COMISIÓN PARA EL MERCADO FINANCIERO

Informe para consulta pública

Ajustes y modificaciones a los archivos D05, D42, D43, I06, I11 e I12 del MSI para Bancos

2026

www.CMFChile.cl

Contenido

I. INTRODUCCIÓN 3

II. DIAGNÓSTICO 4

II.1. Archivos D42 y D43 4

II.2. Archivos I06 e I11 5

II.3. Archivo I12 6

II.4. Archivo D05 6

III. OBJETIVO DE LA PROPUESTA NORMATIVA 7

IV. PROPUESTA NORMATIVA 8

IV.1. Ajustes al sistema de deudores 8

IV.2. Ajustes al sistema de instituciones 9

IV.3. Ajustes a las tablas del MSI de bancos 14

IV.4. Ajustes a los Antecedentes Generales del MSI de bancos 19

V. ANÁLISIS DE IMPACTO REGULATORIO 19

VI. REFERENCIAS 20

VII. ANEXOS 21

I. INTRODUCCIÓN

En el marco de su labor supervisora y fiscalizadora, y considerando las facultades otorgadas por el artículo 5 del Decreto Ley N°3.538 de 1980, la Comisión para el Mercado Financiero (en adelante, CMF o Comisión) realiza solicitudes de información periódica a sus distintos supervisados. Estos requerimientos son realizados mediante archivos normativos, cuyas instrucciones de preparación y entrega se encuentran principalmente contenidas en distintos Manuales del Sistema de Información (MSI).

Por otra parte, la Circular N°2.348 de 15 de mayo de 2024, ajustó el Capítulo 18-3 de la Recopilación Actualizada de Normas (RAN) de bancos, para distinguir la forma de modificar parámetros y aspectos técnicos de los archivos normativos. En este tenor, el Capítulo 18-3 de la RAN de bancos establece que las modificaciones a las instrucciones de los archivos deberán ser realizadas mediante Circulares o Normas de Carácter General, según corresponda. Por otro lado, los ajustes de carácter técnico deberán llevarse cabo a través de Oficios Circulares.

Considerando lo anterior, este proyecto realiza ajustes técnicos al archivo D05 "Deudores de operaciones transfronterizas" y modifica los archivos D42 "Créditos para la vivienda con subsidio", D43 "Remates y cesiones en pago de viviendas subsidiadas", I06 "Oficinas, personal, horarios de atención y cajeros automáticos", I11 "Parque de cajeros automáticos y tiempos de indisponibilidad o *Downtime*" e I12 "Incidentes de Ciberseguridad" del Manual de Sistema de Información (MSI) para bancos.

Los archivos D42 y D43 fueron, ambos, creados mediante la Carta Circular Manual de Sistema Información N°7 de 26 de febrero de 2007. Si bien ambos archivos guardan relación con viviendas subsidiadas, el archivo D42 fue concebido con la finalidad de obtener información específica de los créditos hipotecarios para vivienda asociados a programas habitacionales y de subsidio. Por su parte el archivo D43 tenía por finalidad abastecer a la Comisión con información estadística sobre las viviendas rematadas o recibidas en pago cuyo valor no superase las 1.000 UF, monto que se ampliaría hasta 2.000 UF a través de la Carta Circular N°5 de 26 de mayo de 2014.

El archivo I06, creado mediante la Carta Circular Manual Sistema Información N°7 de 21 de noviembre de 2006, nace con la finalidad de obtener información más detallada sobre oficinas, personal y cajeros automáticos que la que entregaba el hasta entonces vigente archivo I04 "Personal, oficinas y cajeros automáticos". La Carta Circular anteriormente indicada fijó el primer envío del archivo I06 para abril de 2007, así como también estableció que el archivo I04 dejaría de entregarse, mas no definió una fecha concreta para este hito[1].

[1] Finalmente, el archivo I04 fue derogado el 7 de febrero de 2008, y su exigencia de envío fue suprimida a través de la Carta Circular Manual del Sistema de Información N°5/2008.

Por su parte, el 17 de marzo de 2015, la Superintendencia de Bancos e Instituciones Financieras (ex SBIF) emitió la Circular N°3.578, la cual incorporó en el Capítulo 1-7 de la RAN de Bancos, un requerimiento de información mediante el que se instruye a las instituciones bancarias mantener sistemas de información que les permitan generar estadísticas del funcionamiento de su red de cajeros automáticos. En dicho tenor, la ex SBIF publicó la Carta Circular Manual Sistema Información N°2 de 2015, que creó el archivo I11 con el objetivo de poner a su disposición información sobre el funcionamiento de los cajeros automáticos de las instituciones bancarias, de acuerdo con lo establecido en el Capítulo 1-7 de la RAN de bancos.

Finalmente, a través de la Carta Circular Manual Sistema Información N°6 de 18 de diciembre de 2018, y con el propósito de contar con una mejor información referida a los incidentes de ciberseguridad y reforzar la sistematización de esta, la ex SBIF da origen al archivo I12. En esta línea, el archivo requiere que las entidades obligadas a informar identifiquen los incidentes de ciberseguridad, hayan sido materializados o no. Cabe señalar que la obligación de remitir el archivo I12 también se extiende a cooperativas de ahorro y crédito[2] (CACs), sociedades de apoyo al giro[3] (SAGs), emisores de tarjetas de pago[4], y operadores de tarjetas de pago[5]. Adicionalmente, la NCG N°514 que regula el Sistema de Finanzas Abiertas (SFA) establece a sus regulados el envío mensual de este archivo normativo[6].

Las siguientes secciones del presente informe se distribuyen de la siguiente manera: II. realiza un diagnóstico de los archivos que contempla este proyecto normativo; III. expone los objetivos de la propuesta normativa; IV. presenta la propuesta normativa; y V. desarrolla sobre el impacto esperado de la propuesta normativa.

II. DIAGNÓSTICO

II.1. Archivos D42 y D43

Esta Comisión solicita información referente a créditos, remates y cesiones en pago de viviendas asociadas a programas habitacionales y de subsidio a través de los archivos D42 y D43, identificando el programa habitacional y de subsidio al que pertenece la vivienda y, también, el tramo del valor de la vivienda.

---

[2] Ver el Catálogo de Archivos del Sistema de Información del MSI CACs (Link).
[3] Ver el Anexo N°1 de la Circular N°23 para SAGs (Link).
[4] Ver el Anexo N°5 de la Circular N°1 para emisores de tarjetas de pago (Link).
[5] Ver el Anexo N°4 de la Circular N°1 para operadores de tarjetas de pago (Link).
[6] El título VIII.A del Anexo N°3 del texto refundido de la NCG N°514 establece lo siguiente: *"Las entidades, además de comunicar los incidentes del SFA a través de la plataforma Reporte de Incidentes Operacionales (RIO), deberán remitir mensualmente el archivo I12 "Incidentes de Ciberseguridad", del Manual de Sistema de Información.".*

Actualmente, ninguno de los dos archivos cuenta con una periodicidad definida, pues deben remitirse cada vez que la CMF los solicite. Por otro lado, en el desempeño de sus funciones, esta Comisión ha detectado que el campo 05 "Programa habitacional y de subsidio" del archivo D42 y el campo 03 "Tramo del valor original de la vivienda en UF" se encuentran desactualizados con respecto a los tipos de programas existentes y los valores de las viviendas asociadas a estos.

Considerando lo anterior y velando por la mejor completitud de la información de los archivos D42 y D43, esta Comisión estima necesario, actualizar los archivos indicados de acuerdo con las disposiciones vigentes con respecto a este tipo de programas, además de establecer un envío regular para ambos archivos.

II.2. Archivos I06 e I11

Las sucursales bancarias y cajeros automáticos, al facilitar el acceso a servicios bancarios formales, desempeñan un papel fundamental en la inclusión financiera. Por una parte, las sucursales ofrecen atención personalizada y asesoría financiera, lo cual es clave para generar confianza y educación financiera entre los usuarios (Allen et al, 2016; Carlander et al, 2018; Dolata et al, 2019; Maity & Sahu, 2022). Por otro lado, los cajeros automáticos facilitan operaciones básicas como retiros, consultas de saldo y transferencias, incluso en zonas rurales o de difícil acceso, reduciendo barreras geográficas y de horario (Whelan, 2012; Allen et al, 2016; Maity & Sahu, 2022).

Actualmente, la Comisión solicita información sobre oficinas y cajeros automáticos mediante los archivos I06 e I11. En particular, el archivo I06 cuenta con siete registros, de los cuales los seis primeros permiten caracterizar individualmente las diferentes oficinas de las entidades obligadas, mientras que el séptimo refiere a información agregada por comuna sobre cajeros automáticos. Por su parte, el archivo I11, compuesto por tres registros, provee a esta Comisión información individual de los cajeros automáticos de las entidades y sus tiempos e índices de indisponibilidad.

La ubicación de oficinas y sucursales, en el contexto de inclusión financiera, permiten identificar barreras geográficas que puedan existir en la disponibilidad a los servicios financieros que prestan ambas figuras. En esta línea, el primer registro de los archivos I06 e I11 identifica individualmente las oficinas y cajeros automáticos junto con su ubicación, la cual, hasta ahora, ha sido capturada a través de campos que identifican la comuna en la cual se encuentra ubicada la oficina o cajero. Sin embargo, los desarrollos en los sistemas de georreferencia permiten acceder a información más precisa que la obtenida mediante el reporte de la comuna de la sucursal o cajero.

Considerando lo anterior, el uso de coordenadas (latitud y longitud) presenta diversas ventajas, siendo la más relevante su mayor precisión geográfica. Esta información, no solo permite monitorear la operatividad del sistema, sino que también es útil para evaluar su impacto en la inclusión financiera. En este sentido

diversos estudios documentan cómo la proximidad geográfica a servicios financieros, constituye un determinante clave de la inclusión financiera (Brown et al, 2014; Cámara & Tuesta, 2014; Pino & Valdebenito, 2022).

II.3. Archivo I12

Con la finalidad de contar con una base consolidada de los eventos experimentados por entidades obligadas y que permita, además, realizar seguimiento de dichos incidentes, la CMF les exige a bancos, CACs, SAGs, emisores y operadores de tarjetas de pago e instituciones reguladas por la NCG N° 514 el envío del archivo I12 "Incidentes de Ciberseguridad".

El archivo I12 establece la obligación de reportar mensualmente los incidentes y alertas de Ciberseguridad y mantener un seguimiento de tales situaciones en el tiempo, para identificar tipos de vulnerabilidades y amenazas, activos de información e infraestructura potencialmente afectados, la cuantificación de los clientes afectados y los costos involucrados, entre otros factores que permiten caracterizar los incidentes y alertas.

Considerando lo anterior, en el desarrollo de sus funciones esta Comisión ha detectado oportunidades de mejora para el archivo I12 en tres términos. En primer lugar, las definiciones de incidentes y alertas de los registros 1 y 2 del archivo da espacio a interpretaciones de qué debe ser considerado un incidente o una alerta. En segundo lugar, el actual archivo no permite identificar algunas fechas y horas relevantes dentro del desarrollo del incidente, como lo son las fechas y horas de escalamiento, envío de Reporte de Incidente Operacional (RIO) a la CMF y de inicio de acciones de mitigación. Finalmente, las instrucciones de reporte vigente de los campos que permiten identificar el tipo de vulnerabilidad, amenaza, activos de información involucrados y canales, productos y servicios potencialmente afectados solo permiten informar una única categoría por campo, desconociendo la multidimensionalidad que pueden presentar los incidentes de Ciberseguridad. En este sentido, el reporte actual no permite caracterizar de forma íntegra los distintos incidentes informados en el archivo.

Por último, con la publicación de la Ley N°21.663 Ley Marco de Ciberseguridad, resulta preciso actualizar el archivo I12 en concordancia con las definiciones expuestas en dicha Ley.

II.4. Archivo D05

Con la finalidad de proteger la idoneidad de la información de instrumentos que tienen un plazo de vencimiento de 10.000 días o más, y ante consultas de la industria, esta Comisión estima pertinente modificar el largo del campo 17 "Plazo residual de la operación" de este archivo.

III. OBJETIVO DE LA PROPUESTA NORMATIVA

La presente propuesta normativa tiene por objetivo actualizar los archivos D05, D42, D43, I06, I11 e I12 en concordancia con las nuevas tecnologías y disposiciones aplicables, según corresponda. Lo anterior, con la finalidad de resguardar la idoneidad de la información recibida mediante dichos requerimientos de información.

La Comisión, mediante la modificación de los archivos señalados, busca cumplir con los siguientes objetivos específicos (Tabla 1).

Tabla 1: Objetivo de las modificaciones

Archivo normativo	Objetivo del cambio	Campos involucrados
D05	• Permitir el reporte de operaciones con plazos superiores o iguales a 10.000 días. • Ajustes formales.	(17) PLAZO RESIDUAL DE LA OPERACIÓN.
D42	• Ajustar periodicidad. • Actualizar la lista de los programas habitacionales y de subsidios posibles. • Ajustes formales.	(5) PROGRAMA HABITACIONAL Y DE SUBSIDIO.
D43	• Ajustar periodicidad y plazo. • Actualizar los rangos de valores de viviendas al momento del crédito original. • Ajustes formales.	(3) TRAMO DEL VALOR ORIGINAL DE LA VIVIENDA EN UF.
I06	• Agregar coordenadas para identificar la localización de sucursales, para la generación de indicadores de inclusión financiera. • Ajustes formales.	Nuevos campos (15) LATITUD y (16) LONGITUD en el registro 1.
I11	• Ídem I06.	Nuevos campos (11) LATITUD y (12) LONGITUD en el registro 1.
I12	• Actualizar la información requerida respecto de incidentes de Ciberseguridad, para favorecer el monitoreo de	Se modifican los campos (10) TIPO DE VULNERABILIDAD, (11) TIPO DE AMENAZA, (12) TIPO DE ACTIVOS DE INFORMACIÓN INVOLUCRADOS y (13) TIPO DE

	los incidentes operacionales de Ciberseguridad por parte de la Comisión. • Actualizar descripción del archivo. • Ajustar periodicidad. • Ajustes formales.	CANALES, PRODUCTOS O SERVICIOS INVOLUCRADOS y (21) NIVEL DE CRITICIDAD. Se agregan los siguientes campos al registro 1 del archivo: (22) FECHA DE ESCALAMIENTO, (23) HORA DE ESCALAMIENTO, (24) FECHA DE REPORTE A LA CMF, (25) HORA DE REPORTE A LA CMF, (26) FECHA DE INICIO DE ACCIONES DE MITIGACIÓN, (27) HORA DE INICIO DE ACCIONES DE MITIGACIÓN; (28) TIPOS DE ACCIONES REALIZADAS, (29) TIPOS DE PLATAFORMAS INVOLUCRADAS y (30) TIPOS DE COMPROMISOS. Se añade el campo (8) TIPOS DE COMPROMISOS al registro 2.
Tablas	• Actualizar la taxonomía relacionada a incidentes de ciberseguridad.	Tablas 95, 96, 97, 99, 100 y 102 del MSI Bancos. Nuevas Tablas 128 "Tipo de compromisos o consecuencias" y 129 "Nivel de criticidad".
Antecedentes generales	• Ajustar en concordancia con los ajustes propuestos a los archivos D42 y D43.	

Fuente: CMF.

IV. PROPUESTA NORMATIVA

La propuesta normativa realiza modificaciones a archivos del sistema de deudores e instituciones y a las Tablas del MSI de bancos. A continuación, se presenta un resumen de los ajustes que busca realizar la presente propuesta normativa. El detalle de estos ajustes puede encontrarse en la Circular propuesta, anexa a este informe.

IV.1. Ajustes al sistema de deudores

a) Modificaciones al archivo D05 "Deudores de operaciones transfronterizas"

1. Se realiza el ajuste técnico en el archivo, donde se modifica el largo del campo 17 PLAZO RESIDUAL DE LA OPERACIÓN, pasando de 4 a 5 bytes. Lo anterior, con la finalidad de permitir el reporte de operaciones con plazos

iguales o superiores a 10.000 días.

2. En concordancia con el ajuste anterior, se ajusta el largo total del registro único del archivo de 324 a 325 bytes.

3. Se realizan otros ajustes formales.

b) Modificaciones al archivo D42 "Créditos para la vivienda con subsidio"

4. Con el objetivo de obtener la información a la que se refiere el archivo de manera periódica, se reemplaza la periodicidad "A pedido" por "Trimestral".

5. Se modifica la definición del campo 05 PROGRAMA HABITACIONAL Y DE SUBSIDIO para añadir el programa de subsidio establecido en el Decreto Supremo N°19 del 2016 y el programa de habitabilidad rural (DS10) a la codificación permitida en dicho campo, los cuales son incorporados bajo los códigos 13 y 14, respectivamente.

c) Modificaciones al archivo D43 "Remates y cesiones en pago de viviendas subsidiadas"

6. Con el objetivo de obtener la información a la que refiere el archivo de manera periódica, se reemplaza la periodicidad "A pedido" por "Trimestral".

7. Se reemplaza el plazo "Según lo solicitado en cada oportunidad" por "15 días hábiles".

8. Se elimina la expresión "y cuyo valor no supere las 2.000 UF" de la descripción del archivo.

9. Se cambia el nombre del campo 01 PERIODO DE LA TRANSFERENCIA por AÑO DE LA TRANSFERENCIA. En consistencia, se reemplaza la palabra "periodo" por "año" en la definición del campo.

10. Se modifica la definición del campo 03 TRAMO DEL VALOR ORIGINAL DE LA VIVIENDA EN UF para incorporar los tramos "Más de 2.000 UF hasta 3.000 UF", "Más de 3.000 UF hasta 4.000 UF" y "Más de 4.000 UF" a la codificación de tramos permitida en el campo, los cuales son incorporados bajo los códigos 06, 07 y 08, respectivamente.

11. Se realizan otros ajustes formales.

IV.2. Ajustes al sistema de instituciones

a) Ajustes al archivo I06 "Oficinas, personal, horarios de atención y cajeros automáticos"

12. Se agrega al registro 1 del archivo el campo 15 LATITUD, formato

s9(02)V9(06), con la siguiente definición:

"*Coordenada geográfica que indica la posición norte-sur de la ubicación de la oficina, medida en grados decimales. El formato corresponde a un número decimal con 6 decimales. Valores negativos indican ubicaciones en el hemisferio sur.*"

13. Se agrega al registro 1 del archivo el campo 16 LONGITUD, formato s9(03)V9(06), con la siguiente definición:

    "*Coordenada geográfica que indica la posición este-oeste de la ubicación de la oficina, medida en grados decimales. El formato corresponde a un número decimal con 6 decimales. Valores negativos indican ubicaciones en el hemisferio occidental.*"

14. En consideración a las modificaciones anteriores, se ajusta el largo del registro 1 del archivo a 173 bytes. En concordancia, se ajustan el largo de los *fillers* y el largo total de los demás registros.

15. Se realizan otros ajustes formales.

b) Ajustes al archivo I11 "Parque de cajeros automáticos y tiempos de indisponibilidad o *Downtime*"

16. Se agrega al registro 1 del archivo el campo 11 LATITUD, formato s9(02)V9(06), con la siguiente definición:

    "*Coordenada geográfica que indica la posición norte-sur de la ubicación del cajero automático, medida en grados decimales. El formato corresponde a un número decimal con 6 decimales. Valores negativos indican ubicaciones en el hemisferio sur*."

17. Se agrega al registro 1 del archivo el campo 12 LONGITUD, formato s9(03)V9(06), con la siguiente definición:

    "*Coordenada geográfica que indica la posición este-oeste de la ubicación de la del cajero automático, medida en grados decimales. El formato corresponde a un número decimal con 6 decimales. Valores negativos indican ubicaciones en el hemisferio occidental.*"

18. En consideración a las modificaciones anteriores, se ajusta el largo del registro 1 del archivo a 117 bytes. En concordancia, se ajustan el largo de los *fillers* y el largo total de los demás registros.

A modo de ejemplo para los cambios indicados en los números 12, 13, 16 y 17, si la ubicación a reportar es Paralelo 33.44167077866651 Sur (S) y Meridiano 70.65128404991411 Oeste (W), deberá reportarse en los archivos -33,441671 en LATITUD y -70,651284 en LONGITUD.

c) Ajustes al archivo I12 "Incidentes de Ciberseguridad"

19. Se intercala la frase "y Alertas" entre las palabras "Incidentes" y la expresión "de Ciberseguridad" en el nombre del archivo.

20. Se modifica la periodicidad del archivo de Mensual a "Trimestral".

21. Se ajusta la descripción del archivo para actualizar la definición de "incidente" en concordancia con la definición de "Incidente de Ciberseguridad" contenida en el artículo 2 de la Ley N°21.663.

22. Se ajusta la descripción de los registros 1 para incidentes y 2 para alertas, con el fin de precisar un criterio único y taxativo para restringir la interpretación de los términos del reporte. Lo anterior para que los incidentes no consideren criterios internos como justificación para omitir el reporte de un incidente o alerta, tales como su naturaleza, volumen de afectación, duración, tipo de activos involucrados, entre otros.

23. Se realizan las siguientes modificaciones al registro 1 del archivo:

i) Se cambian los nombres de los campos 06 FECHA DEL REPORTE y 07 HORA DEL REPORTE por FECHA DE DETECCIÓN y HORA DE DETECCIÓN, respectivamente.

ii) Se hacen ajustes a la definición del campo 09 HORA DE LA MITIGACIÓN.

iii) Se modifican las definiciones y los largos de los campos 10 TIPO DE VULNERABILIDAD; 11 TIPO DE AMENAZA; 12 TIPO DE ACTIVOS DE INFORMACIÓN INVOLUCRADOS; y 13 TIPOS DE CANALES, PRODUCTOS O SERVICIOS INVOLUCRADOS, para permitir el reporte de más de un código dentro de un mismo registro.

iv) En concordancia con el ajuste anterior, se modifica el largo de los campos señalados, según corresponda, y se ajustan los nombres de los mismos para que su denominación sea plural.

v) Se reemplaza la definición del campo 21 NIVEL DE CRITICIDAD por la siguiente:

"*Se debe indicar para cada incidente el nivel de criticidad, entendido como el impacto en términos de ciberseguridad de acuerdo con la codificación indicada en la Tabla 129 "Nivel de criticidad". En caso de que el incidente informado presente simultáneamente características asociadas a más de un nivel de criticidad, se debe informar el código vinculado al nivel de mayor criticidad.*"

vi) Se añade el nuevo campo 22 FECHA DE ESCALAMIENTO, formato F(08), con la siguiente definición

"*Corresponde indicar la fecha (AAAAMMDD) en la que la situación fue comunicada al Equipo de Respuesta a Incidentes de la entidad.*"

vii) Se agrega el nuevo campo 23 HORA DE ESCALAMIENTO, formato 9(06), cuya definición es la siguiente:

"*Corresponde indicar la hora (HHMMSS) en la que la situación fue comunicada al Equipo de Respuesta a Incidentes de la entidad (formato de 24 hrs.).*"

viii) Se incorpora el nuevo campo 24 FECHA DE REPORTE A LA CMF, formato F(08), con la siguiente definición:

"Corresponde informar la fecha (AAAAMMDD) en la que el incidente fue informado a la Comisión a través de los canales y mecanismos dispuestos para tal efecto en el Reporte de Incidentes Operacionales (RIO) de la CMF. En caso de que el incidente no haya sido informado a la Comisión, el campo debe completarse con "19000101"."

ix) Se incluye el nuevo campo 25 HORA DE REPORTE A LA CMF, formato 9(06), definido como se muestra a continuación:

"Corresponde informar la hora (HHMMSS) en la que el incidente fue informado a la Comisión a través de los canales y mecanismos dispuestos para tal efecto, en formato de 24 hrs, en el Reporte de Incidentes Operacionales (RIO) de la CMF. En caso de que el incidente no haya sido informado a la Comisión, el campo se debe completar con nueves ("999999")."

x) Se agrega el nuevo campo 26 FECHA DE INICIO DE ACCIONES DE MITIGACIÓN, formato F(08), cuya definición es la siguiente:

"Corresponde informar la fecha (AAAAMMDD) en la que la entidad financiera da inicio al proceso o a las acciones de mitigación."

xi) Se añade el nuevo campo 27 HORA DE INICIO DE ACCIONES DE MITIGACIÓN, formato 9(06), con la siguiente definición:

"Corresponde informar la hora (HHMMSS) en la que la entidad financiera da inicio al proceso o a las acciones de mitigación (formato de 24 hrs.)."

xii) Se introduce el nuevo campo 28 TIPOS DE ACCIONES REALIZADAS, formato 9(36), con la siguiente definición:

"*Se deberán informar las acciones realizadas para gestionar el incidente, de acuerdo con los códigos establecidos en la Tabla 102 "Tipo de acción realizada".*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla

102. En cada posición se deberá consignar el código correspondiente cuando la acción haya sido realizada, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si las acciones realizadas corresponden a los códigos 04, 13 y 15, se deberá informar "000000040000000000001300150000000000". Si únicamente se realizó la acción identificada con el código 13, se deberá informar "000000000000000000001300000000000000"."

xiii) Se agrega el nuevo campo 29 TIPOS DE PLATAFORMAS INVOLUCRADAS, formato 9(26), con la siguiente definición:

"*Se deberán informar las plataformas informáticas afectadas por el incidente, de acuerdo con los códigos establecidos en la Tabla 100 "Tipo de plataforma informática".*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 100. En cada posición se deberá consignar el código correspondiente cuando la plataforma informática haya sido afectada, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si las plataformas informáticas afectadas corresponden a los códigos 02, 05 y 12, se deberá informar "00020000050000000000120000". Si únicamente resulta afectada la plataforma identificada con el código 13, se deberá informar "00000000000000000000001300"."

xiv) Se añade el nuevo campo 30 TIPOS DE COMPROMISOS, formato 9(22), con la siguiente definición:

"Se deberán informar los tipos de compromisos derivados del incidente, de acuerdo con los códigos establecidos en la Tabla 128 "Tipos de compromisos".

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 128. En cada posición se deberá consignar el código correspondiente cuando el tipo de compromiso sea aplicable, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si los tipos de compromisos identificados corresponden a los códigos 02, 05 y 11, se deberá informar "00020000050000000000011". Si únicamente resulta aplicable el código 11, se deberá informar "00000000000000000000011"."

La Tabla 2 indica los campos multidimensionales del registro 1 del archivo I12 (campo, nombre, n° de alternativas (totales), n° alternativas a seleccionar (hasta), tabla de referencia).

Tabla 2: Campos multidimensionales del archivo I12

N° del campo	Nombre del campo	N° de alternativas totales	N° de alternativas a seleccionar	N° Tabla MSI de referencia
10	Tipos de vulnerabilidades	10	3	95
11	Tipos de amenazas	11	3	96
12	Tipos de activos de información involucrados	21	21	97
13	Tipos de canales, productos o servicios involucrados	20	20	98
28	Tipos de acciones realizadas	18	18	102
29	Tipos de plataformas involucradas	13	13	100
30	Tipos de compromisos	11	11	128

Fuente: CMF.

24. Se realizan las siguientes modificaciones al registro 2 del archivo:

    i) Se eliminan los campos 05 PLATAFORMA INVOLUCRADA, 06 NATURALEZA DE LA AMENAZA y 07 ACCIONES REALIZADAS.

    ii) Se actualiza la definición del campo 03 ORIGEN DE LOS DATOS, indicando nuevos orígenes más granulares.

    iii) Se agrega el nuevo campo 05 PERIODO DE LAS ALERTAS, con la siguiente definición:

    "*Corresponde informar el mes (AAAAMM) al cual se refiere la información de las alertas reportadas en este registro.*"

25. Considerando las modificaciones anteriores, se ajustan los largos de los dos registros del archivo a 410 bytes y se aumenta el largo del *filler* del segundo registro a 385 bytes.

26. Se realizan ajustes formales y de institucionalidad.

IV.3. Ajustes a las tablas del MSI de bancos

27. Se agrega la Tabla 128 "Tipos de compromisos" al catálogo de tablas, con lo siguientes códigos y glosas:

"***Tabla 128: Tipos de compromisos***

Código	***Tipo de compromiso***
01	***Uso no autorizado de redes y sistemas informáticos:*** *Uso no autorizado de sistemas de la institución afectada, ya sea a*

	través de explotación de vulnerabilidades, uso no autorizado de credenciales, acceso a almacenamiento en nube, u otros.
02	***Actividades de phishing o fraude en infraestructura propia:*** *Envío de phishing a través de servidores de la institución afectada, o almacenamiento de sitios fraudulentos en redes y sistemas informáticos de la institución afectada.*
03	***Actividades de phishing o fraude relacionadas con la institución:*** *Envío de phishing relacionado con la institución afectada por parte de terceros, o almacenamiento de sitios fraudulentos por parte de terceros.*
04	***Ejecución no autorizada de código:*** *Inclusión y ejecución no autorizada de código en sistemas de la institución afectada.*
05	***Exfiltración y/o exposición de datos:*** *Pérdida de información confidencial con o sin divulgación pública, y/o información confidencial expuesta accidental o intencionalmente.*
06	***Exfiltración y/o exposición de configuraciones:*** *Pérdida o exposición accidental de configuraciones y parámetros confidenciales de un sistema o aplicación de la institución afectada.*
07	***Exfiltración y/o exposición de código fuente:*** *Pérdida o exposición excesiva del código fuente de un sistema de la institución afectada.*
08	***Indisponibilidad y/o denegación de servicio:*** *Pérdida total del funcionamiento de un servicio, sistema o servidor, o saturación de red impidiendo su operación normal.*
09	***Degradación de servicio:*** *Pérdida parcial del rendimiento o funcionalidad de un servicio, sistema o servidor.*
10	***Modificación no autorizada de datos:*** *Alteración no autorizada de información contenida en sistemas, servicios o servidores.*
11	***Manipulación no autorizada de configuración:*** *Cambio no autorizado de configuraciones en sistemas, servicios o servidores.*

”

28. Se añade la Tabla 129 “Nivel de criticidad” al catálogo de tablas, considerando la siguiente codificación:

“***Tabla 129: Nivel de criticidad***

Código	***Nivel de criticidad***	***Características (debe cumplirse al menos una de las condiciones para calificar en el nivel)***
1	*Menor*	• *Afectación de algún sistema de información no crítico y con mecanismos de contingencia probados y efectivos.* • *No tiene efectos en la entrega de servicios o en las operaciones.* • *Tiene un impacto social menor o nulo.* • *Sin impacto contractual, legal o regulatorio.* *Generalmente estas situaciones no tienen efectos negativos, excepto el registro, chequeo de salud de sistemas y la revisión correlacionada con eventos de similar naturaleza, recurrentes en el tiempo.*

2	*Baja*	• *Afectación comprobada de algún sistema de información productivo, no crítico, con alguna perdida apreciable de negocios o de operaciones. (p.e., <5% del volumen de los negocios u operaciones normales, soportadas por el o los sistemas de información afectados, en el tiempo de inactividad o inestabilidad).* • *Presenta un efecto mínimo en las operaciones o en la entrega de servicios, sin afectar la disponibilidad de servicios críticos.* • *Tiene algún impacto social apreciable, con reclamos específicos y directamente relacionados con el incidente.* • *Los impactos contractuales, legales o regulatorios son acotados y con mitigadores efectivos.*
3	*Media*	• *Afectación comprobada, acotada y temporal, de sistemas de información importantes o críticos, con pérdidas significativas de negocio u operaciones (p.e., >=5% y <20% del volumen de las operaciones normales, soportadas por el o los sistemas de información afectados, en el tiempo de inactividad o inestabilidad).* • *Inhabilita temporalmente la entrega de un servicio crítico a un conjunto de clientes o usuarios, sin sobrepasar la tolerancia definida.* • *Tiene un impacto social significativo, como muchos reclamos específicos, obligando a desplegar notas informativas en los sistemas en línea de la institución.* • *Los impactos contractuales, legales o regulatorios son acotados, significando eventuales requerimientos formales de información, acciones legales puntuales, supervisoras o de fiscalización.*
4	*Alta*	• *Afectación comprobada de sistemas de información críticos, extensa en el tiempo y cuyo impacto real puede no estar completamente determinado, resultando en pérdidas muy importantes de negocios u operaciones. (p.e., >=20% del volumen de las operaciones normales, soportadas por el o los sistemas de información afectados, en el tiempo de inactividad o inestabilidad).* • *Inhabilita temporalmente, la entrega de algunos servicios críticos a sus usuarios, superando la tolerancia definida, con potencial activación de planes DRP o de operación alternativa.* • *Tiene un impacto social importante, un volumen de reclamos que satura canales, obligando a desplegar notas de prensa y activar planes de gestión de crisis y control de daños, incluida la activación de seguros.* • *Los impactos contractuales, legales o regulatorios son importantes y pueden conducir a sanciones, multas o demandas masivas.*

”

29. Se realizan las siguientes modificaciones a la Tabla 95 “Tipo de vulnerabilidad”:

i) En la glosa del código 02 se elimina la palabra “*lógicos*”.

ii) Se intercala la expresión “*, monitoreo o autorización de acceso*” entre las frases “Inadecuada definición” y “de los servicios” en la glosa que acompaña al código 05.

iii) En la glosa que acompaña al código 06, se introduce la frase "*, mantención, protección"* entre las expresiones "Inadecuada definición" y "o control de…".

iv) Se eliminan los códigos 08, 09 y 10, junto con sus respectivas glosas.

v) Se agregan los siguientes códigos "*11 Infraestructura o equipamiento obsoleto."*; "*12 Personal sin capacitación o con entrenamiento deficiente."*; y "*99 Otro."*.

30. Se realizan los siguientes ajustes a la Tabla 96 "Tipo de amenaza":

i) Se reemplaza la palabra "estructura" por "*infraestructura*" en la glosa que acompaña al código 02.

ii) En la glosa del código 04, se añade el término "*actos*" previo al concepto "maliciosos".

iii) Se incorporan los siguientes códigos: "*10 Uso de Dispositivos no autorizados o desconocidos*"; "*11 Publicación fraudulenta de un Sitio web, App móvil, API u otro.*"; y "*99 Otro*".

31. Se modifican los siguientes aspectos de la Tabla 97 "Tipos de activos de información":

i) En las glosas de los códigos 01 y 02, se elimina el término "sus" de la expresión "de sus clientes".

ii) Se añaden los siguientes códigos: "*12 Copias de respaldo*"; "*13 Equipos de energía, clima y seguridad física, y aquellos orientados a su monitoreo"; "14 Equipos de infraestructura TI (enlaces, networking, o storage)."; "15 Equipos o dispositivos de ofimática o propósito específico (IoT, cajas de cifrado, ATM, appliances de seguridad, robots, etc.)"; "16 Equipamiento de terceros administrados por la entidad, o por encargo de la entidad."; "17 Sistemas operativos, de plataforma y de base de datos."; "18 Sistemas de negocio o aplicaciones de la producción."; "19 Personal crítico por Business Impact Analysis (BIA) u otro análisis de impacto o de riesgo."; "20 Personal no crítico."*; y "*99 Otro."*.

32. Se ajusta la Tabla 99 "Tipo de alertas" en los siguientes términos:

i) Se agrega la siguiente frase "*o cualquier otro lenguaje de programación*" al final de la glosa que acompaña al código 10.

ii) Se agregan los siguientes códigos: *"22 Comportamiento anómalo"; "23 Afectación de la integridad de archivos específicos"; "24 Falla técnica en hardware o software, sobrecarga o saturación"; "25 Dispositivos no autorizados o desconocidos dentro de la red"; "26*

Acciones no autorizadas de ABM"; y *"99 Otro"*.

33. Se modifica la Tabla 100 "Tipo de plataforma informática" considerando lo siguiente:

i) Se añade la siguiente frase "*o Extranet*" al final de la glosa del código 01.

ii) Se agrega la expresión "*y recursos de colaboración*" en la glosa que acompaña al código 02.

iii) Se complementa la glosa del código 03, incorporándose los siguiente: "*y mensajería institucional".*

iv) Se agrega la frase "*o Sitio web de la entidad"* al final de la glosa que acompaña al código 05.

v) En la glosa del código 07, se complementa con la siguiente frase "*físicos o virtuales on-premise*".

vi) Se elimina el código "06 Sitio Web Seguros".

vii) Se incorporan los siguientes códigos: "*09 Aplicación móvil de la entidad"; "10 Aplicaciones y sistemas empresariales, de negocio o backoffice"; "11 Componentes en la nube, en cualquier modalidad de servicio: IaaS, PaaS, SaaS, etc. (sistemas, estaciones y servidores, almacenamiento, redes, entre otros.)"; "12 Otros dispositivos para transacciones y consultas bancarias"; "13 Otros dispositivos IoT";* y "*99 Otro"*.

34. Se ajusta la Tabla 102 "Tipo de acción realizada" en los términos que se indican a continuación:

i) Se complementa la glosa asociada al código 01 con lo siguiente: "*, remitente y/o dirección de origen*".

ii) Se reemplaza la glosa del código 02 por la siguiente "*Bloqueo por detección de firmas o análisis de comportamiento anómalo*".

iii) Se incorpora la frase "o *de plataformas comprometidas"* al final de la glosa del código 07.

iv) Se eliminan los códigos 06 y 08, junto con sus respectivas glosas.

v) Se añaden los siguientes códigos: "*10 Generación o despliegue de Indicador de Compromiso (IoC) o Indicador de Alerta (IoA)"; "11 Instalación, activación o configuración de un componente, o servicio adicional de seguridad"; "12 Aislamiento y revisión interna del equipo comprometido"; "13 Retiro, o reemplazo, del equipo y reinstalación de software"; "14 Activación del Equipo de Crisis o de respuesta a*

Incidentes"; "15 Acciones con Servicio de Inteligencia"; "16 Auditoría, revisión y/o Forense interno"; "17 Auditoría, revisión y/o Forense externo"; "18 Revisión de analistas de Seguridad o Ciberseguridad"; "19 No se registran acciones"; y *"99 Otro"*.

IV.4. Ajustes a los Antecedentes Generales del MSI de bancos

35. Se ajusta la periodicidad y plazo los archivos D42 y D43, según corresponda, en consistencia con los ajustes 4, 6 y 7 de la sección IV.1.

V. ANÁLISIS DE IMPACTO REGULATORIO

Considerando que los ajustes propuestos se traducen, en su gran mayoría, en la incorporación de nuevos campos a informar, la propuesta normativa que se presenta incrementa los costos asociados a desarrollos informáticos de las entidades fiscalizadas. No obstante, considerando que no aumenta el número de los archivos a preparar y remitir a esta Comisión, las modificaciones propuestas corresponden a un incremento marginal en los costos asociados.

Las nuevas exigencias de la propuesta normativa permiten mantener la idoneidad de la información, toda vez que permiten ajustarse al marco legal nacional vigente y mejorar la precisión de la información con la cual cuenta esta Comisión para efectos de su función supervisora y estadística.

Por otra parte, la Estrategia Institucional de Inclusión Financiera de la CMF[7], publicada el 13 de enero de 2025, define 4 pilares básicos para la inclusión financiera: acceso, uso, calidad y bienestar. Considerando lo anterior, y en relación con el pilar asociado al acceso, la estrategia identifica como objetivo prioritario visibilizar y evaluar las brechas de inclusión financiera e incentivar mejoras en la infraestructura, cobertura de servicios y canales de atención. En este sentido, los ajustes propuestos a los archivos I06 e I11 dan acceso a la Comisión a información más precisa respecto al acceso a la red de servicios financieros que mantienen las instituciones, propendiendo a la generación de mejores indicadores en materia de inclusión financiera, alineados con el mandato de desarrollo de mercado de esta Comisión.

[7] Ver: Link.

VI. REFERENCIAS

Brown, M., Guin, B., & Kirschenmann, K. (2016). Microfinance banks and financial inclusion. *Review of Finance*, *20*(3), 907-946.

Allen, F., Demirguc-Kunt, A., Klapper, L., & Peria, M. S. M. (2016). The foundations of financial inclusion: Understanding ownership and use of formal accounts. *Journal of financial Intermediation*, *27*, 1-30.

Cámara, N., & Tuesta, D.(2014). Measuring financial inclusión: A multidimensional index. *BBVA Research Paper, 14*(26), 1-56.

Carlander, A., Gamble, A., Garling, T., Hauf, J.C., Johansson L.O., & Holmen, M. (2018). The role of perceived quality of personal service in influencing trust and satisfaction with banks. *Financial Services Review, 27*(1), 83-98.

CMF (2025). Estrategia Institucional de Inclusión Financiera. Ver: Link.

Dolata, M., Agotai, D., Schubiger, S., & Schwabe, G. (2019). Pen-and-paper rituals in service interaction: Combining high-touch and high-tech in financial advisory encounters. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), 1-24.

Maity, S., & Sahu, T.N. (2022). Bank Branch outreach and Access to banking services toward financial inclusion: an experimental evidence. *Rajagiri Management Journal, 17*(12), 170-182.

Valdebenito, A., & Pino, G. (2022). Local financial access and income inequality in Chile. *Economics Letters*, *210*, 110170.

Whelan, S. (2012). Automated Teller Machines. *CGAP IT Innovation Series. www.cgap.org*.

VII. ANEXOS

REF: Introduce ajustes a los archivos D05, D42, D43, I06, I11 e I12 del MSI Bancos y sus Antecedentes Generales; modifica las tablas 95, 96, 97, 99, 100 y 102 del MSI Bancos; e incorpora las tablas 128 "Tipos de compromisos" y 129 "Nivel de criticidad" a la sección Tablas del MSI Bancos

---

CIRCULAR N°X.XXX

Bancos
Cooperativas de Ahorro y Crédito
Empresas Emisoras de Tarjetas de Pago
Sociedades de Apoyo al Giro
Empresas Operadoras de Tarjetas de Pago

DD de MES de 2026

Esta Comisión para el Mercado Financiero (en adelante "Comisión"), en uso de las facultades legales, en especial lo dispuesto en los numerales 1, 4 y 18 del artículo 5 y en el numeral 3 del artículo 20 del Decreto Ley N°3.538, de 1980; y en virtud de lo acordado por el Consejo de la Comisión en Sesión Ordinaria N°XXX, de DD de MES de 2026, ha estimado necesario impartir las siguientes actualizaciones al Manual de Sistema de Información de Bancos como sigue:

1. Se introducen los siguientes ajustes al archivo D05 "Deudores de operaciones transfronterizas":

   i) En el primer registro, se reemplaza el nombre del campo CÓDIGO DE LA IF por CÓDIGO DE LA INSTITUCIÓN FINANCIERA.

   ii) Se modifica el largo del campo 17 PLAZO RESIDUAL DE LA OPERACIÓN, pasando de 4 a 5 bytes.

   iii) En concordancia, se ajusta el largo total del registro único del archivo de 324 a 325 bytes.

2. Se realizan las siguientes modificaciones al archivo D42 "Créditos para la vivienda con subsidio":

   i) En la definición de términos del primer registro, se reemplaza el

nombre CÓDIGO DE LA IF por CÓDIGO DE LA INSTITUCIÓN FINANCIERA.

ii) Se reemplaza la periodicidad "A pedido" por "Trimestral".

iii) Se modifica la definición del campo 05 PROGRAMA HABITACIONAL Y DE SUBSIDIO para añadir el programa de subsidio establecido en el Decreto Supremo N°19 del 2016 y el programa de habitabilidad rural (DS10) a la codificación de dicho campo, quedando los siguientes códigos permitidos:

"

01	*Créditos traspasados a la banca por el SERVIU.*
02	*Subsidio Habitacional "Nueva Básica".*
03	*Subsidio Habitacional "Subsidio Unificado".*
04	*Subsidio habitacional en reemplazo del subsidio unificado, Decreto N° 40 de 2004, MINVU. (*)*
05	*Subsidio Leasing Habitacional.*
06	*Subsidio Rural.*
07	*Vivienda Progresiva.*
08	*Programa Especial para Trabajadores, PET.*
09	*Fondo Solidario. (*)*
10	*Subsidio Extraordinario Decreto N° 4 de 2009.*
11	*Sistema Integrado de Subsidio Habitacional, Decreto N° 1 de 2011, MINVU. (*)*
12	*Subsidio Extraordinario Decreto N° 116 de 2015.*
13	*Subsidio DS N°19 del 2016.*
14	*Subsidio Habitabilidad Rural DS 10.*
99	*Otros*

(*) Los subsidios originalmente otorgados de acuerdo con las condiciones del Decreto N° 40 de 2004 o del Decreto N° 174 de 2005 (Fondo Solidario), se informarán con los respectivos códigos 04 o 09, aunque los beneficiarios se hayan acogido a lo dispuesto en el inciso final del artículo 75 del Decreto N° 1 de 2011, por resultarles más favorables las condiciones de este último Decreto.

"

3. Se modifican los siguientes aspectos del archivo D43 "Remates y cesiones en pago de viviendas subsidiadas":

i) En la definición de términos del primer registro, se reemplaza el nombre CÓDIGO DE LA IF por CÓDIGO DE LA INSTITUCIÓN FINANCIERA.

ii) Se reemplaza la periodicidad "A pedido" por "Trimestral".

iii) Se reemplaza el plazo "Según lo solicitado en cada oportunidad" por "15 días hábiles".

iv) Se elimina la expresión "*y cuyo valor no supere las 2.000 UF*" de la descripción del archivo.

v) Se cambia el nombre del campo 01 PERIODO DE LA TRANSFERENCIA por AÑO DE LA TRANSFERENCIA. En consistencia, se reemplaza la palabra "periodo" por "año" en la definición del campo.

vi) Se modifica la definición del campo 03 TRAMO DEL VALOR ORIGINAL DE LA VIVIENDA EN UF para incorporar los tramos "Más de 2.000 UF hasta 3.000 UF", "Más de 3.000 UF hasta 4.000 UF" y "Más de 4.000 UF" a la codificación de dicho campo, quedando los siguientes códigos permitidos:

"

01	*Hasta 400 UF.*
02	*Más de 400 hasta 600 UF.*
03	*Más de 600 hasta 800 UF.*
04	*Más de 800 hasta 1.000 UF.*
05	*Más de 1.000 UF hasta 2.000 UF.*
06	*Más de 2.000 UF hasta 3.000 UF*
07	*Más de 3.000 UF hasta 4.000 UF*
08	*Más de 4.000 UF*

"

4. Se ajusta el archivo I06 "Oficinas, personal, horarios de atención y cajeros automáticos" en los siguientes términos:

i) En la definición de términos del primer registro, se reemplaza el nombre CÓDIGO DE LA IF por CÓDIGO DE LA INSTITUCIÓN FINANCIERA.

ii) Se agrega al registro 1 del archivo el campo 15 LATITUD, formato s9(02)V9(06), con la siguiente definición:

"*Coordenada geográfica que indica la posición norte-sur de la ubicación de la oficina, medida en grados decimales. El formato corresponde a un número decimal con 6 decimales. Valores negativos indican ubicaciones en el hemisferio sur.*"

iii) Se agrega al registro 1 del archivo el campo 16 LONGITUD, formato s9(03)V9(06), con la siguiente definición:

"*Coordenada geográfica que indica la posición este-oeste de la ubicación de la oficina, medida en grados decimales. El formato corresponde a un número decimal con 6 decimales. Valores negativos indican ubicaciones en el hemisferio occidental.*"

iv) Se ajusta el largo del registro 1 del archivo a 173 bytes.

v) Se modifican el largo de los *fillers* y el largo total de los demás registros en concordancia con el ajuste anterior.

5. Se realizan los siguientes ajustes al archivo I11 "Parque de cajeros

automáticos y tiempos de indisponibilidad o *Downtime*":

i) Se agrega al registro 1 del archivo el campo 11 LATITUD, formato s9(02)V9(06), con una definición análoga a la expuesta en el ajuste 4.ii).

ii) Se agrega al registro 1 del archivo el campo 12 LONGITUD, formato s9(03)V9(06), con una definición análoga a la expuesta en el ajuste 4.iii).

iii) Se ajusta el largo del registro 1 del archivo a 117 bytes.

iv) Se modifican el largo de los *fillers* y el largo total de los demás registros en concordancia con el ajuste anterior.

6. Se actualiza el archivo I12 "Incidentes de Ciberseguridad" en los siguientes términos:

i) Se intercala la frase "y Alertas" entre las palabras "Incidentes" y la expresión "de Ciberseguridad" en el nombre del archivo.

ii) Se reemplaza la periodicidad "Mensual" por "Trimestral".

iii) Se reemplaza la descripción del archivo por la siguiente:

"*Mediante este archivo las instituciones financieras informarán todos los incidentes y alertas en materia de Ciberseguridad ocurridos en el trimestre que se informa y la información actualizada o complementaria de incidentes reportados en periodos anteriores. Se entenderá por "incidente de ciberseguridad" todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos afectadas por un evento de seguridad digital. Se considerarán "alertas" a aquellos eventos advertidos, pero no materializados.*"

iv) En el primer registro, se reemplaza el nombre del campo "Código del banco" por "Código de la institución financiera".

v) En la definición de términos del primer registro, se reemplaza el nombre CÓDIGO DE LA IFI por CÓDIGO DE LA INSTITUCIÓN FINANCIERA.

vi) Se realizan los siguientes ajustes al registro 1 que contiene el detalle de los incidentes:

a) Se reemplaza la descripción del registro por la siguiente:

"*En este registro se deben informar todos los incidentes de*

ciberseguridad materializados, sin exclusiones debido a criterios internos de relevancia o materialidad.".

b) Se cambian los nombres de los campos 06 FECHA DEL REPORTE y 07 HORA DEL REPORTE por FECHA DE DETECCIÓN y HORA DE DETECCIÓN, respectivamente.

c) Se elimina el segundo párrafo de la definición del campo 09 HORA DE LA MITIGACIÓN.

d) Se complementa la definición del campo 09 HORA DE LA MITIGACIÓN, incorporándose el paréntesis "*(999999)*" después de la frase "completar el campo con nueves" del primer párrafo de la definición.

e) Se ajusta el nombre del campo 10 TIPO DE VULNERABILIDAD a TIPOS DE VULNERABILIDADES y se reemplaza su definición por la siguiente:

"*Se deberán informar los tipos de vulnerabilidades que, de acuerdo con la evaluación de la entidad a la fecha de envío del archivo, hayan contribuido a la materialización del incidente, de acuerdo con los códigos establecidos en la Tabla 95 "Tipo de vulnerabilidad". El número de vulnerabilidades informados no debe exceder de tres.*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 95.

Por ejemplo, si los tipos de vulnerabilidades identificados corresponden a los códigos 01, 07 y 11, se deberá informar "010711". Si únicamente resulta aplicable el tipo de vulnerabilidad identificado con el código 11, se deberá informar "110000"."

Con lo anterior, se aumenta el largo del campo a 06 bytes.

f) Se ajusta el nombre del campo 11 TIPO DE AMENAZA a TIPOS DE AMENAZAS y se reemplaza su definición por la siguiente:

"*Se deberán informar los tipos de amenazas que, de acuerdo con la evaluación de la entidad a la fecha de envío del archivo, mejor describan el origen y expliquen la materialización del incidente, de acuerdo con los códigos establecidos en la Tabla 96 "Tipo de amenaza". El número de amenazas a ser informados no debe exceder de tres.*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 96.

Por ejemplo, si los tipos de amenazas identificados corresponden a los códigos 01, 07 y 11, se deberá informar "010711". Si únicamente resulta aplicable el tipo de amenaza identificado con el código 11, se deberá informar "110000"."

Con lo anterior, se aumenta el largo del campo a 06 bytes.

g) En el nombre del campo 12 TIPO DE ACTIVOS DE INFORMACIÓN INVOLUCRADOS, se reemplaza la palabra "TIPO" por "*TIPOS"* y se reemplaza su definición por la siguiente:

"*Se deberán informar los tipos de activos de información afectados o puestos en riesgo por el incidente, de acuerdo con los códigos establecidos en la Tabla 97 "Tipos de activos de información".*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 97. En cada posición se deberá consignar el código correspondiente cuando el tipo de activo de información haya sido afectado o puesto en riesgo, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si los tipos de activos de información afectados o puestos en riesgo corresponden a los códigos 04, 12 y 16, se deberá informar "00000004000000000000001200000160000000000". Si únicamente resulta afectado o puesto en riesgo el tipo de activo de información identificado con el código 12, se deberá informar "00000000000000000000001200000000000000000"."

Con lo anterior, se aumenta el largo del campo a 42 bytes.

h) En el nombre del campo 13 TIPO DE CANALES, PRODUCTOS O SERVICIOS INVOLUCRADOS, se reemplaza la palabra "TIPO" por "TIPOS" y se reemplaza su definición por la siguiente:

"Se deberán informar los canales, productos o servicios prestados por la institución cuya disponibilidad o funcionamiento se haya visto afectado por el incidente, de acuerdo con los códigos establecidos en la Tabla 98 "Tipo de canales, productos o servicios".

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 98. En cada posición se deberá consignar el código correspondiente cuando el canal, producto o servicio haya sido afectado, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si los productos afectados corresponden a los códigos

04, 12 y 16, se deberá informar "00000004000000000000012000001600000000". Si únicamente resulta afectado el producto identificado con el código 12, se deberá informar "00000000000000000000012000000000000000"."

Con lo anterior, se aumenta el largo del campo a 40 bytes.

i) Se reemplaza la definición del campo 21 NIVEL DE CRITICIDAD por la siguiente:

"*Se debe indicar para cada incidente el nivel de criticidad, entendido como el impacto en términos de ciberseguridad de acuerdo con la codificación indicada en la Tabla 129 "Nivel de criticidad". En caso de que el incidente informado presente simultáneamente características asociadas a más de un nivel de criticidad, se debe informar el código vinculado al nivel de mayor criticidad.*"

j) Se añade el nuevo campo 22 FECHA DE ESCALAMIENTO, formato F(08), con la siguiente definición

"*Corresponde indicar la fecha (AAAAMMDD) en la que la situación fue comunicada al Equipo de Respuesta a Incidentes de la entidad.*"

k) Se agrega el nuevo campo 23 HORA DE ESCALAMIENTO, formato 9(06), cuya definición es la siguiente:

"*Corresponde indicar la hora (HHMMSS) en la que la situación fue comunicada al Equipo de Respuesta a Incidentes de la entidad (formato de 24 hrs.).*"

l) Se incorpora el nuevo campo 24 FECHA DE REPORTE A LA CMF, formato F(08), con la siguiente definición:

"*Corresponde informar la fecha (AAAAMMDD) en la que el incidente fue informado a la Comisión a través de los canales y mecanismos dispuestos para tal efecto en el Reporte de Incidentes Operacionales (RIO) de la CMF. En caso de que el incidente no haya sido informado a la Comisión, el campo debe completarse con "19000101".*"

m) Se incluye el nuevo campo 25 HORA DE REPORTE A LA CMF, formato 9(06), definido como se muestra a continuación:

"*Corresponde informar la hora (HHMMSS) en la que el incidente fue informado a la Comisión a través de los canales y mecanismos dispuestos para tal efecto, en formato de 24 hrs., en el Reporte de Incidentes Operacionales (RIO) de la CMF. En caso de que el incidente no haya sido informado a la Comisión, el campo se debe completar con nueves ("999999").*"

n) Se agrega el nuevo campo 26 FECHA DE INICIO DE ACCIONES DE MITIGACIÓN, formato F(08), cuya definición es la siguiente:

"*Corresponde informar la fecha (AAAAMMDD) en la que la entidad financiera da inicio al proceso o a las acciones de mitigación.*"

o) Se añade el nuevo campo 27 HORA DE INICIO DE ACCIONES DE MITIGACIÓN, formato 9(06), con la siguiente definición:

"*Corresponde informar la hora (HHMMSS) en la que la entidad financiera da inicio al proceso o a las acciones de mitigación (formato de 24 hrs.).*"

p) Se introduce el nuevo campo 28 TIPOS DE ACCIONES REALIZADAS, formato 9(36), con la siguiente definición:

"*Se deberán informar las acciones realizadas para gestionar el incidente, de acuerdo con los códigos establecidos en la Tabla 102 "Tipo de acción realizada".*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 102. En cada posición se deberá consignar el código correspondiente cuando la acción haya sido realizada, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si las acciones realizadas corresponden a los códigos 04, 13 y 15, se deberá informar "00000004000000000000130015000000000". Si únicamente se realizó la acción identificada con el código 13, se deberá informar "00000000000000000000130000000000000"."

q) Se agrega el nuevo campo 29 TIPOS DE PLATAFORMAS INVOLUCRADAS, formato 9(26), con la siguiente definición:

"*Se deberán informar las plataformas informáticas afectadas por el incidente, de acuerdo con los códigos establecidos en la Tabla 100 "Tipo de plataforma informática".*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 100. En cada posición se deberá consignar el código correspondiente cuando la plataforma informática haya sido afectada, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si las plataformas informáticas afectadas corresponden a los códigos 02, 05 y 12, se deberá informar "00020000050000000000120000". Si únicamente resulta afectada la plataforma identificada con el código 13, se deberá informar

"00000000000000000000001300"."

r) Se añade el nuevo campo 30 TIPOS DE COMPROMISOS, formato 9(22), con la siguiente definición:

"*Se deberán informar los tipos de compromisos derivados del incidente, de acuerdo con los códigos establecidos en la Tabla 128 "Tipos de compromisos".*

Para ello, el campo se completará con una secuencia de códigos de dos caracteres, respetando el orden en que estos se presentan en la Tabla 128. En cada posición se deberá consignar el código correspondiente cuando el tipo de compromiso sea aplicable, o "00" en caso contrario, hasta completar la longitud definida para el campo.

Por ejemplo, si los tipos de compromisos identificados corresponden a los códigos 02, 05 y 11, se deberá informar "00020000050000000000011". Si únicamente resulta aplicable el código 11, se deberá informar "00000000000000000000011"."

vii) Se realizan las siguientes modificaciones al registro 2 que contiene el detalle de las alertas:

a) Se reemplaza la descripción del registro por la siguiente:

"*En este registro se deben informar para cada mes en forma acumulada las alertas detectadas y registradas en todos los sistemas y tecnologías de seguridad que dispone la entidad, propios o contratados como servicios, e independientemente de si hayan sido gestionadas o no. Para el caso de tecnologías que filtran o depuran el tráfico de red que llega a la entidad, el número de alertas a informar corresponde al que ocurre o se detecta antes de dicho proceso.*"

b) Se reemplaza la tabla con los códigos y taxonomías en la definición del campo 03 ORIGEN DE DATOS por la siguiente:

Código	Origen de datos
07	Antifraude (Antispam, Antiphishing, entre otros)
08	Antimalware (AV, EDR, XDR, entre otros)
09	Control Acceso y Autentificación (MFA, PAM, IDM, entre otros)
10	Inteligencia Seguridad (UEBA, Inmunización, Señuelos, entre otros)
11	Prevención Fuga Información (DBFW, DLP, CASB, entre otros)
12	Protección Tráfico (FW, IDS, IPS, AntiDoS, entre otros)

13	Seguridad Dispositivos Móviles (AV, MDM, entre otros)
14	Protección Aplicaciones (WAF, CASB, CDN, entre otros)
15	Correlación (SIEM)
16	Reporte de usuarios o de proveedores
17	Otra tecnología o fuente no clasificada

c) Se eliminan los campos 05 PLATAFORMA INVOLUCRADA, 06 NATURALEZA DE LA AMENAZA y 07 ACCIONES REALIZADAS.

d) Se agrega el nuevo campo 05 PERIODO DE LAS ALERTAS, con la siguiente definición:

"*Corresponde informar el mes (AAAAMM) al cual se refiere la información de las alertas reportadas en este registro.*"

viii) Considerando las modificaciones anteriores, se ajustan los largos de los dos registros del archivo a 410 bytes y se aumenta el largo del *filler* del segundo registro a 385 bytes.

ix) Se realizan ajustes de acuerdo con la nueva institucionalidad.

7. Se ajustan las tablas del MSI de bancos en los siguientes términos:

i) Se agrega la Tabla 128 "Tipos de compromisos" al catálogo de tablas, con lo siguientes códigos y glosas:

"

Tabla 128: Tipos de compromisos

Código	***Tipo de compromiso***
01	***Uso no autorizado de redes y sistemas informáticos:*** *Uso no autorizado de sistemas de la institución afectada, ya sea a través de explotación de vulnerabilidades, uso no autorizado de credenciales, acceso a almacenamiento en nube, u otros.*
02	***Actividades de phishing o fraude en infraestructura propia:*** *Envío de phishing a través de servidores de la institución afectada, o almacenamiento de sitios fraudulentos en redes y sistemas informáticos de la institución afectada.*
03	***Actividades de phishing o fraude relacionadas con la institución:*** *Envío de phishing relacionado con la institución afectada por parte de terceros, o almacenamiento de sitios fraudulentos por parte de terceros.*
04	***Ejecución no autorizada de código:*** *Inclusión y ejecución no autorizada de código en sistemas de la institución afectada.*

05	***Exfiltración y/o exposición de datos:*** *Pérdida de información confidencial con o sin divulgación pública, y/o información confidencial expuesta accidental o intencionalmente.*
06	***Exfiltración y/o exposición de configuraciones:*** *Pérdida o exposición accidental de configuraciones y parámetros confidenciales de un sistema o aplicación de la institución afectada.*
07	***Exfiltración y/o exposición de código fuente:*** *Pérdida o exposición excesiva del código fuente de un sistema de la institución afectada.*
08	***Indisponibilidad y/o denegación de servicio:*** *Pérdida total del funcionamiento de un servicio, sistema o servidor, o saturación de red impidiendo su operación normal.*
09	***Degradación de servicio:*** *Pérdida parcial del rendimiento o funcionalidad de un servicio, sistema o servidor.*
10	***Modificación no autorizada de datos:*** *Alteración no autorizada de información contenida en sistemas, servicios o servidores.*
11	***Manipulación no autorizada de configuración:*** *Cambio no autorizado de configuraciones en sistemas, servicios o servidores.*

"

ii) Se añade la Tabla 129 "Nivel de criticidad" al catálogo de tablas, considerando la siguiente codificación:

"

Tabla 129: Nivel de criticidad

Código	***Nivel de criticidad***	***Características (debe cumplirse al menos una de las condiciones para calificar en el nivel)***
1	*Menor*	• *Afectación de algún sistema de información no crítico y con mecanismos de contingencia probados y efectivos.* • *No tiene efectos en la entrega de servicios o en las operaciones.* • *Tiene un impacto social menor o nulo.* • *Sin impacto contractual, legal o regulatorio.* *Generalmente estas situaciones no tienen efectos negativos, excepto el registro, chequeo de salud de sistemas y la revisión correlacionada con eventos de similar naturaleza, recurrentes en el tiempo.*
2	*Baja*	• *Afectación comprobada de algún sistema de información productivo, no crítico, con alguna perdida apreciable de negocios o de operaciones. (p.e., <5% del volumen de los negocios u operaciones normales, soportadas por el o los sistemas de información afectados, en el tiempo de inactividad o inestabilidad).* • *Presenta un efecto mínimo en las operaciones o en la entrega de servicios, sin afectar la disponibilidad de servicios críticos.* • *Tiene algún impacto social apreciable, con reclamos específicos y directamente relacionados con el incidente.* • *Los impactos contractuales, legales o regulatorios son acotados y con mitigadores efectivos.*

3	*Media*	• *Afectación comprobada, acotada y temporal, de sistemas de información importantes o críticos, con pérdidas significativas de negocio u operaciones (p.e., >=5% y <20% del volumen de las operaciones normales, soportadas por el o los sistemas de información afectados, en el tiempo de inactividad o inestabilidad).* • *Inhabilita temporalmente la entrega de un servicio crítico a un conjunto de clientes o usuarios, sin sobrepasar la tolerancia definida.* • *Tiene un impacto social significativo, como muchos reclamos específicos, obligando a desplegar notas informativas en los sistemas en línea de la institución.* • *Los impactos contractuales, legales o regulatorios son acotados, significando eventuales requerimientos formales de información, acciones legales puntuales, supervisoras o de fiscalización.*
4	*Alta*	• *Afectación comprobada de sistemas de información críticos, extensa en el tiempo y cuyo impacto real puede no estar completamente determinado, resultando en pérdidas muy importantes de negocios u operaciones. (p.e., >=20% del volumen de las operaciones normales, soportadas por el o los sistemas de información afectados, en el tiempo de inactividad o inestabilidad).* • *Inhabilita temporalmente, la entrega de algunos servicios críticos a sus usuarios, superando la tolerancia definida, con potencial activación de planes DRP o de operación alternativa.* • *Tiene un impacto social importante, un volumen de reclamos que satura canales, obligando a desplegar notas de prensa y activar planes de gestión de crisis y control de daños, incluida la activación de seguros.* • *Los impactos contractuales, legales o regulatorios son importantes y pueden conducir a sanciones, multas o demandas masivas.*

"

iii) Se realizan las siguientes modificaciones a la Tabla 95 "Tipo de vulnerabilidad":

a) En la glosa del código 02 se elimina la palabra "*lógicos*".

b) Se intercala la expresión "*, monitoreo o autorización de acceso*" entre las frases "Inadecuada definición" y "de los servicios" en la glosa que acompaña al código 05.

c) En la glosa que acompaña al código 06, se introduce la frase "*, mantención, protección"* entre las expresiones "Inadecuada definición" y "o control de…".

d) Se eliminan los códigos 08, 09 y 10, junto con sus respectivas glosas.

e) Se agregan los siguientes códigos "*11 Infraestructura o equipamiento obsoleto.*"; "*12 Personal sin capacitación o con*

entrenamiento deficiente.”; y “*99 Otro.*”.

iv) Se realizan los siguientes ajustes a la Tabla 96 “Tipo de amenaza”:

a) Se reemplaza la palabra “estructura” por “*infraestructura*” en la glosa que acompaña al código 02.

b) En la glosa del código 04, se añade el término “*actos*” previo al concepto “maliciosos”.

c) Se incorporan los siguientes códigos: “*10 Uso de Dispositivos no autorizados o desconocidos*”; “*11 Publicación fraudulenta de un Sitio web, App móvil, API u otro.*”; y “*99 Otro*”.

v) Se modifican los siguientes aspectos de la Tabla 97 “Tipos de activos de información”:

a) En las glosas de los códigos 01 y 02, se elimina el término “sus” de la expresión “de sus clientes”.

b) Se añaden los siguientes códigos: “*12 Copias de respaldo*”; “*13 Equipos de energía, clima y seguridad física, y aquellos orientados a su monitoreo”; “14 Equipos de infraestructura TI (enlaces, networking, o storage).”; “15 Equipos o dispositivos de ofimática o propósito específico (IoT, cajas de cifrado, ATM, appliances de seguridad, robots, etc.)”; “16 Equipamiento de terceros administrados por la entidad, o por encargo de la entidad.”; “17 Sistemas operativos, de plataforma y de base de datos.”; “18 Sistemas de negocio o aplicaciones de la producción.”; “19 Personal crítico por Business Impact Analysis (BIA) u otro análisis de impacto o de riesgo.”; “20 Personal no crítico.”;* y “*99 Otro.*”.

vi) Se ajusta la Tabla 99 “Tipo de alertas” en los siguientes términos:

a) Se agrega la siguiente frase “*o cualquier otro lenguaje de programación*” al final de la glosa que acompaña al código 10.

b) Se agregan los siguientes códigos: *“22 Comportamiento anómalo”; “23 Afectación de la integridad de archivos específicos”; “24 Falla técnica en hardware o software, sobrecarga o saturación”; “25 Dispositivos no autorizados o desconocidos dentro de la red”; “26 Acciones no autorizadas de ABM”;* y *“99 Otro”*.

vii) Se modifica la Tabla 100 “Tipo de plataforma informática” considerando lo siguiente:

a) Se añade la siguiente frase “*o Extranet*” al final de la glosa del código 01.

b) Se agrega la expresión "*y recursos de colaboración*" en la glosa que acompaña al código 02.

c) Se complementa la glosa del código 03, incorporándose los siguiente: "*y mensajería institucional".*

d) Se agrega la frase "*o Sitio web de la entidad"* al final de la glosa que acompaña al código 05.

e) En la glosa del código 07, se complementa con la siguiente frase "*físicos o virtuales on-premise*".

f) Se elimina el código "06 Sitio Web Seguros".

g) Se incorporan los siguientes códigos: "*09 Aplicación móvil de la entidad"; "10 Aplicaciones y sistemas empresariales, de negocio o backoffice"; "11 Componentes en la nube, en cualquier modalidad de servicio: IaaS, PaaS, SaaS, etc. (sistemas, estaciones y servidores, almacenamiento, redes, entre otros.)"; "12 Otros dispositivos para transacciones y consultas bancarias"; "13 Otros dispositivos IoT";* y "*99 Otro"*.

viii) Se ajusta la Tabla 102 "Tipo de acción realizada" en los términos que se indican a continuación:

a) Se complementa la glosa asociada al código 01 con lo siguiente: "*, remitente y/o dirección de origen*".

b) Se reemplaza la glosa del código 02 por la siguiente "*Bloqueo por detección de firmas o análisis de comportamiento anómalo*".

c) Se incorpora la frase "*o de plataformas comprometidas"* al final de la glosa del código 07.

d) Se eliminan los códigos 06 y 08, junto con sus respectivas glosas.

e) Se añaden los siguientes códigos: "*10 Generación o despliegue de Indicador de Compromiso (IoC) o Indicador de Alerta (IoA)"; "11 Instalación, activación o configuración de un componente, o servicio, adicional de seguridad"; "12 Aislamiento y revisión interna del equipo comprometido"; "13 Retiro, o reemplazo, del equipo y reinstalación de software"; "14 Activación del Equipo de Crisis o de Respuesta a Incidentes"; "15 Acciones con Servicio de Inteligencia"; "16 Auditoría, revisión y/o Forense interno"; "17 Auditoría, revisión y/o Forense externo"; "18 Revisión de analistas de Seguridad o Ciberseguridad"; "19 No se registran acciones";* y "*99 Otro"*.

8. Se modifica el catálogo de archivos contenido en los Antecedentes Generales

del MSI de bancos en los mismos términos indicados en los ajustes 2.ii), 3.ii) y 3.iii).

En consecuencia, se incorporan y reemplazan, según corresponda, las hojas de los cuerpos normativos correspondientes.

VIGENCIA:

Los cambios realizados entrarán en vigencia dos meses a contar de la publicación de esta circular.

CATHERINE TORNEL LEÓN
PRESIDENTA
COMISIÓN PARA EL MERCADO FINANCIERO