**CIRCULAR 13/2026 dirigida a las instituciones de crédito, relativa a las Modificaciones a la Circular 3/2025 (Seguridad Informática).**

Al margen un logotipo, que dice: Banco de México.- "2026, Año de Margarita Maza Parada".

CIRCULAR 13/2026

**A LAS INSTITUCIONES DE CRÉDITO:**

**ASUNTO: MODIFICACIONES A LA CIRCULAR 3/2025 (SEGURIDAD INFORMÁTICA)**

El Banco de México, con el objetivo de fortalecer la integridad y resiliencia del abastecimiento de moneda nacional en el país, aumentar la certeza jurídica de los requerimientos de seguridad informática y continuidad operativa aplicables a las operaciones de caja, mejorar la infraestructura de tecnologías de la información que las soportan, así como brindar claridad a las instituciones de crédito respecto a los requerimientos de seguridad informática que deben cumplir, ha resuelto modificar las Disposiciones en materia de operaciones de caja, corresponsalía y manejo de piezas presuntamente falsas o alteradas, contenidas en la Circular 3/2025.

Así también, se propone homologar, en la materia objeto de la presente reforma, la estructura de la referida Circular 3/2025 con otras disposiciones emitidas por este Instituto Central en materia de seguridad informática, fomentando la consistencia y eficiencia regulatoria, a través de una mayor precisión y claridad en sus requerimientos, para su adecuada instrumentación por parte de las instituciones de crédito.

Cabe mencionar que, con fundamento en el numeral 13, fracción IV, de las Políticas para la consulta pública de las disposiciones de carácter general que emita el Banco de México, las modificaciones a que se refiere la presente comunicación fueron exceptuadas del proceso de consulta pública tomando en cuenta que en dicha consulta no resulta conveniente compartir detalles técnicos en materia de seguridad informática cuyo acceso está restringido únicamente a las Instituciones de Crédito participantes de SAM, SIBUC y AUDI. En este contexto, la consulta pública no tendría como resultado la obtención de insumos relevantes y retrasaría la publicación de estas modificaciones. Lo anterior, afectaría la adecuada y pronta implementación de los controles de seguridad informática por parte de las Instituciones de Crédito y, en consecuencia, generaría posibles riesgos en el cumplimiento de las obligaciones previstas.

Por lo anterior, con fundamento en lo dispuesto por los artículos 28, párrafos séptimo y octavo, de la Constitución Política de los Estados Unidos Mexicanos, 2o., 3o., fracción I, 4o., 24, párrafos primero y segundo, 25 y 37, de la Ley del Banco de México, 19 y 20 de la Ley Monetaria de los Estados Unidos Mexicanos, 48 y 48 Bis 1 de la Ley de Instituciones de Crédito, 22 de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, 1o., 4o., párrafos primero y cuarto, 8o., párrafos cuarto y octavo, 10, párrafo primero, 16 Bis, fracción II, y 14 Bis, en relación con el 17, fracción I, del Reglamento Interior del Banco de México, que le otorgan la atribución de expedir disposiciones a través de la Dirección de Programación y Distribución de Efectivo y de la Dirección General Jurídica, respectivamente, así como Segundo, fracciones III y X, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México ha resuelto **modificar** los artículos 1, 19, 97, 124, 125 y 126, así como el Anexo 6, y **adicionar** el Anexo 22 de la Circular 3/2025 dirigida a las instituciones de crédito, relativa a las Disposiciones en materia de operaciones de caja, corresponsalía y manejo de piezas presuntamente falsas o alteradas, para quedar en los términos siguientes:

**DISPOSICIONES EN MATERIA DE OPERACIONES DE CAJA, CORRESPONSALÍA Y MANEJO DE PIEZAS PRESUNTAMENTE FALSAS O ALTERADAS**

"**Artículo 1. Definiciones**

**…**

**GENERALES**

**…**

| | |
|---|---|
| Componentes de Infraestructura de Conexión: | a la Infraestructura de Cómputo, software, así como a la Infraestructura de Telecomunicaciones y cualquier otro elemento, que forme parte de la arquitectura de comunicaciones para operar con los sistemas SIBUC, AUDI y SAM. |

**…**

| | |
|---|---|
| Elemento Técnico de Seguridad: | Se deroga. |

**…**

| | |
|---|---|
| Identificación Oficial: | a la credencial para votar vigente con fotografía emitida por el Instituto Nacional Electoral, pasaporte vigente emitido por la Secretaría de Relaciones Exteriores, cartilla del servicio militar nacional o tarjeta única de identidad militar vigente, emitidas por la Secretaría de la Defensa Nacional, o la Clave Única de Registro de Población a la cual se refiere el artículo 91 Bis y demás aplicables de la Ley General de Población, expedidos por las autoridades competentes, de acuerdo con la normativa aplicable. Tratándose de personas de nacionalidad extranjera quedan incluidos los documentos emitidos por la Secretaría de Relaciones Exteriores o el Instituto Nacional de Migración que acrediten su calidad migratoria o legal estancia en el país, así como el pasaporte vigente emitido por la autoridad competente en el extranjero. |
| ... | |
| Incidente de Ciberseguridad: | a cualquier evento ocurrido en la Institución de Crédito que: i) podría comprometer la confidencialidad, integridad o disponibilidad de un sistema informático o de la información que esta procesa, almacena o transmite; o ii) constituye una violación o amenaza inminente de violación de las disposiciones, políticas o procedimientos de seguridad informática aplicables. |
| Infraestructura de Cómputo: | a los elementos de cómputo, ya sean físicos o virtuales, utilizados por las Instituciones de Crédito para el procesamiento y almacenamiento de datos, con independencia del carácter o rol con el que lo hagan, ya sea como Institución de Crédito, Usuario, o Administrador del Corresponsal para operar con los sistemas SIBUC, AUDI o SAM. |
| Infraestructura de Telecomunicaciones: | a los elementos de red, físicos o lógicos, los cuales brindan el servicio de conectividad y transportan los datos de los diferentes programas de cómputo que son utilizados por las Instituciones de Crédito para conectarse y operar con los sistemas SIBUC, AUDI o SAM, con independencia del carácter o rol con el que lo hagan, ya sea como Institución de Crédito, Usuario o Administrador del Corresponsal. |
| ... | |
| Requerimientos de Seguridad Informática: | a las obligaciones en materia de seguridad informática previstas en el Anexo 22 de esta Circular y en el documento denominado “Anexo Técnico de los Requerimientos de Seguridad Informática”, que contiene las especificaciones técnicas de seguridad informática para los Componentes de Infraestructura de Conexión necesarios para operar con el SIBUC, AUDI y SAM, a que se refiere el Capítulo XIV del Título III de la presente Circular, y que el Banco de México da a conocer a las Instituciones de Crédito, los Usuarios, Administradores de los Corresponsales y E.T.V. a través de los sistemas SIBUC, AUDI o SAM.<br><br>El documento denominado “Anexo Técnico de los Requerimientos de Seguridad Informática” se dará a conocer a través de los sistemas mencionados en el párrafo anterior, lo cual será considerado como válidamente realizado para todos los efectos legales a que haya lugar. Lo anterior, con independencia de la fecha en la que los destinatarios los consulten. |
| ...” | |

"**Artículo 19. Situaciones de contingencia**

En el evento de que el Banco de México les indique a los Usuarios y Administradores de los Corresponsales que se operará en modo de contingencia, las Operaciones de Caja se realizarán de conformidad con el procedimiento señalado al efecto en el Instructivo de Caja.

En aquellos casos en que se presente un evento en una Institución de Crédito, Corresponsal, o Usuario que afecte su operación o conexión con alguno de los sistemas SIBUC, AUDI o SAM la institución estará obligada a gestionar su continuidad operativa, conforme a la normativa interna emitida en términos del requerimiento relativo a la gestión operativa prevista en el "Anexo Técnico de los Requerimientos de Seguridad Informática"."

"**Artículo 97. Reclamación por Piezas Presuntamente Falsas**

**…**

**…**

I. Un número de recibo asignado por el SAM o por la Institución de Crédito, observando los criterios establecidos en el Anexo 9.

II. **…**

**…**"

"**Artículo 124. Características del esquema de conexión para el SIBUC, AUDI y SAM**

a. El Usuario o Administrador del Corresponsal podrá conectarse al SIBUC a través de Internet utilizando solo la Infraestructura de Cómputo que dicho Usuario o Administrador del Corresponsal asigne para ello. Para tal efecto, el Usuario o Administrador del Corresponsal deberá enviar a la Oficina de Seguimiento de Operaciones de Caja, al correo osoc@banxico.org.mx del Banco de México, mediante el formato previsto en el Anexo 19, en Excel, el cual deberá contener la firma electrónica de alguna Persona Autorizada del Usuario o Persona Facultada del Administrador del Corresponsal de que se trate, una relación de los segmentos de red o direcciones IP públicas de la Infraestructura de Cómputo con la cual se accede al SIBUC, incluyendo aquellas utilizadas por las E.T.V. que acceden al SIBUC, designadas por el Usuario o Administrador del Corresponsal conforme a lo previsto en el inciso k. del presente artículo. Los segmentos de red deberán ser escritos en máscaras de subred que tengan como mínimo una longitud de /16, o en otra longitud que agrupe las direcciones IP públicas (de /17 a /29, preferentemente de /24) de la Infraestructura de Cómputo que accede al SIBUC.

b. El Usuario, Institución de Crédito o Administrador del Corresponsal podrá conectarse al AUDI a través de Internet utilizando solo la Infraestructura de Cómputo que dicho Usuario, Institución de Crédito o Administrador del Corresponsal asigne para ello. Para tal efecto, el Usuario, Institución de Crédito o Administrador del Corresponsal deberá enviar a la Oficina de Seguimiento de Operaciones de Caja, al correo osoc@banxico.org.mx del Banco de México, mediante el formato previsto en el Anexo 20, en Excel, el cual deberá contener la firma electrónica de alguna Persona Autorizada del Usuario o Persona Facultada del Administrador del Corresponsal de que se trate, para usuarios administradores del SIBUC o bien, la firma electrónica del Usuario o Institución de Crédito registrada ante el Banco de México en la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados para usuarios administradores del SAM, una relación de los segmentos de red o direcciones IP públicas de la Infraestructura de Cómputo con la cual se accede al AUDI, incluyendo aquellas utilizadas por las E.T.V. que acceden al AUDI, designadas por el Usuario, Institución de Crédito o Administrador del Corresponsal conforme a lo previsto en el inciso k. del presente artículo. Los segmentos de red deberán ser escritos en máscaras de subred que tengan como mínimo una longitud de /16, o en otra longitud que agrupe las direcciones IP públicas (de /17 a /29, preferentemente de /24) de la Infraestructura de Cómputo que acceda al AUDI.

c. El Usuario o Institución de Crédito podrá conectarse al SAM a través de Internet utilizando solo la Infraestructura de Cómputo que dicho Usuario o Institución de Crédito asigne para ello. Para tal efecto, el Usuario o Institución de Crédito deberá enviar a la Subgerencia de Atención a la Falsificación de Moneda, al correo OEPPF@banxico.org.mx del Banco de México, mediante el formato previsto en el Anexo 21, en Excel, el cual deberá contener la firma electrónica del Usuario o Institución de Crédito registrada ante el Banco de México en la Dirección de Operación y Continuidad de Sistemas de Pagos e Infraestructuras de Mercados para usuarios administradores del SAM, una relación de los segmentos de red públicos de la Infraestructura de Cómputo, con la cual se accede al SAM, incluyendo aquellas utilizadas por las E.T.V. que acceden al SAM, designadas por el Usuario o Institución de Crédito conforme a lo previsto en el inciso k. del presente artículo. Los segmentos de red deberán ser escritos en máscaras de subred que tengan como mínimo una longitud de /16, o en otra longitud que agrupe las direcciones IP públicas (de /17 a /29, preferentemente de /24) de la Infraestructura de Cómputo que acceda al SAM.

d. Los Usuarios, Instituciones de Crédito o Administrador del Corresponsal deberán enviar al Banco de México, al correo osoc@banxico.org.mx, mediante el formato previsto en los Anexos 19 o 20, según corresponda o bien al correo OEPPF@banxico.org.mx mediante el formato previsto en el Anexo 21, dentro de los primeros 10 Días Hábiles Bancarios de cada mes, el detalle de las altas o bajas a la relación mencionada en los incisos anteriores. La solicitud de las altas o bajas de los segmentos de red o direcciones IP públicas de la Infraestructura de Cómputo con la cual se accede al SIBUC, AUDI y SAM, será atendida a más tardar 10 Días Hábiles Bancarios posteriores a su recepción.

e. Se deroga.

f. En caso de que se presenten Incidentes de Ciberseguridad en alguno de los Componentes de Infraestructura de Conexión o en las aplicaciones que utilizan las Instituciones de Crédito, Usuarios o Administradores del Corresponsal para interactuar con el SIBUC, AUDI o SAM, dichas instituciones deberán reportarlo dentro de los 30 minutos siguientes al momento en que identificaron el Incidente de Ciberseguridad a través del correo: ciberseguridad-banxico@banxico.org.mx, y enviar el reporte de seguimiento en un plazo no mayor a 24 horas a partir de la identificación, conforme al Apéndice 1 del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

   Derivado de lo mencionado en este inciso, el Banco de México podrá determinar las acciones que considere convenientes sobre los sistemas SIBUC, AUDI y SAM con el objetivo de salvaguardar la seguridad informática e integridad de estos y de sus usuarios.

g. Las Instituciones de Crédito, Usuarios o Administradores del Corresponsal que utilizan los servicios del SIBUC, AUDI y SAM deberán participar en los ejercicios de Ciberresiliencia a los que los convoque el Banco de México para mantener el buen funcionamiento del SIBUC, AUDI y SAM, lo anterior se realizará en los términos y condiciones que establezca el Instituto Central.

h. Los Componentes de Infraestructura de Conexión deberán ser provistos, administrados y soportados por propia Institución de Crédito, Usuario o Administrador del Corresponsal.

i. Los Componentes de Infraestructura de Conexión deberán de cumplir, en todo momento, con los Requerimientos de Seguridad Informática.

j. Se deroga.

k. Las Instituciones de Crédito y Usuarios podrán designar a una o varias E.T.V. para que realicen operaciones en los sistemas SIBUC, AUDI y SAM en su nombre y por su cuenta. En tal caso, dichas Instituciones de Crédito y Usuarios asumirán plena responsabilidad por las operaciones realizadas, así como del cumplimiento de los Requerimientos de Seguridad Informática en los Componentes de Infraestructura de Conexión utilizados por las E.T.V. que hayan designado para tales fines.

l. El Banco de México establecerá los mecanismos de autenticación para fortalecer la seguridad informática de los sistemas SIBUC, AUDI y SAM.

**Artículo 125. Verificación de Componentes de Infraestructura de Conexión**

El Banco de México podrá, en todo momento, verificar que los Componentes de Infraestructura de Conexión cumplan con las características y especificaciones técnicas y de seguridad informática previstas en los Requerimientos de Seguridad Informática.

Asimismo, el Banco de México podrá realizar dicha verificación a través del ejercicio de sus facultades de inspección a la Institución de Crédito, Usuario o Administrador del Corresponsal, o bien, a través del ejercicio de su facultad de vigilancia mediante requerimientos de información que la Institución de Crédito, Usuario o Administrador del Corresponsal deba suministrar en la forma, términos, plazos y condiciones que el Banco de México le indique.

El Banco de México podrá modificar o actualizar el "Anexo Técnico de Requerimientos de Seguridad Informática" conforme a las necesidades operativas y tecnológicas derivadas de la presente Circular.

Las Instituciones de Crédito y los Usuarios estarán obligados a verificar que los Componentes de Infraestructura de Conexión de las E.T.V. cumplan, en todo momento, con lo establecido en el "Anexo Técnico de los Requerimientos de Seguridad Informática", a través de los esquemas de verificación que la Institución de Crédito establezca.

Los informes detallados del cumplimiento que generen las E.T.V. solo deberán ser entregados a la Institución de Crédito en los casos en los que sean solicitados por el Banco de México a la Institución de Crédito.

**Artículo 126. Controles de seguridad informática alternos a los estipulados en el "Anexo Técnico de los Requerimientos de Seguridad Informática"**

El Banco de México podrá autorizar el uso de otros controles de seguridad informática alternos a los especificados en el Anexo 22, cuyas características, así como el proceso para realizar la solicitud de autorización, son establecidos en el "Anexo Técnico de los Requerimientos de Seguridad Informática".

La Institución de Crédito, el Usuario o el Administrador del Corresponsal que desee obtener la autorización a que se refiere el párrafo anterior, deberá presentar una solicitud por escrito, dirigida a la Gerencia de Autorizaciones y Consultas de Banca Central del Banco de México, conforme a lo que se establece en el "Anexo Técnico de los Requerimientos de Seguridad Informática".

En caso de que el Banco de México no emita su resolución a la solicitud indicada en el párrafo anterior, dentro de los veinte Días Hábiles Bancarios siguientes a la presentación de esta, se entenderá la resolución en sentido negativo. A petición de la Institución de Crédito, el Usuario o Administrador del Corresponsal de que se trate, el Banco de México expedirá constancia de tal circunstancia, dentro de los cinco Días Hábiles Bancarios siguientes a la presentación de la petición respectiva."

**TRANSITORIOS**

**PRIMERO.-** La presente circular entrará en vigor el 1 de enero de 2027.

**SEGUNDO.-** En tanto no entren en vigor las presentes reformas, permanecerán vigentes los Requerimientos de Seguridad Informática versión 2.0.2, dados a conocer a través de los sistemas SIBUC, AUDI y SAM con fecha 24 de septiembre de 2025.

Ciudad de México, a 03 de noviembre de 2026.- BANCO DE MÉXICO: Director General Jurídico, **Erik Mauricio Sánchez Medina**.- Rúbrica.- Directora de Programación y Distribución de Efectivo, **Isabel Morales Pasantes**.- Rúbrica.

Para cualquier consulta sobre el contenido de la presente Circular, el Banco de México se pone a su disposición a través de la Dirección de Autorizaciones y Sanciones de Banca Central al teléfono (55) 5237-2000 extensión 3200.

"**ANEXO 6**

**RECIBO DE RETENCIÓN DE PIEZAS PRESUNTAMENTE FALSAS O PIEZAS ALTERADAS**

Logotipo de la Institución de crédito

ANEXO 6
Página 1 de 2

IMPORTANTE LEER INFORMACIÓN AL REVERSO

RECIBO DE RETENCIÓN DE PIEZAS PRESUNTAMENTE FALSAS O PIEZAS ALTERADAS

(PARA REMITIRSE AL BANCO DE MÉXICO)

| 1 Número de Recibo SAM<br>Código de Barras | Tipo de recibo<br>( ) Retención ( ) Reclamación | Fecha de Retención<br>Día / Mes / Año |
|---|---|---|

2 Tipo de Recibo

DATOS DE LA INSTITUCIÓN DE CRÉDITO QUE RETIENE LA(S) PIEZA(S)

Nombre de la Institución de Crédito:
Nombre y número de sucursal:
Domicilio:
Teléfono (clave):

DATOS DEL TENEDOR

La(s) pieza(s) que le retuvieron puede(n) resultar auténtica(s), de ser así, es importarte localizarle para reembolsarle su importe.

Nombre:
Domicilio:
Teléfono (clave):
Correo electrónico:

3 DATOS DE LA(S) PIEZA(S)

( ) Billete ( ) Moneda

DETALLE DE LA(S) PIEZA(S) PRESUNTAMENTE FALSA(S) O PIEZA(S) ALTERADA(S)

| Cantidad de Piezas | Denominación | Divisa | Folio Billete | Serie | Fecha Emisión | Nota |
|---|---|---|---|---|---|---|
| | | | | | | |

4 SECCIÓN PARA PRESENTAR RECLAMACIÓN POR HABER OBTENIDO PIEZA(S) PRESUNTAMENTE FALSA(S) DE UNA VENTANILLA O DE UN CAJERO AUTOMÁTICO

Fecha de Reclamación: Día / Mes / Año

5 DATOS DE LA INSTITUCIÓN DE CRÉDITO DONDE SE PRESENTA LA RECLAMACIÓN

Nombre de la Institución de Crédito:
Nombre y número de sucursal:
Domicilio:
Teléfono (clave):

Tipo de Operación ( ) Cajero Automático ( ) Ventanilla

Tipo de Identificación ( ) Credencial para Votar ( ) Pasaporte ( ) CURP biométrica ( ) Tarjeta única de identidad militar ( ) Cartilla Militar ( ) Tarjeta de residente Permanente

Número de Identificación: _____

Fecha de Operación: Día / Mes / Año

Describa con el mayor detalle posible cómo obtuvo la(s) pieza(s) presuntamente falsa(s) (fecha, lugar, hora, operación realizada, quién le atendió). Puede anexar más páginas de ser necesario.

_____ _____

6 (Nombre y firma del Tenedor)
Declaro bajo protesta de decir verdad que los datos contenidos en el presente formato son ciertos

(Nombre y firma del cajero receptor)
Denominación de la institución de crédito y sello

ESTIMADO TENEDOR, BANCO DE MÉXICO LE AGRADECE LA ENTREGA VOLUNTARIA DE LAS PIEZAS PRESUNTAMENTE FALSAS O PIEZAS ALTERADAS PARA SU ANÁLISIS.

Original para el Tenedor
Copia para la Institución de Crédito
Copia para el Banco de México "

"**ANEXO 22**

**REQUERIMIENTOS DE SEGURIDAD INFORMÁTICA**

Las Instituciones de Crédito que operen en cualquiera de los sistemas SIBUC, AUDI o SAM deberán cumplir, en todo momento, con los Requerimientos de Seguridad Informática previstos en el presente Anexo, lo anterior con independencia del carácter o rol con el que participen, ya sea como Institución de Crédito, Usuario o Administrador del Corresponsal.

Para tales efectos, las Instituciones de Crédito deberán contar, en todo momento, con al menos una persona que funja como responsable de la seguridad informática de los Componentes de Infraestructura de Conexión, de conformidad con lo especificado en el numeral 1) del párrafo tercero del presente Anexo 22.

Las Instituciones de Crédito deberán documentar e implementar efectivamente controles para:

1) Designar, al menos, una persona responsable en materia de seguridad informática de los Componentes de Infraestructura de Conexión. Lo anterior, conforme a lo especificado en el requerimiento "Personas responsables de la seguridad informática de los sistemas" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

2) Controlar el acceso lógico a la Infraestructura de Cómputo. Lo anterior, de conformidad con lo especificado en el requerimiento sobre el "Control de acceso lógico" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

2 Bis) Bloquear de manera automática la Infraestructura de Cómputo al registrar inactividad. Lo anterior, de conformidad con lo especificado en el requerimiento sobre el "Bloqueo automático" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

2 Ter) Gestionar el acceso a las cuentas de usuario de la Infraestructura de Cómputo, así como sus privilegios y contraseñas. Lo anterior, de conformidad con lo especificado en el requerimiento sobre la "Gestión de cuentas de usuarios y contraseñas en la Infraestructura de Cómputo" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

3) Contar con la documentación que muestre los elementos que conforman a los Componentes de Infraestructura de Conexión, así como la interconexión entre ellos, como son diagramas de red, esquemas o mapas. Lo anterior, de conformidad con lo especificado en el requerimiento sobre los "Diagramas de red, esquemas o mapas de los Componentes de Infraestructura de Conexión" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

3 Bis) Generar, implementar y habilitar las políticas de filtrado de datos en la Infraestructura de Telecomunicaciones para controlar y especificar los flujos de información. Lo anterior, de conformidad con lo especificado en el requerimiento sobre los "Filtros de control de acceso y protocolos de reasignación de direccionamiento IP (NAT)" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

Implementar protocolos de reasignación de direccionamiento IP (NAT) en uno o varios componentes de la Infraestructura de Telecomunicaciones y mantener un listado actualizado que relacione el direccionamiento IP local interno con el direccionamiento IP global externo. Lo anterior, de conformidad con lo especificado en el requerimiento sobre los "Filtros de control de acceso y protocolos de reasignación de direccionamiento IP (NAT)" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

3 Ter) Administrar la Infraestructura de Telecomunicaciones mediante protocolos y mecanismos que permitan controlar, autenticar, autorizar y registrar las actividades de los administradores y operadores. Lo anterior, de conformidad con lo especificado en el requerimiento sobre la "Administración de la Infraestructura de Telecomunicaciones" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

4) Gestionar la continuidad operativa de SIBUC, AUDI y SAM. Lo anterior, conforme a lo establecido en el requerimiento sobre la "Gestión de la continuidad operativa de los sistemas" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

5) Usar protocolos seguros de comunicación en la Infraestructura de Cómputo y prescindir de aquellos que se consideren inseguros. Lo anterior, conforme a lo especificado en el requerimiento sobre los "Protocolos seguros de comunicación" del "Anexo Técnico de los Requerimientos de Seguridad Informática".

6) Llevar a cabo la detección y gestión de vulnerabilidades informáticas en la Infraestructura de Cómputo, a través del uso de herramientas tecnológicas. Lo anterior, conforme a lo especificado en el requerimiento sobre la “Gestión de vulnerabilidades en la Infraestructura de Cómputo”, del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

7) Inhibir la activación de servicios, así como la instalación de cualquier aplicación y software en la Infraestructura de Cómputo, que no sean indispensables para la operación con el SIBUC, AUDI y SAM o para el correcto funcionamiento y/o seguridad del sistema operativo en los equipos de la Infraestructura de Cómputo. Lo anterior, conforme a lo especificado en el requerimiento sobre “Inhibir la instalación de aplicaciones o software no indispensables” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

8) Detectar y gestionar los Incidentes de Ciberseguridad que se presenten en los Componentes de Infraestructura de Conexión, así como contar con mecanismos para minimizar afectaciones a su operación, a sus Componentes de Infraestructura de Conexión y a su información, relacionada con el SIBUC, AUDI y SAM, que pudieran derivar tanto de dichos Incidentes de Ciberseguridad como de aquellos que se presenten en la infraestructura de cualquiera de sus proveedores. Lo anterior, de conformidad con lo especificado en el requerimiento sobre la “Detección y gestión de Incidentes de Ciberseguridad” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

9) Llevar a cabo un registro centralizado de bitácoras en la Infraestructura de Cómputo, así como para identificar patrones anómalos e Incidentes de Ciberseguridad, a través del uso de herramientas tecnológicas. Lo anterior, conforme a lo especificado en el requerimiento sobre el “Registro centralizado de bitácoras” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

10) Realizar pruebas de penetración en la Infraestructura de Cómputo, así como elaborar los planes de trabajo y reportes que deriven de los resultados de dichas pruebas. La periodicidad de las pruebas de penetración, los reportes y su resguardo, y planes de trabajo que se deben emitir con motivo de las mismas, así como las características que deben reunir las personas que ejecuten las mencionadas pruebas de penetración, serán aquellas conforme a lo especificado en el requerimiento sobre las “Pruebas de penetración en la Infraestructura de Cómputo” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

11) Realizar un borrado seguro de la información en la Infraestructura de Cómputo a través del uso de herramientas tecnológicas. Lo anterior, conforme a lo especificado en el requerimiento sobre el “Borrado seguro de la información” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

12) Inhibir, a través de mecanismos lógicos, el uso de dispositivos de almacenamiento extraíbles y periféricos de la Infraestructura de Cómputo. Lo anterior, conforme a lo especificado en el requerimiento sobre la “Inhibición del uso de dispositivos de almacenamiento extraíbles y periféricos de la Infraestructura de Cómputo” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

13) Llevar a cabo la detección de virus informáticos y códigos maliciosos, en la Infraestructura de Cómputo a través del uso de herramientas tecnológicas. Lo anterior, conforme a lo especificado en el requerimiento sobre la “Detección de virus informáticos y códigos maliciosos” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

14) Generar y resguardar bitácoras de los eventos de auditoría referentes a la actividad de las cuentas de usuario del sistema operativo de la Infraestructura de Cómputo. Lo anterior, conforme a lo especificado en el requerimiento sobre la “Generación y resguardo de bitácoras” del “Anexo Técnico de los Requerimientos de Seguridad Informática”.

En adición a lo anterior, las Instituciones de Crédito deberán contar con normativa interna, en la cual estén establecidos todos los controles indicados en los numerales anteriores, en los términos especificados en el requerimiento correspondiente del “Anexo Técnico de los Requerimientos de Seguridad Informática” a que hace referencia cada uno de esos numerales. La citada normativa interna deberá constar por escrito, estar debidamente formalizada conforme a la normativa y procedimientos internos de la propia Institución de Crédito, así como establecer una fecha cierta de inicio de vigencia.”