protocolos de cifrado. En el caso que la Operación Monetaria sea realizada a través de Banca por Internet, el Factor de Autenticación**

Vigente		Propuesta
		adicional al que se refiere el presente párrafo podrá ser solicitado por Banca Móvil.
	Artículo 307.- Las Instituciones, para la contratación de los servicios de Banca Electrónica con sus clientes, adicionalmente a lo previsto en el Artículo 306 anterior, se sujetarán a lo siguiente: I. Deberán obtener el consentimiento expreso mediante firma autógrafa de sus clientes, previa identificación de estos, mediante firma electrónica avanzada o fiable de sus clientes, siempre y cuando estas se sujeten a lo establecido en el Código de Comercio para estos efectos, o bien, mediante alguno de los procesos previstos en los Artículos 51 Bis 6 y, en su caso, 51 Bis 8 de estas disposiciones. Las Instituciones podrían utilizar alguna otra forma de contratación, tratándose de los servicios siguientes: a) Pago Móvil. b) Aquellos ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, cuando estos se refieran exclusivamente a la operación de Cuentas Bancarias de los Niveles 1 a 3. c) Los previstos en la fracción V de este artículo. d) Banca Móvil, Banca por Internet, Banca Telefónica Audio Respuesta y Banca Telefónica Voz a Voz, cuando estén asociados a Cuentas Bancarias de Niveles 1 a 3, según corresponda, y sean para realizar operaciones diferentes a las previstas en el Artículo 313 de las presentes disposiciones. e) Los contratados a través de Cajeros Automáticos y Terminales Punto de Venta, caso en el cual deberán solicitar a los Usuarios un segundo Factor de Autenticación de las Categorías 3 o 4 a que se refiere el Artículo 310 de estas disposiciones. Adicionalmente, la Institución deberá notificar al Usuario dicha contratación a través del número de línea de Teléfono Móvil que tenga registrado y podrá solicitar la confirmación de la contratación a través de un medio distinto al Cajero Automático o Terminal Punto de Venta en el que se hubiera contratado el servicio. El servicio respectivo deberá habilitarse después de un periodo mínimo de veinticuatro horas posteriores a la notificación o, en su caso, a la confirmación que se hubiere realizado. (205) Asimismo, las Instituciones deberán pactar al momento de la contratación con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones realizadas a través de los servicios antes mencionados que no sean reconocidas por los propios Usuarios, y que las ~~reclamaciones~~ derivadas de estas operaciones deberán ser abonadas a los Usuarios o bien, tratándose del otorgamiento de créditos que los recursos serán retirados de la cuenta del Usuario sin cobro de comisión alguna, a más tardar cuarenta y ocho horas posteriores a la reclamación, excepto cuando el Usuario hubiese confirmado dicha contratación en los términos descritos.	Artículo 307.- . . . I. . . . a) a d) . . . e) . . . Asimismo, las Instituciones deberán pactar al momento de la contratación con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones realizadas a través de los servicios antes mencionados que no sean reconocidas por los propios Usuarios, y que las **Reclamaciones Monetarias** derivadas de estas operaciones deberán ser abonadas a los Usuarios o bien, tratándose del otorgamiento de créditos que los recursos serán retirados de la cuenta del Usuario sin cobro de comisión alguna, a más tardar cuarenta y ocho horas posteriores a la reclamación, excepto cuando el Usuario hubiese confirmado dicha contratación en los términos descritos.

Vigente	Propuesta
II. Podrán permitir a sus Usuarios la contratación de servicios y operaciones adicionales a los originalmente convenidos o modificar las condiciones previamente pactadas con el Usuario, desde el servicio de Banca Electrónica de que se trate, o bien, contratar el uso de otro servicio de Banca Electrónica, siempre y cuando las Instituciones requieran un segundo Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de las presentes disposiciones, adicional al utilizado, en su caso, para iniciar la Sesión. En estos casos, las Instituciones deberán enviar una notificación en términos de lo previsto por la fracción VI del Artículo 316 Bis 1 de estas disposiciones y el servicio correspondiente quedará habilitado para su uso en el periodo determinado por cada Institución, sin que pueda ser menor a treinta minutos contados a partir de que se haya efectuado la contratación. III. Tratándose de los servicios mencionados en los incisos a) y d) de la fracción I anterior, la contratación podrá llevarse a cabo de conformidad con las fracciones I y II anteriores, o bien, a través de los centros de atención telefónica de las propias Instituciones, sujetándose a lo señalado en el Artículo 310, fracción I de estas disposiciones. En todo caso, para el servicio de Pago Móvil, las Instituciones deberán autenticar a los clientes utilizando procedimientos que aseguren que el propio cliente es quien está solicitando el servicio. a) Derogado. b) Derogado. Segundo párrafo. - Derogado. IV. Tratándose de Cuentas Bancarias de Niveles 2, 3 y 4, deberán solicitar a sus Usuarios al momento de la contratación, datos de algún medio de comunicación, tales como su dirección de correo electrónico o número de teléfono móvil para la recepción de Mensajes de Texto SMS, a fin de que las Instituciones les hagan llegar las notificaciones a que se refiere el Artículo 316 Bis 1 de estas disposiciones. V. En la contratación de Banca por Internet a fin de que los clientes realicen operaciones entre la cuenta registrada a su nombre por la Institución como cuenta originadora, y otra cuenta en otra Institución cuyo titular sea el propio cliente como Cuenta Destino, será responsabilidad de la Institución contratante verificar que la Cuenta Destino en la otra Institución se encuentre registrada a nombre del propio cliente. En todo caso, la Institución deberá obtener previamente la autorización de la Comisión para la contratación del servicio de Banca por Internet a que se refiere esta fracción, en cuya solicitud deberá exponer los controles que permitirán a los Usuarios realizar las operaciones de forma segura, sujetándose a lo siguiente:	II. a VI. . . .

Vigente		Propuesta
	a) Al momento de la contratación del servicio de Banca por Internet, las Instituciones deberán requerir a sus Usuarios el registro de una única Cuenta Destino cuyo titular sea el propio Usuario, sin que se requiera un segundo Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de estas disposiciones, en términos de lo previsto en el Artículo 314 de las presentes disposiciones. Si las cuentas originadoras son Cuentas Bancarias de Niveles 2 y 3, o bien, cuentas de administración de valores con los mismos niveles transaccionales, no será necesario que la Cuenta Destino sea del propio Usuario. b) Para realizar transferencias de recursos dinerarios o instrucciones de cargo entre la cuenta originadora registrada en la Institución y la Cuenta Destino a que se refiere el párrafo anterior, las Instituciones deberán requerir a sus Usuarios un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de estas disposiciones, sin que le sea aplicable el primer párrafo del Artículo 313 de las presentes disposiciones, debiendo contemplar, en todo caso, controles que aseguren que es el Usuario quien está instruyendo a la Institución, y c) En caso de que un Usuario solicite cambiar la Cuenta Destino a que se refiere el inciso a) de esta fracción, podrá realizarlo mediante el procedimiento mencionado en la fracción I del presente artículo, o bien, en el evento de realizar la modificación a través de la Banca por Internet, las Instituciones deberán requerir un Factor de Autenticación de las Categorías 3 o 4 a que se refiere el Artículo 310 de las presentes disposiciones, adicional al utilizado para iniciar la Sesión. Para la contratación de los servicios de Banca por Internet, Banca Telefónica Audio Respuesta o Banca Telefónica Voz a Voz relacionados con Cuentas Bancarias de Niveles 2 y 3 u otras con los mismos niveles transaccionales, como cuentas originadoras, a fin de realizar las operaciones descritas en esta fracción, las Instituciones podrán utilizar mecanismos de identificación similares a los requeridos para la apertura de dicha cuenta originadora. VI. Tratándose de las Cuentas Bancarias de Nivel 1, dichas cuentas no podrán asociarse a servicios de Banca Electrónica para realizar Operaciones Monetarias, exceptuándose aquellos servicios ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta. En el caso de las operaciones que se realicen a través de Terminales Punto de Venta, estas solo podrán efectuarse cuando el Usuario presente la tarjeta de débito de que se trate en el Establecimiento.	
	Artículo 309.- Las Instituciones, en el uso del Identificador de Usuario y los Factores de Autenticación, deberán ajustarse a lo siguiente: I. Proveer lo necesario para impedir la lectura en la pantalla del Dispositivo de Acceso, de la información de identificación y Autenticación proporcionada por el Usuario, salvo que se trate de Banca Telefónica de Audio Respuesta.	Artículo 309.- . . . I. . . .

Vigente	Propuesta
En caso de que la tecnología utilizada en Pago Móvil no permita implementar lo señalado en el párrafo anterior y la información de los factores de autenticación se almacene en el dispositivo, las Instituciones podrán ofrecer tal servicio obteniendo la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.	. . .
Asimismo, las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán prever que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones realizadas a través de Pago Móvil que no cumplan con lo previsto en el primer párrafo de la presente fracción y que no sean reconocidas por los Usuarios. Las ~~reclamaciones~~ derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.	Asimismo, las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán prever, al momento de la contratación con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones realizadas a través de Pago Móvil que no cumplan con lo previsto en el primer párrafo de la presente fracción y que no sean reconocidas por los Usuarios. Las **Reclamaciones Monetarias** derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la Reclamación Monetaria.
Asegurar que en la generación, entrega, almacenamiento, desbloqueo y restablecimiento de los Factores de Autenticación, únicamente sea el Usuario quien los reciba, active, conozca, desbloquee y restablezca. El Usuario podrá autorizar a un tercero para recibir dichos Factores de Autenticación, siempre que las Instituciones mantengan procedimientos para que dichas autorizaciones sean de carácter eventual y puedan ser revocados por el cliente cuando así lo solicite.	. . .
II. Contar con procedimientos para invalidar los Factores de Autenticación para impedir su uso en un servicio de Banca Electrónica, cuando un Usuario o la misma Institución cancele el uso de dicho servicio o cuando dicho Usuario deje de ser cliente de la Institución.	II. . . .
Artículo 310.- Las Instituciones deberán utilizar Factores de Autenticación para verificar la identidad de sus Usuarios y la facultad de estos para realizar operaciones a través del servicio de Banca Electrónica. Dichos Factores de Autenticación, dependiendo del Medio Electrónico de que se trate y de lo establecido en las presentes disposiciones, deberán ser de cualquiera de las categorías siguientes:	Artículo 310.- . . .
I. Factor de Autenticación Categoría 1: Se compone de información obtenida mediante la aplicación de cuestionarios al Usuario, por parte de operadores telefónicos o remotos, en los cuales se requieran datos que el Usuario conozca. En ningún caso los Factores de Autenticación de esta categoría podrán componerse únicamente de datos que hayan sido incluidos en comunicaciones impresas o electrónicas enviadas por las Instituciones a sus clientes.	I. a II. . . .
Las Instituciones, en la utilización de los Factores de Autenticación de esta categoría, para verificar la identidad de sus Usuarios, deberán observar lo siguiente:	

Vigente		Propuesta
	a) Definir previamente los cuestionarios que serán practicados por los operadores telefónicos o remotos, impidiendo que sean utilizados de forma discrecional, y b) Validar al menos una de las respuestas proporcionadas por sus Usuarios, a través de herramientas informáticas, sin que el operador pueda consultar o conocer anticipadamente los datos de Autenticación de los Usuarios. II. Factor de Autenticación Categoría 2: Se compone de información que solo el Usuario conozca e ingrese a través de un Dispositivo de Acceso, tales como Contraseñas y Números de Identificación Personal (NIP), y deberán cumplir con las características siguientes: a) En ningún caso se podrá utilizar como tales, la información siguiente: i El Identificador de Usuario. ii El nombre de la Institución. iii Más de tres caracteres idénticos en forma consecutiva. iv. Más de tres caracteres consecutivos numéricos o alfabéticos. No resultará aplicable lo previsto en el presente inciso para el caso de Pago Móvil, Banca Móvil y las operaciones realizadas a través de Cajeros Automáticos y Terminales punto de Venta, siempre que las Instituciones informen al Usuario al momento de la contratación, de la importancia de la composición de las Contraseñas para estos servicios. b) Su longitud deberá ser de al menos seis caracteres, salvo por los servicios ofrecidos a través de Cajeros Automáticos y Terminales Punto de Venta, en cuyo caso será de al menos cuatro caracteres. i Derogado. ii Derogado. iii Derogado. c) La composición de estos Factores de Autenticación podrá incluir caracteres numéricos, alfabéticos u otros, cuando el Dispositivo de Acceso lo permita. Las Instituciones deberán permitir al Usuario cambiar sus Contraseñas, Números de Identificación Personal (NIP) y otra información de Autenticación estática, cuando este último así lo requiera, utilizando los servicios de Banca Electrónica. Tratándose de Contraseñas o Números de Identificación Personal (NIP) definidos o generados por las Instituciones durante la contratación de un	

Vigente		Propuesta
	servicio de Banca Electrónica o durante el restablecimiento de dichas contraseñas, las propias Instituciones deberán prever mecanismos y procedimientos por medio de los cuales el Usuario deba modificarlos inmediatamente después de iniciar la Sesión correspondiente. Las Instituciones deberán contar con controles que les permitan validar que las nuevas Contraseñas o Números de Identificación Personal (NIP) utilizadas por sus Usuarios, sean diferentes a los definidos o generados por las propias Instituciones. Las Instituciones deberán recomendar a sus Usuarios en el proceso de contratación del servicio de Banca Electrónica, que mantengan Contraseñas seguras. III. Factor de Autenticación Categoría 3: Se compone de información contenida, recibida o generada por medios o dispositivos electrónicos, así como la obtenida por dispositivos generadores de Contraseñas dinámicas de un solo uso. Dichos medios o dispositivos deberán ser proporcionados por las Instituciones a sus Usuarios y la información contenida, recibida o generada por ellos deberá cumplir con las características siguientes: a) Contar con propiedades que impidan su duplicación o alteración. b) Ser información dinámica que no podrá ser utilizada en más de una ocasión. c) Tener una vigencia que no podrá exceder de dos minutos. d) No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes o comisionistas de la Institución o por terceros. Las Instituciones podrán proporcionar a sus Usuarios medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen información de la Cuenta Destino y en el caso de operaciones no monetarias, cualquier otra información relacionada con el tipo de operación o servicio de que se trate, de manera que dicha Contraseña únicamente pueda ser utilizada para la operación solicitada. En estos casos, no será aplicable lo dispuesto en el inciso c) de la presente fracción, así como lo establecido en el cuarto párrafo del Artículo 314 de estas disposiciones en relación al tiempo en que deberán quedar habilitadas las Cuentas Destino. Asimismo, las Instituciones podrán considerar dentro de esta categoría a la información contenida en el circuito o chip de las Tarjetas Bancarias con Circuito Integrado, siempre y cuando dichas tarjetas se utilicen únicamente para operaciones que se realicen a través de Cajeros Automáticos y Terminales Punto de Venta y tales Dispositivos de Acceso obtengan la información de la tarjeta a través del dicho circuito o chip.	III. . . . .

Vigente	Propuesta
Las Instituciones que aprueben la celebración de operaciones mediante el uso de tarjetas bancarias sin circuito integrado, en Cajeros Automáticos y Terminales Punto de Venta, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas. Las ~~reclamaciones~~ derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.	Las Instituciones que aprueben la celebración de operaciones mediante el uso de tarjetas bancarias sin circuito integrado, en Cajeros Automáticos y Terminales Punto de Venta, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en el uso de dichas tarjetas. Las **Reclamaciones Monetarias** derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la Reclamación Monetaria.
Tratándose de Banca Host to Host, las Instituciones podrán utilizar como Factor de Autenticación de esta Categoría, cualquier mecanismo que les permita verificar que los equipos de cómputo o dispositivos utilizados por los Usuarios para establecer la comunicación, son los que la propia Institución autorizó.	. . .
Las Instituciones podrán utilizar tablas aleatorias de Contraseñas como Factor de Autenticación de esta Categoría, siempre y cuando dichas tablas cumplan con las características listadas en los incisos a), b) y d) de la presente fracción. Para el caso del inciso a), las Instituciones deberán asegurarse que las propiedades que impidan la duplicación o alteración se cumplan hasta el momento de la entrega al Usuario. En todo caso, las Instituciones deberán obtener la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura.	. . .
Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por aquellos realizadas a través del servicio de Banca Electrónica de que se trate. Las ~~reclamaciones~~ derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la ~~reclamación~~.	Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios que asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por aquellos realizadas a través del servicio de Banca Electrónica de que se trate. Las **Reclamaciones Monetarias** derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la **Reclamación Monetaria**.
IV. Factor de Autenticación Categoría 4: Se compone de información del Usuario derivada de sus propias características físicas, tales como huellas dactilares, geometría de la mano, patrones en iris o retina y reconocimiento facial, entre otras. Previo a la captura de los datos biométricos mencionados de sus Usuarios, las Instituciones deberán capturar los mismos datos biométricos de sus empleados, directivos y funcionarios encargados de esta función, y verificar que los datos biométricos de clientes no correspondan con los de dichos empleados, directivos y funcionarios. Tratándose de la captura de huellas dactilares e identificación facial que las Instituciones pretendan mantener en sus bases de datos para efectos de autenticación de sus clientes, empleados, directivos y funcionarios, estas deberán sujetarse a los requerimientos técnicos que se establecen en el Anexo 71 de las presentes disposiciones.	IV. . . .
Tratándose de huellas dactilares, será necesario que, para conformar las bases de datos a que se refiere el párrafo anterior y poderlas usar con posterioridad	. . .

Vigente		Propuesta
	para efectos de autenticación, las Instituciones den de alta a sus clientes, empleados, directivos y funcionarios previa verificación de sus huellas con los registros del Instituto Nacional Electoral o de la Secretaría de Relaciones Exteriores, u otra autoridad financiera o fiscal mexicanas, o dependencia federal, que provea un servicio de verificación de información biométrica. Las Instituciones que utilicen los Factores de Autenticación de esta categoría, deberán aplicar para cada operación a la información de Autenticación obtenida por dispositivos biométricos, elementos que aseguren que dicha información sea distinta cada vez que sea generada, a fin de constituir Contraseñas de un solo uso, que en ningún caso puedan utilizarse nuevamente o duplicarse con la de otro Usuario. Las Instituciones podrán considerar dentro de esta categoría la firma autógrafa de sus Usuarios en los comprobantes generados por las Terminales Punto de Venta o bien la plasmada en dispositivos ópticos que produzcan la imagen digitalizada de la firma, únicamente cuando los propios Usuarios realicen Operaciones Monetarias referidas al pago de bienes o servicios a través de dichas Terminales Punto de Venta.	. . . . . .
	Artículo 313.- Las Instituciones deberán solicitar a sus Usuarios, para la celebración de operaciones o prestación de servicios a través de Medios Electrónicos, un segundo Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de estas disposiciones, adicional al utilizado, en su caso, para iniciar la Sesión y en cada ocasión en que se pretenda realizar cada una de las operaciones y servicios siguientes: I. Transferencias de recursos dinerarios a Cuentas Destino de terceros u otras Instituciones, incluyendo el pago de créditos y de bienes o servicios, así como las autorizaciones e instrucciones de domiciliación de pago de bienes o servicios. Cuando las Cuentas Destino hayan sido registradas en Oficinas Bancarias utilizando la firma autógrafa del Usuario, previa identificación de este o bien, el Usuario haya solicitado que dichas cuentas se consideren como Cuentas Destino Recurrentes, las Instituciones podrán permitir a los Usuarios realizar dichas operaciones utilizando un solo Factor de Autenticación de las Categorías 2, 3 ó 4 a que se refiere el artículo 310 de estas disposiciones. Asimismo, las Instituciones deberán proveer lo necesario para que los Usuarios puedan desactivar o dar de baja las Cuentas Destino registradas en el servicio de Banca Electrónica de que se trate. De igual forma, tratándose de transferencias de recursos dinerarios a cuentas de quienes se consideren donatarias autorizadas en términos de las disposiciones fiscales que resulten aplicables, cuyo monto agregado diario no exceda al equivalente en moneda nacional a las operaciones de Baja Cuantía, o bien, el equivalente en moneda nacional a 1,000 UDIs mensuales, no será necesario el uso de un segundo Factor de Autenticación, ni realizar el registro previo de la cuenta donataria destino conforme a lo estipulado en el Artículo	Artículo 313.- . . . I. a IX. . . .

Vigente		Propuesta
	314 de las presentes disposiciones, siempre y cuando cada una de dichas transferencias se realicen dentro de la misma sesión de otra transacción o transferencia, respecto de la cual sí se requiera el citado segundo Factor de Autenticación. En tales supuestos, se deberá emitir el comprobante por cada una de las operaciones conforme al artículo 316 bis y realizar la notificación prevista en el Artículo 316 Bis 1 de las presentes disposiciones. II. Pago de contribuciones. III. Establecimiento e incremento de límites de monto para Operaciones Monetarias a que se refiere el Artículo 315 de las presentes disposiciones, para el servicio de que se trate u otros servicios de Banca Electrónica; IV. Registro de Cuentas Destino de terceros u otras Instituciones para el servicio de que se trate u otros servicios de Banca Electrónica; V. Alta y modificación del medio de notificación a que se refiere el Artículo 316 Bis 1 de estas disposiciones, salvo lo previsto en el último párrafo de dicho artículo; VI. Consultas de estados de cuenta de uno o más periodos u otras consultas que permitan conocer información relacionada con el Usuario y sus cuentas, tales como el domicilio, límites de crédito, beneficiarios o cotitulares, u otra que pueda ser utilizada como información de Autenticación. No será necesario el referido segundo factor, para el caso de la consulta de estados de cuenta, siempre que el Usuario haya iniciado su sesión con un Factor de Autenticación de las Categorías 3 o 4. Las Instituciones podrán permitir a los Usuarios la impresión de estados de cuenta utilizando una tarjeta bancaria y un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, en equipos electrónicos o de telecomunicaciones ubicados únicamente dentro de las Oficinas Bancarias que la Comisión determine, mediante disposiciones de carácter general, que cuentan con las medidas máximas de seguridad conforme a lo establecido por el artículo 96 de la Ley. Igualmente, las Instituciones podrán permitir a sus Usuarios consultar los estados de cuenta, requiriendo únicamente un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de estas disposiciones, siempre y cuando dichas consultas versen sobre operaciones de crédito y se realice la notificación a que se hace referencia en el Artículo 316 Bis 1 de las presentes disposiciones. En estos casos, las Instituciones deberán solicitar un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de estas disposiciones, para dar cumplimiento a lo previsto por la fracción V del presente artículo. VII. Contratación de otro servicio de Banca Electrónica o de operaciones y servicios adicionales a los originalmente convenidos, conforme a lo dispuesto en el Artículo 307 de estas disposiciones;	

Vigente	Propuesta
VIII. Desbloqueo de Contraseñas o Números de Identificación Personal (NIP) respecto de otros servicios de Banca Electrónica que el Usuario tenga contratados, y IX. Retiro de efectivo en Cajeros Automáticos.	
Las Instituciones no se encontrarán obligadas a solicitar a sus Usuarios un Factor de Autenticación de las Categorías 3 ó 4 a que se refiere el Artículo 310 de las presentes disposiciones, cuando se trate de las Operaciones Monetarias que se realicen a través de Pago Móvil. Dichas operaciones podrán realizarse utilizando al menos un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, debiendo las Instituciones asegurar que las Operaciones Monetarias se realizan a través del número de línea que se encuentra asociado al servicio.	. . .
Tratándose de Operaciones Monetarias consideradas como Micro Pagos, cuyo Dispositivo de Acceso sea un Teléfono Móvil o una Terminal Punto de Venta, podrán ser realizadas sin que las Instituciones soliciten Factores de Autenticación. Las Instituciones deberán prever, al momento de la contratación con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en dichos casos. Las ~~reclamaciones~~ derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.	Tratándose de Operaciones Monetarias consideradas como Micro Pagos, cuyo Dispositivo de Acceso sea un Teléfono Móvil o una Terminal Punto de Venta, podrán ser realizadas sin que las Instituciones soliciten Factores de Autenticación. Las Instituciones deberán pactar, al momento de la contratación con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones que no sean reconocidas por los Usuarios en dichos casos. Las **Reclamaciones Monetarias** derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la **Reclamación Monetaria**.
Asimismo, las Instituciones podrán enviar a solicitud de sus Usuarios, estados de cuenta a través de correo electrónico, siempre y cuando la información se transmita de forma Cifrada o con mecanismos que eviten su lectura por parte de terceros no autorizados, y requieran un Factor de Autenticación Categoría 2 a que se refiere el Artículo 310 de las presentes disposiciones, para que el Usuario tenga acceso, el cual deberá ser distinto al utilizado para acceder al servicio de Banca por Internet. Las Instituciones deberán establecer medidas que protejan la confidencialidad de los datos transmitidos y del Factor de Autenticación utilizado.	. . .
Tratándose de los servicios de Banca por Internet proporcionados a Usuarios que sean personas morales, las Instituciones podrán implementar mecanismos mediante los cuales una persona autorizada por el Usuario, realice la solicitud para efectuar las operaciones, y otra persona distinta que sea designada por el propio Usuario, autorice su ejecución. En estos casos, se podrá exceptuar a las Instituciones de la obligación de que el servicio de Banca por Internet cumpla con el tiempo de habilitación de la cuenta así como respecto del uso de un segundo Factor de Autenticación por cada operación, siempre y cuando las Instituciones implementen controles que permitan diferenciar las funciones aplicables a la persona que solicita una operación, respecto de aquellas que aplican a la persona que autoriza su ejecución. En el supuesto establecido en el presente párrafo, las Instituciones	. . .

Vigente		Propuesta
	deberán obtener la previa autorización de la Comisión, en cuya solicitud deberán exponer los controles que les permitirán a los Usuarios realizar operaciones de forma segura. Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por los Usuarios en dichos casos. Las ~~reclamaciones~~ derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la ~~reclamación~~.	Las Instituciones que obtengan la autorización a que se refiere el párrafo anterior, deberán pactar con sus Usuarios, que las propias Instituciones asumirán los riesgos y por lo tanto los costos de las operaciones no reconocidas por los Usuarios en dichos casos. Las **Reclamaciones Monetarias** derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la **Reclamación Monetaria**.
	Artículo 316 Bis 14.- Las Instituciones deberán mantener en bases de datos todas las operaciones efectuadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios y que, al menos, incluya la información relacionada con operaciones ~~no reconocidas por los Usuarios y el~~ trámite que, en su caso, haya promovido el Usuario, ~~tales~~ como ~~folio de reclamación, fecha de reclamación, causa o motivo de la reclamación, fecha de la operación, cuenta origen, tipo de producto, servicio de Banca Electrónica en el que se realizó la operación, importe, estado de la reclamación, resolución, fecha de resolución, monto abonado, monto recuperado y monto quebrantado~~. ~~La información anterior deberá mantenerse en la Institución durante un periodo no menor a cinco años contado a partir de su registro, sin perjuicio de otras disposiciones que resulten aplicables.~~	Artículo 316 Bis 14.- Las Instituciones deberán mantener **por un plazo de al menos 5 años,** en **sus** bases de datos todas las operaciones efectuadas a través del servicio de Banca Electrónica que no sean reconocidas por sus Usuarios y que, al menos, incluya la información relacionada con **estas** operaciones **y la relativa al** trámite que, en su caso, haya promovido el Usuario, **tal** como**, la información establecida en el reporte regulatorio R27 A-2701 Reclamaciones Monetarias**.
	Artículo 339.- Las Instituciones deberán establecer e implementar en todas sus Sucursales y Módulos Bancarios, las siguientes medidas mínimas de seguridad y protección: I. Dispositivo blindado para la protección de efectivo y valores con mecanismo de retardo físico o electrónico incorporado. En su defecto, el área donde se ubique el dispositivo blindado para la protección de efectivo y valores deberá contar con un mecanismo de acceso con retardo físico o electrónico. II. Exhibición de fotografías de personas que presuntamente hubieren cometido algún ilícito en perjuicio de alguna Institución o del Público Usuario. III. Normativa sobre métodos y límites en el manejo y traslado de valores y efectivo. IV. Procesos de coordinación operativa entre la Unidad Especializada y los cuerpos de seguridad pública, así como, en su caso, entre las referidas instancias y la Sociedad de Apoyo.	Artículo 339.- . . . I. a IV. . . . **V. Las relativas para procurar las condiciones de privacidad de los retiros y otras transacciones que el Público Usuario realice en**

Vigente		Propuesta
		ventanillas, respecto de aquellos que se encuentran en la sala de espera de las Sucursales y Módulos Bancarios.
	Sin correlativo.	**T R A N S I T O R I O S** **PRIMERO.– La presente Resolución entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación, contando con los plazos establecidos en los siguientes transitorios para el cumplimiento de las obligaciones contenidas en esta.** **SEGUNDO.- Las instituciones de banca múltiple, contarán:** **I. Hasta el 1 julio de 2024, para enviar a la Comisión por única ocasión en una fecha distinta a la establecida en el artículo 164 Bis 1, la primera entrega del Plan de gestión para la prevención del fraude.** **II. Hasta el 2 de enero de 2025, para implementar lo establecido en el Plan de gestión para la prevención del fraude entregado a la Comisión el 1 de julio de 2024, así como, para ajustarse a lo establecido en la presente Resolución.** **III. Hasta el 2 de julio de 2025, para que se determine el Monto Transaccional del Usuario, ya sea por la Institución o por el propio Usuario, cuando no se haya establecido para las cuentas, productos o servicios vigentes al 2 de enero de 2025.** **TERCERO.- Las instituciones de banca de desarrollo, contarán:** **I. Hasta el 31 de enero de 2025, para enviar a la Comisión por única ocasión en una fecha distinta a la establecida en el artículo 164 Bis 1, la primera entrega del Plan de gestión para la prevención del fraude.** **II. Hasta el 2 de enero de 2026, para implementar lo establecido en el Plan de gestión para la prevención del fraude entregado a la Comisión el 31 de enero de 2025, así como, para ajustarse a lo establecido en la presente Resolución.** **III. Hasta el 2 de julio de 2026, para que se determine el Monto Transaccional del Usuario, ya sea por la Institución o por el propio Usuario, cuando no se haya establecido para las cuentas, productos o servicios vigentes al 2 de enero de 2026.** **CUARTO.- A partir del 2 de enero de 2026, las Instituciones estarán obligadas a incluir la evaluación referida en el artículo 160 fracción XV y en el último párrafo del Anexo 12-E, así como los eventos del delito de**

Vigente		Propuesta
		fraude concluidos y analizados, y los indicadores referidos en el inciso d) y e) de la fracción III, e inciso d), fracción II del Anexo 12-E de la presente Resolución Modificatoria. **QUINTO.- Las instituciones deberán enviar a la Comisión el código de conducta que resulte de las modificaciones previstas en el artículo 142 fracción III, a más tardar al 1 de julio de 2025 para las instituciones de banca múltiple y al 1 de julio de 2026 para las instituciones de banca de desarrollo.**
	Sin correlativo.	**Anexo 12-E** **Lineamientos mínimos del Plan de gestión para la prevención del fraude**
	Sin correlativo.	**El Plan de Gestión de Fraude debe considerar los elementos mínimos siguientes: contar con mecanismos de identificación, medición, prevención, control y respuesta de posibles eventos por Conductas observables para la gestión del fraude, esquemas de reporte que consideren aspectos cuantitativos y cualitativos, así como la ejecución de revisiones y auditorías periódicas para reajustar oportunamente, en su caso, los parámetros de los modelos, mecanismos y procesos de vigilancia, bajo los siguientes principios.**
	Sin correlativo.	• **Gobierno corporativo: Se debe establecer un gobierno corporativo que muestre los principios para la gestión de las Conductas observables para la gestión del fraude y las expectativas del Consejo y la Dirección General, respecto a su compromiso con valores éticos para la atención de Conductas observables para la gestión del fraude, el cual debe documentarse en las políticas institucionales del área de prevención de fraudes. Asimismo, deben establecerse los incentivos de conformidad a lo establecido en la Sección Octava, Capítulo VI del Título Segundo de las presentes Disposiciones, así como los requisitos para que los funcionarios y empleados alcancen las metas y el buen desempeño en la atención de Conductas observables para la gestión del fraude, así como vigilar y documentar el cumplimiento de dichas metas.** • **Medición y monitoreo de las Conductas observables para la gestión del fraude: La Dirección General de la Institución debe garantizar que se realicen evaluaciones para identificar los esquemas de las Conductas observables para la gestión del fraude, evaluando su probabilidad e importancia y las actividades de control de dichas conductas existentes. Se deben utilizar los resultados de esas evaluaciones para retroalimentar y fortalecer el diseño del sistema de gestión de riesgos de la Institución. Las políticas que se establezcan deben definir y comunicar claramente**

Vigente		Propuesta
		el compromiso del Consejo y la Dirección General para la atención de las Conductas observables para la gestión del fraude. • **Colaboración, investigación e intercambio de información: Las Instituciones deben de contar con políticas, procesos de comunicación y de investigaciones internas los cuales deben documentarse en los manuales de políticas y procedimientos de la Institución, así como sistemas de control interno que garanticen un enfoque coordinado para llevar a cabo investigaciones apropiadas, respuestas oportunas, y la atención de las denuncias de sospecha de Conductas observables para la gestión del fraude, así como de aquellas confirmadas. Para efectos del presente párrafo, tratándose de instituciones de banca de desarrollo, se deberá involucrar a su órgano interno de control.**
	Sin correlativo.	**Los procesos del Plan de Gestión para la prevención del fraude deben contener una combinación de controles preventivos, de detección y de respuesta a las Conductas observables para la gestión del fraude. Todos los procesos deben realizarse y estar debidamente documentados. Los proyectos mínimos que se deben considerar en el Plan de Gestión para la prevención del fraude son:**
	Sin correlativo.	**I. Prevención de Conductas observables para la gestión del fraude.**
	Sin correlativo.	**a) Establecer en la Institución una cultura que promueva el comportamiento ético en todos los niveles del personal, a través de campañas, capacitaciones y el establecimiento de manuales de ética.**
	Sin correlativo.	**b) Incluir en su código de conducta o declaración de ética las medidas y responsabilidades que los empleados tienen en materia de tratamiento y prevención de Conductas observables para la gestión del fraude, así como las correspondientes sanciones en caso de su incumplimiento.**
	Sin correlativo.	**c) Capacitar, al menos una vez al año, a los empleados para la atención de Conductas observables para la gestión del fraude de acuerdo con sus funciones y responsabilidades.**
	Sin correlativo.	**d) Capacitar, al menos una vez al año, a los empleados en la atención al Público Usuario que sean víctimas de posibles Conductas observables para la gestión del fraude.**
	Sin correlativo.	**e) Proporcionar al Usuario capacitación sobre los riesgos de las Conductas observables para la gestión del fraude y las medidas preventivas que estos pueden tomar para reducir el riesgo de convertirse en víctimas. En el caso de operaciones a través del servicio de Banca electrónica, lo señalado en el presente**

Vigente		Propuesta
		párrafo será complementario con lo referido en el artículo 306, fracción III de las presentes Disposiciones.
	Sin correlativo.	**f) Implementar estrategias para la prevención de fraudes en el proceso de originación de crédito, con el objetivo de prevenir la aceptación de información falsa en las solicitudes de crédito.**
	Sin correlativo.	**g) Establecer medidas para prevenir la realización de Conductas observables para la gestión del fraude en Personas en Situación de Vulnerabilidad , a través de capacitación del personal, promoción de nuevos modelos de atención de servicios bancarios, campañas de educación financiera señalando que las Instituciones nunca solicitan información confidencial al Usuario, programas de asesoría con personal en los cajeros automáticos de las sucursales, campañas antifraude, programas de asesoría remota y alternativas de solución a problemas sobre los productos y servicios bancarios e implementación de acciones que permitan nuevos modelos de atención.**
	Sin correlativo.	**h) Establecer medidas para combatir conductas tendientes a obtener datos confidenciales del Usuario, a través de una solicitud fraudulenta por correo electrónico, sitios web, llamadas telefónicas, Mensajes SMS, entre otros medios, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza; estableciendo como mínimo, las siguientes medidas: campañas permanentes dirigidas al Usuario, señalando que las Instituciones nunca solicitan información confidencial al Usuario; consejos sobre la identificación de correos electrónicos falsos, llamadas o mensajes de texto fraudulentos; promoción de canales de comunicación protegidos y cifrados para transmitir información sensible con el Usuario; establecimiento de procedimientos claros para la denuncia de este tipo de conductas; implementación de soluciones en línea como software antivirus y antimalware; y monitoreo de sitios web falsos.**
	Sin correlativo.	**i) Brindar campañas informativas al Público Usuario con la finalidad de prevenir Conductas observables para la gestión del fraude.**
	Sin correlativo.	**II. Detección de Conductas observables para la gestión del fraude.**
	Sin correlativo.	**a) Contar con sistemas y controles para la revisión y seguimiento de operaciones, capaces de detectar anomalías y operaciones que se aparten del Monto Transaccional del Usuario o relacionadas con posibles actividades fraudulentas. En el caso de**

Vigente		Propuesta
		operaciones a través de Medios Electrónicos, lo señalado en el presente párrafo será complementario con lo referido en el artículo 316 Bis 13, de las presentes Disposiciones.
	Sin correlativo.	**b) Contar con modelos, sistemas de monitoreo o informes diseñados para detectar y alertar actos fraudulentos en todas las líneas de negocios como son de manera enunciativa, mas no limitativa, informes de excepción, informes de mantenimiento de archivos, procesos de vigilancia de empleados, monitoreo de cuentas, control de accesos al sistema, patrones y anulaciones.**
	Sin correlativo.	**c) Contar con sistemas automatizados de alertamiento de operaciones dirigidas a los Usuarios, que se aparten del Monto Transaccional del Usuario y de los parámetros basados en el consumo y la localización de Operaciones Monetarias generadas por el Usuario, de tal forma que este pueda detectar el inicio de operaciones e intentos fallidos de iniciarlas, así como procesos documentados en manuales para la gestión de alertas.** **La información que resulte de los sistemas de alertamiento formará parte de la evidencia referida en el inciso f), fracción IV del Anexo 12-F de las presentes disposiciones. Asimismo, las instituciones deberán implementar procesos con el objetivo de proteger los recursos de los Usuarios cuando se presenten los alertamientos referidos, tales como recomendar al Usuario el cambio de contraseñas, cambio de Factores de Autenticación, en su caso, entre otros, cuya metodología debe estar documentada en el presente plan.**
	Sin correlativo.	**d) Diseñar indicadores operativos relativos a la detección de Conductas observables para la gestión del fraude. Los indicadores y su seguimiento con corte a la fecha de aprobación del Plan de Gestión para la prevención del fraude deberán formar parte de este como un anexo.**
	Sin correlativo.	**e) Analizar los datos de pérdidas derivadas de Conductas observables para la gestión del fraude, transacciones, cancelaciones, Reclamaciones Monetarias, errores y datos de quejas del Público Usuario, con la finalidad de detectar posibles hechos de comisión del delito de fraude.**
	Sin correlativo.	**f) Incorporar canales internos y sistemas de informes mediante los cuales los empleados de las Instituciones puedan denunciar de manera anónima Conductas observables para la gestión del fraude.**
	Sin correlativo.	**III. Respuesta a Conductas observables para la gestión del fraude.**

Vigente		Propuesta
	Sin correlativo.	**a) Investigar todos los casos de las Conductas observables para la gestión del fraude, para determinar hechos e identificar riesgos y debilidades de control.**
	Sin correlativo.	**b) Establecer procedimientos documentados y aprobados por la Dirección General que rijan la investigación de casos reales o sospechas de Conductas observables para la gestión del fraude. Estos procedimientos deben designar al personal responsable de supervisar y llevar a cabo la investigación, y establecer normas relativas al procedimiento de la investigación, como las normas que rigen la realización de entrevistas, el tratamiento de las pruebas o evidencias, el tratamiento de las personas involucradas y el informe de los resultados.**
	Sin correlativo.	**c) Informar al Consejo, a través del de la persona titular o responsable del área encargada de prevención de fraudes, todos los eventos relevantes de las Conductas observables para la gestión del fraude, definiendo su relevancia en el propio Plan de Gestión para la prevención del fraude. Asimismo, en dicho plan se deberá establecer la periodicidad con la que deberá informarse al Consejo.**
	Sin correlativo.	**d) Registrar todos los hechos determinados como comisión del delito de fraude por las autoridades competentes y analizarlos para mejorar el Plan de Gestión para la prevención del fraude. Los eventos concluidos y sus análisis a la fecha de aprobación del Plan de Gestión para la prevención del fraude deberán formar parte de este como un anexo, agrupando por casuística del delito de fraude y describiendo cómo se llevaron a cabo, qué medidas de control, en su caso, fallaron y los ajustes o nuevas medidas de control que se implementaron para prevenir que las medidas de control vuelvan a fallar, en su caso.**
		e) Establecer una serie de indicadores para el seguimiento de Conductas observables para la gestión del fraude. Los indicadores y su seguimiento con corte a la fecha de aprobación del Plan de Gestión para la prevención del fraude deberán formar parte de este como un anexo.
		f) Establecer un canal de comunicación interbancario donde se comparta la información relativa a la casuística y las posibles personas físicas empleadas de las Instituciones que cometieron Conductas observables para la gestión del fraude internas, sólo en caso de que la infracción respecto al código de conducta de las Instituciones esté documentado.
		g) Establecer un canal de comunicación interbancario, a través del cual las instituciones de crédito intercambiarán información cuando tengan alertamientos, incluyendo Reclamaciones

Vigente		Propuesta
		Monetarias de sus clientes por presuntas actividades fraudulentas realizadas por personas físicas o morales ,que involucren a más de una institución y, así como las acciones que llevarán a cabo para colaborar entre ellas para evitar la materialización de un delito, así como, para compartir los comportamientos y tendencias del delito de fraude detectadas dentro del Sistema Financiero, datos y la documentación necesaria para la resolución de Reclamaciones Monetarias recibidas por el Público Usuario.
		La persona titular de la dirección general es responsable de monitorear la revisión, al menos una vez al año, para que se garantice que la estrategia puede contribuir a un enfoque de respuesta a Conductas observables para la gestión del fraude. Cada una de las unidades de negocio deben llevar a cabo pruebas y revisiones basadas en los controles que pudieron haber fallado. Asimismo, al menos una vez cada dos años, de manera alternada con la auditoría interna señalada en la fracción XV del artículo 160 de las presentes disposiciones, un auditor externo independiente debe determinar la efectividad y debilidades del Plan de gestión para la prevención del fraude, estableciendo recomendaciones para su mejora continua, tomando en cuenta los hechos identificados que representaron la comisión de fraudes, realizando el seguimiento de las acciones correctivas implementadas por las áreas o funciones responsables de atender dichas recomendaciones. El informe de cada auditoría formará parte de Plan de gestión para la prevención del fraude como anexo
	Sin correlativo.	**Anexo 12-F** **De la información que las instituciones deberán poner a disposición del Usuario o la Comisión derivado de Reclamaciones Monetarias**
	Sin correlativo.	**Las Instituciones deberán asegurarse que los procesos y aspectos básicos de dictaminación de Reclamaciones Monetarias sean transparentes, considerando al menos lo siguiente:**
	Sin correlativo.	**I. Cada Institución debe tener establecido un procedimiento para Reclamaciones Monetarias documentado en sus manuales de procedimientos y ponerlo a disposición del Usuario en su página de Internet, y en sucursal por un aviso visible o mediante la utilización de pantallas visibles informativas o cualquier otro medio semejante, que permita al Usuario obtener de manera expedita o descargar por escrito el procedimiento de Reclamaciones Monetarias.** **Estos procedimientos deberán prever las consideraciones que sean aplicables cuando la Reclamación Monetaria sea realizada por un Usuario integrante de algún grupo de Personas en Situación de Vulnerabilidad.**

Vigente		Propuesta
	Sin correlativo.	**II. La Institución deberá poner a disposición del Usuario que presentó la Reclamación Monetaria, al menos cada 20 días hábiles, una actualización acerca del progreso de la investigación de la Reclamación Monetaria hasta que sea resuelta o ya no pueda ser procesada dentro de la Institución, a través de los canales que la Institución haya establecido en sus procedimientos para la atención de reclamaciones.**
	Sin correlativo.	**III. En el caso de Reclamaciones Monetarias que resultaron no procedentes para el Usuario, la Institución deberá contar con la evidencia y el detalle de los siguientes elementos mínimos, los cuales deberán estar a disposición de la Comisión o cualquier otra autoridad competente:**
	Sin correlativo.	**a) Monto Transaccional del Usuario, así como la información determinada por la institución respecto del monto, número, tipo, naturaleza, frecuencia y canales que comúnmente realiza el Usuario que presentó la Reclamación Monetaria.**
	Sin correlativo.	**b) Transaccionalidad declarada por el Usuario en la apertura de la cuenta, que entre otros incluya canales, periodicidad y monto de sus Operaciones Monetarias.**
	Sin correlativo.	**c) Reclamaciones Monetarias del Usuario que sean del conocimiento de la institución en los últimos 12 meses, señalando el medio o canal por el cual haya sido comunicado a la institución, y la fecha en que se registraron.**
	Sin correlativo.	**d) Evidencia del registro de la Reclamación Monetaria en sistemas o bitácoras de la institución.**
	Sin correlativo.	**e) Verificación de la legitimidad y apego al sistema de control interno de la institución, de las operaciones realizadas por la institución sobre la cuenta donde se realizó la Operación Monetaria, en los 90 días naturales anteriores a la fecha de la Reclamación Monetaria:** **i) Que se utilizaron los mecanismos y procedimientos de autenticación estipulados y regulatoriamente permitidos para realizar la transacción siempre que la Institución hubiere permitido al Usuario utilizar la categoría de Factor de Autenticación previsto en las presentes disposiciones y, no así, un Factor de Autenticación de una categoría menor a la antes referida.** **ii) Que se realizó de conformidad con los límites de monto pactados con el Usuario conforme al artículo 315 de las presentes disposiciones.**

Vigente		Propuesta
		iii) Que, si el monto de la Operación Monetaria reclamada es mayor al Monto Transaccional del Usuario, se verificaron los procedimientos estipulados en el artículo 287 Bis I de las presentes disposiciones. **iv) Que, para el caso de Reclamaciones Monetarias por Operaciones Monetarias realizadas a través de Banca Electrónica, el registro de las Cuentas Destino fue realizado acorde a la normativa aplicable, y que la Institución cumplió con la obligación de asegurarse de que sus clientes registraron en el servicio de Banca Electrónica de que se trate, las Cuentas Destino previamente a su uso, ya sea para ser utilizadas dentro del mismo servicio o, en otros servicios de Banca Electrónica.** **v) Que la generación de comprobantes y notificación de operaciones fue realizada de conformidad con el artículo 316 bis 1 de las presentes disposiciones y quedó registrado en la contabilidad de la Institución y hace fe en juicio de acuerdo con el artículo 100 de la Ley, sin que la Institución esté obligada a acreditar que el Usuario consultó el referido comprobante o notificación.** **vi) Alta o cambios en los datos de contacto, claves confidenciales, Factores de Autenticación o de beneficiarios, asociados a las cuentas afectadas.**
	Sin correlativo.	**f) Un resumen de los alertamientos generados en los últimos 30 días, por los sistemas de la Institución, asociados a las cuentas del Usuario, sean o no relativos a la Operación Monetaria asociada a la Reclamación Monetaria. En caso de no haber alertamientos en dicho periodo, deberá señalarse.**
	Sin correlativo.	**g) Gestiones realizadas con otras Instituciones para la devolución de recursos de la Operación Monetaria asociada a la Reclamación Monetaria, en su caso.**
	Sin correlativo.	**h) Si el Usuario pertenece a un grupo de Personas en Situación de Vulnerabilidad. En tal caso, en el diseño de recolección de los datos las Instituciones deberán señalar a los Usuarios que la declaración es de forma libre y voluntaria por lo que se contempla la opción de No responde.**

<table>
<tr><th colspan="2">Vigente</th><th>Propuesta</th></tr>
<tr><td></td><td>Sin correlativo.</td><td>i) Dictámenes o reportes operativos, técnicos, telefónicos, o de cualquier otra índole que genere la institución, con motivo de la Reclamación Monetaria.</td></tr>
<tr><td></td><td>Sin correlativo.</td><td>IV. En el caso de Reclamaciones Monetarias no procedentes para el Usuario, las Instituciones deberán incluir en la dictaminación de resolución una leyenda que especifique al Usuario que, en caso de que este no esté de acuerdo con la respuesta proporcionada por la Institución, puede iniciar una reclamación o queja ante las Unidades Especializadas de la Institución, y que también podrá iniciar de manera formal ante la Comisión Nacional de Protección y Defensa a los Usuarios de Servicios Financieros el procedimiento al que tienen derecho, detallando los canales y procedimientos para realizar la Reclamación Monetaria ante esa instancia.</td></tr>
<tr><td></td><td>Sin correlativo.</td><td>V. Las Instituciones deberán conservar por al menos cinco años los registros de todas las dictaminaciones de las Reclamaciones Monetarias, y documentación entregada al Publico Usuario que presenta la Reclamación Monetaria, para que puedan ser revisados por la Comisión o cualquier otra autoridad competente.</td></tr>
<tr><td></td><td>Sin correlativo.</td><td>El presente anexo no será obligatorio para aquellas reclamaciones presentadas a las Unidades Especializadas de las Instituciones, ni a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros en los términos de la Ley de Protección y Defensa al Usuario de Servicios Financieros</td></tr>
<tr><td></td><td>Anexo 36
Reportes regulatorios
Índice</td><td>Anexo 36
Reportes regulatorios
Índice</td></tr>
<tr><td></td><td>Serie R01 a Serie R26 . . .</td><td>Serie R01 a Serie R26 . . .</td></tr>
<tr><td></td><td></td><td>Serie R27 Reclamaciones Monetarias Periodicidad
<table><tr><td>A-2701</td><td>Reclamaciones Monetarias</td><td>Mensual</td></tr></table></td></tr>
<tr><td></td><td></td><td>Serie R28 a Serie R34 . . .</td></tr>
<tr><td></td><td></td><td><u>SERIE R01 CATÁLOGO MÍNIMO</u> a <u>SERIE R26 INFORMACIÓN POR COMISIONISTAS . . .</u></td></tr>
</table>

<table>
<tr><th>Vigente</th><th>Propuesta</th></tr>
<tr><td><u>SERIE R27 RECLAMACIONES</u></td><td><u>SERIE R27 RECLAMACIONES MONETARIAS</u></td></tr>
<tr><td>Esta serie se integra por un (1) reporte, cuya frecuencia de elaboración y presentación debe ser ~~trimestral~~.</td><td>Esta serie se integra por un (1) reporte, cuya frecuencia de elaboración y presentación debe ser mensual</td></tr>
<tr><td>REPORTE

A-2701 Reclamaciones

Este reporte solicita información de las ~~r~~eclamaciones ~~m~~onetarias de los ~~clientes, relacionadas con productos de captación y colocación,~~ especifica el canal transaccional de la operación. Asimismo, el reporte considera información respecto a los datos de la gestión de las reclamaciones ~~de los clientes~~. Para efectos de este reporte se entenderá por reclamación a todas aquellas operaciones monetarias no reconocidas por ~~los clientes~~ y que así lo han comunicado a la ~~i~~nstitución por cualquier canal o medio puesto a su disposición.</td><td>REPORTE

A-2701 Reclamaciones Monetarias

Este reporte solicita información de las Reclamaciones Monetarias del Usuario derivadas de operaciones activas y pasivas, especificando el canal transaccional de la operación. Asimismo, el reporte considera información respecto a los datos de la gestión de las reclamaciones del Usuario. Para efectos de este reporte se entenderá por reclamación a todas aquellas operaciones monetarias no reconocidas por el Usuario y que así lo han comunicado a la Institución por cualquier canal o medio puesto a su disposición.</td></tr>
<tr><td>FORMATO DE CAPTURA

Las instituciones llevarán a cabo el envío de la información relacionada con el reporte A-2701 Reclamaciones descrito anteriormente, mediante la utilización del siguiente formato de captura:</td><td>FORMATO DE CAPTURA

. . .</td></tr>
<tr><td>
<table>
<tr><th colspan="2">INFORMACIÓN SOLICITADA</th></tr>
<tr><td rowspan="4">SECCIÓN IDENTIFICADOR DEL REPORTE</td><td>PERIODO</td></tr>
<tr><td>CLAVE DE LA INSTITUCIÓN</td></tr>
<tr><td>REPORTE</td></tr>
<tr><td>~~NÚMERO DE SECUENCIA~~</td></tr>
<tr><td rowspan="2">~~SECCIÓN DATOS DE LA INSTITUCIÓN~~</td><td>~~FOLIO DE RECLAMACIÓN~~</td></tr>
<tr><td>~~FECHA DE RECLAMACIÓN~~</td></tr>
<tr><td rowspan="4">SECCIÓN DATOS DE LA RECLAMACIÓN</td><td>FECHA DE SUCESO</td></tr>
<tr><td>NÚMERO DE CUENTA/NÚMERO DE TDC/NÚMERO DE TDD/NÚMERO DE TPB</td></tr>
<tr><td>PRODUCTO</td></tr>
<tr><td>CANAL EN EL CUAL SE REALIZÓ LA TRANSACCIÓN NO RECONOCIDA</td></tr>
</table>
</td><td>
<table>
<tr><th colspan="2">INFORMACIÓN SOLICITADA</th></tr>
<tr><td rowspan="3">SECCIÓN IDENTIFICADOR DEL REPORTE</td><td>PERIODO</td></tr>
<tr><td>CLAVE DE LA INSTITUCIÓN</td></tr>
<tr><td>REPORTE</td></tr>
<tr><td rowspan="8">SECCIÓN DATOS DE LA RECLAMACIÓN</td><td>FECHA DE RECLAMACIÓN</td></tr>
<tr><td>ORIGEN DE LA RECLAMACIÓN</td></tr>
<tr><td>FECHA DE SUCESO</td></tr>
<tr><td>ESTADO DONDE SE ORIGINÓ LA RECLAMACIÓN MONETARIA</td></tr>
<tr><td>MUNICIPIO DONDE SE ORIGINÓ LA RECLAMACIÓN MONETARIA</td></tr>
<tr><td>RFC DEL CLIENTE</td></tr>
<tr><td>CURP DEL CLIENTE</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Vigente</th><th>Propuesta</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>MOTIVO DE LA RECLAMACIÓN</td></tr>
<tr><td></td><td>~~IMPORTE RECLAMADO~~</td></tr>
<tr><td></td><td>ESTADO DE LA RECLAMACIÓN</td></tr>
<tr><td>SECCIÓN DATOS DE LA RESOLUCIÓN</td><td>RESOLUCIÓN</td></tr>
<tr><td></td><td>FECHA DE RESOLUCIÓN</td></tr>
<tr><td></td><td>CAUSA DE RESOLUCIÓN</td></tr>
<tr><td></td><td>IMPORTE ABONADO AL CLIENTE</td></tr>
<tr><td></td><td>FECHA DE ABONO AL CLIENTE</td></tr>
<tr><td></td><td>IMPORTE RECUPERADO</td></tr>
<tr><td></td><td>QUEBRANTO PARA LA INSTITUCIÓN</td></tr>
<tr><td></td><td>ORIGEN DE LA RECLAMACIÓN</td></tr>
</table>
</td><td>
<table>
<tr><td></td><td>PERSONA FÍSICA O MORAL</td></tr>
<tr><td></td><td>NÚMERO DE CUENTA/NÚMERO DE TDC/NÚMERO DE TDD/NÚMERO DE TPB</td></tr>
<tr><td></td><td>PERSONA EN SITUACIÓN DE VULNERABILIDAD</td></tr>
<tr><td></td><td>MONTO TRANSACCIONAL DEL USUARIO</td></tr>
<tr><td></td><td>USO DE FACTOR DE AUTENTICACIÓN Y CATEGORÍA</td></tr>
<tr><td></td><td>USO DE FACTOR DE AUTENTICACIÓN Y CATEGORÍA CUANDO SE SUPERA EL MONTO TRANSACCIONAL DEL USUARIO</td></tr>
<tr><td></td><td>PRODUCTO</td></tr>
<tr><td></td><td>IDENTIFICADOR DE INSTITUCION, COMISIONISTA O COMERCIO DONDE SE REALIZA LA OPERACION</td></tr>
<tr><td></td><td>NOMBRE DEL ADQUIRIENTE EN CASO DE OERACIONES EN TPV</td></tr>
<tr><td></td><td>CANAL EN EL CUAL SE REALIZÓ LA TRANSACCIÓN</td></tr>
<tr><td></td><td>MOTIVO DE LA RECLAMACIÓN</td></tr>
<tr><td></td><td>TRANSACCIÓN CON TECNOLOGÍA DE PAGO SIN CONTACTO</td></tr>
<tr><td></td><td>MONTO DE LA RECLAMACIÓN MONETARIA</td></tr>
<tr><td></td><td>ESTADO DE LA RECLAMACIÓN</td></tr>
<tr><td>SECCIÓN DATOS DE LA RESOLUCIÓN</td><td>RESOLUCIÓN</td></tr>
<tr><td></td><td>FECHA DE RESOLUCIÓN</td></tr>
<tr><td></td><td>CAUSA DE RESOLUCIÓN</td></tr>
<tr><td></td><td>IMPORTE ABONADO AL CLIENTE</td></tr>
<tr><td></td><td>FECHA DE ABONO AL CLIENTE</td></tr>
<tr><td></td><td>IMPORTE RECUPERADO</td></tr>
<tr><td></td><td>MEDIO POR EL CUAL SE RECUPERO EL IMPORTE</td></tr>
<tr><td></td><td>QUEBRANTO PARA LA INSTITUCIÓN</td></tr>
<tr><td>SECCIÓN DATOS DEL FRAUDE</td><td>CONDUCTA OBSERVABLE DE GESTIÓN DEL FRAUDE</td></tr>
</table>
</td></tr>
<tr><td></td><td>Las instituciones reportarán la información que se indica en la presente serie, la cual deberá cumplir con las validaciones y estándares de calidad que indique la ~~Comisión Nacional Bancaria y de Valores~~ (Comisión)~~,~~ ajustándose a las características y especificaciones que para efectos de llenado y envío de información se presentan en los instructivos de llenado, los cuales se publican y actualizan en el ~~Sistema Interinstitucional de Transferencia de Información~~ (SITI)~~ o en el que en su caso, dé a conocer la Comisión. Una vez superadas las</td><td>Las Instituciones reportarán la información que se indica en la presente serie, la cual deberá cumplir con las validaciones y estándares de calidad que indique la Comisión, ajustándose a las características y especificaciones que, para efectos de llenado y envío de información, se presentan en los instructivos de llenado, los cuales se publican y actualizan en el SITI o en el que, en su caso, dé a conocer la Comisión. Una vez</td></tr>
</table>

Vigente		Propuesta
	validaciones y estándares de calidad, el SITI generará un acuse de recibo electrónico. La información~~,~~ deberá enviarse una sola vez y se recibirá asumiendo que reúne todas las características y especificaciones, en virtud de lo cual no podrá ser modificada y deberá presentar consistencia con los diversos reportes en los que se incluya la misma información con un nivel distinto de integración, por lo que, de no reunir la calidad y características exigibles o haber sido presentada de forma incompleta, se considerará como no cumplida la obligación de su presentación y, en consecuencia, se procederá a la imposición de las sanciones correspondientes de conformidad con las disposiciones legales que resulten aplicables.	superadas las validaciones y estándares de calidad, el SITI generará un acuse de recibo electrónico. La información deberá enviarse una sola vez y se recibirá asumiendo que reúne todas las características y especificaciones, en virtud de lo cual no podrá ser modificada y deberá presentar consistencia con los diversos reportes en los que se incluya la misma información con un nivel distinto de integración, por lo que, de no reunir la calidad y características exigibles o haber sido presentada de forma incompleta, se considerará como no cumplida la obligación de su presentación y, en consecuencia, se procederá a la imposición de las sanciones correspondientes de conformidad con las disposiciones legales que resulten aplicables. **SERIE R28 INFORMACIÓN DE RIESGO OPERACIONAL** a **SERIE R36 PAGOS ANTICIPADOS** . . .