JUNTA MONETARIA
RESOLUCIÓN JM-91-2024

Inserta en el punto octavo del acta 27-2024, correspondiente a la sesión celebrada por la Junta Monetaria el 24 de julio de 2024.

PUNTO OCTAVO: Superintendencia de Bancos solicita a Junta Monetaria emitir el "Reglamento de Medidas de Seguridad en Canales Electrónicos".

RESOLUCIÓN JM-91-2024. Conocido el oficio número 7422-2024, del 15 de julio de 2024, del Superintendente de Bancos, al que se adjunta el dictamen número 7-2024, de la Superintendencia de Bancos, por medio del cual solicita a esta junta emitir el Reglamento de Medidas de Seguridad en Canales Electrónicos.

LA JUNTA MONETARIA

CONSIDERANDO: Que el artículo 55 de la Ley de Bancos y Grupos Financieros establece, que los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, entre otros, la administración del riesgo operacional, del cual forma parte el riesgo tecnológico, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos;
CONSIDERANDO: Que esta junta mediante resolución JM-104-2021, del 26 de noviembre de 2021, emitió un nuevo Reglamento para la Administración del Riesgo Tecnológico, el cual incorpora, entre otros aspectos, lo relacionado con infraestructura de Tecnologías de la Información (TI), sistemas de información, bases de datos y servicios de TI; seguridad de la información; y, ciberseguridad;
CONSIDERANDO: Que el artículo 20, del Reglamento para la Administración del Riesgo Tecnológico, establece, que las instituciones que realicen operaciones y servicios financieros a través de canales electrónicos, deben implementar como mínimo, mecanismos para la protección y control de la infraestructura de TI, los sistemas de información y las bases de datos, incluyendo la gestión de la ciberseguridad; las medidas de seguridad en el intercambio de información, respaldadas por un certificado digital, cifrado de datos u otro mecanismo que permita garantizar la autenticidad, confidencialidad, integridad y disponibilidad de la información; los programas de educación y divulgación de información para clientes; y, lo relacionado al registro y bitácoras de las transacciones efectuadas;
CONSIDERANDO: Que diversos estándares y mejores prácticas internacionales consideran respecto a los canales electrónicos, entre otros aspectos, lo relacionado a la privacidad y protección de datos; múltiples factores de autenticación; conexiones seguras mediante cifrado; políticas para detección de actividades fraudulentas; políticas y prácticas que respeten la privacidad de la información del cliente; sistemas de detección de fraudes; protocolos de autenticación de dominio; sistemas de alerta temprana para amenazas cibernéticas; medidas para identificar y bloquear los códigos maliciosos; políticas de actualización de software; campañas de concientización a los usuarios sobre prácticas seguras en línea; contraseñas complejas; tecnologías de prevención de intrusiones; y, atención a usuarios de productos y servicios financieros;
CONSIDERANDO: Que es necesario que las instituciones cuenten con un centro de prevención y gestión de fraudes cometidos en contra de estas o de sus usuarios en la realización de operaciones y prestación de servicios financieros; y, con una unidad que atienda las inconformidades que presenten dichos usuarios de productos o servicios financieros, con la finalidad de mitigar los riesgos asociados y proteger el prestigio de la institución,

POR TANTO:

Con base en lo considerado, y con fundamento en lo dispuesto en los artículos 26, incisos l y m, y 64 de la Ley Orgánica del Banco de Guatemala; 55, 56, 57, 113 y 129 de la Ley de Bancos y Grupos Financieros; y tomando en cuenta el oficio número 7422-2024 y el dictamen número 7-2024, ambos de la Superintendencia de Bancos,

RESUELVE:

1. Emitir, conforme anexo a la presente resolución, el **Reglamento de Medidas de Seguridad en Canales Electrónicos.**

2. Autorizar a la secretaría de esta junta para que publique la presente resolución en el diario oficial y en otro periódico, la cual cobrará vigencia el 3 de febrero de 2025.

Romeo Augusto Archila Navarro
Secretario
Junta Monetaria

Publicada en el Diario de Centro América el 1 de agosto de 2024

ANEXO A LA RESOLUCIÓN JM- 91- 2024

REGLAMENTO DE MEDIDAS DE SEGURIDAD EN CANALES ELECTRÓNICOS

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. Este reglamento tiene por objeto regular las medidas mínimas que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deben cumplir para administrar la seguridad en canales electrónicos en la realización de operaciones y prestación de servicios financieros, para fortalecer la gestión del riesgo tecnológico; establecer medidas relacionadas con la prevención y gestión de fraudes; y, con la atención de inconformidades de usuarios de productos y servicios financieros.

Artículo 2. Definiciones. Para los efectos de este reglamento se establecen las definiciones siguientes:

Amenaza: causa potencial de un incidente no deseado que puede provocar daños a la institución.

Canales electrónicos: medios que permiten la realización de transacciones, la prestación de servicios financieros y el intercambio de información utilizando plataformas electrónicas.

Factores de autenticación: información utilizada para verificar la identidad del individuo, estos pueden ser por:

a) **Conocimiento:** algo que conoce, como una contraseña o Número de Identificación Personal (PIN, por sus siglas en inglés), entre otros.

b) **Posesión:** algo que posee, como una tarjeta de débito o un teléfono móvil, entre otros.

c) **Inherencia:** algo inherente a este, como su huella dactilar o reconocimiento facial, entre otros.

Fraude de carácter operacional: actos que perjudiquen a la institución o a sus usuarios de productos y servicios financieros, tales como, pero no circunscritos a, operaciones no autorizadas con pérdidas pecuniarias; ingreso no autorizado o con niveles excesivos a los sistemas de información; falsificaciones; apropiación de cuentas o de identidad; daños malintencionados por intromisión en los sistemas informáticos incluyendo canales electrónicos; o, ingeniería social.

El fraude de carácter operacional se podrá denominar en forma simplificada como “fraude” o “fraudes”.

Institución o instituciones: se refiere a los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore y las empresas especializadas en servicios financieros que forman parte de un grupo financiero.

Perfil transaccional: conjunto de características asociadas al comportamiento habitual del usuario de productos y servicios financieros, de acuerdo con los análisis sistematizados realizados por la institución.

Usuarios de productos y servicios financieros: personas individuales o jurídicas que utilizan los productos y/o servicios financieros de la institución, sin que necesariamente existan transferencias de fondos o mantengan una relación contractual con la institución.

Vulnerabilidad: debilidad en un sistema o control que puede ser explotado de forma malintencionada para comprometer la confidencialidad, disponibilidad o integridad de la información.

CAPÍTULO II
ORGANIZACIÓN

Artículo 3. Políticas y procedimientos. Las instituciones considerando la naturaleza, complejidad y volumen de sus operaciones, deberán establecer e implementar políticas y procedimientos que les permitan realizar permanentemente una adecuada:

a) Administración de la seguridad en canales electrónicos, como complemento a lo establecido en el Reglamento para la Administración del Riesgo Tecnológico;

b) Prevención del riesgo de fraude en contra de la institución o de sus usuarios de productos y servicios financieros; asimismo, la gestión de los fraudes cometidos; y,

c) Atención de inconformidades de sus usuarios de productos y servicios financieros.

Dichas políticas y procedimientos deberán comprender, como mínimo, lo establecido en este reglamento.

El Consejo de Administración o quien haga sus veces, en lo sucesivo el Consejo, es el responsable de velar porque se implemente e instruir para que se mantenga en adecuado funcionamiento y ejecución lo establecido en este artículo.

Artículo 4. Responsabilidad del Consejo de Administración. El Consejo como mínimo deberá:

a) Aprobar las políticas y procedimientos a que se refiere el artículo anterior, así como, conocer y resolver sobre las propuestas de actualización y autorizar las modificaciones respectivas;

b) Conocer los reportes que le remita el Comité de Gestión de Riesgos sobre la administración de la seguridad en canales electrónicos mediante los cuales la institución proporciona productos y servicios financieros; las vulnerabilidades y amenazas que puedan comprometer la seguridad en dichos canales electrónicos y su evolución en el tiempo; así como, las medidas correctivas adoptadas;

c) Conocer los reportes que le remita el Comité de Gestión de Riesgos u otro comité que el Consejo designe, sobre fraudes cometidos en contra de la institución o de sus usuarios de productos y servicios financieros, las distintas tipologías y su evolución en el tiempo, así como las medidas correctivas adoptadas.

   Cuando el Consejo designe otro comité para atender lo relacionado con prevención del riesgo de fraude en contra de la institución o de sus usuarios de productos y servicios financieros, asimismo, con la gestión de los fraudes

cometidos, dicho comité deberá cumplir las atribuciones indicadas en el artículo 5 de este reglamento que estén relacionadas con dicho tema;

d) Conocer los reportes que le remita el Comité de Gestión de Riesgos sobre la atención de inconformidades de los usuarios de productos y servicios financieros que puedan afectar el prestigio de la institución, el seguimiento y respuesta correspondiente;

e) Conocer los reportes sobre el nivel de cumplimiento de las políticas y procedimientos aprobados, así como las propuestas de acciones a adoptar con relación a los incumplimientos. Asimismo, en caso de incumplimiento el Consejo deberá adoptar las medidas que correspondan, sin perjuicio de las sanciones legales que el caso amerite;

f) Instituir un centro o área de monitoreo y prevención del riesgo de fraude, asignar las atribuciones y recursos para el adecuado desarrollo de sus funciones, así como designar al funcionario responsable del mismo;

g) Instituir una unidad o área de atención de usuarios de productos y servicios financieros, asignar sus atribuciones y recursos para el adecuado desarrollo de sus funciones, designar al funcionario responsable de la misma, así como establecer los plazos de respuesta oportuna sobre las inconformidades presentadas por los usuarios de productos y servicios financieros de la institución; y,

h) Aprobar los modelos de canales electrónicos o sus modificaciones sustanciales previo a su implementación, de acuerdo con las políticas establecidas por la institución. Se exceptúan de la aprobación previa, aquellas modificaciones que deben realizarse de forma inmediata para evitar pérdidas financieras a la institución o a sus usuarios de productos y servicios financieros, las cuales, a la brevedad posible, se harán de conocimiento del Consejo para su aprobación.

Las actuaciones del Consejo deberán hacerse constar en el acta correspondiente a cada reunión, haciendo referencia a los antecedentes, fundamentos y demás consideraciones para la toma de decisiones.

Artículo 5. Responsabilidad del Comité de Gestión de Riesgos. El Comité de Gestión de Riesgos, en lo sucesivo el Comité, tendrá a su cargo la dirección, implementación, ejecución y adecuado funcionamiento de las políticas y procedimientos a que hace referencia el artículo 3 de este reglamento, para lo cual tendrá las funciones siguientes:

a) Someter al Consejo, para su aprobación, las políticas y procedimientos descritos en el artículo 3 de este reglamento, así como revisarlas, al menos anualmente, y proponer las actualizaciones que correspondan;

b) Proponer al Consejo la actualización del Manual para la Administración del Riesgo Tecnológico que se derive de la administración de la seguridad en canales electrónicos; y, lo relacionado a los incisos b) y c) del artículo 3 de este reglamento en el Manual para la Administración del Riesgo Operacional;

c) Definir la estrategia para la implementación de las políticas y procedimientos aprobados y su adecuado cumplimiento;

d) Analizar los reportes que le remita la Unidad de Administración de Riesgos, a que se refiere el artículo 6 de este reglamento, sobre la administración de la

seguridad en canales electrónicos mediante los cuales la institución proporciona productos y servicios financieros; las vulnerabilidades y amenazas que puedan comprometer la seguridad en dichos canales electrónicos; su evolución en el tiempo; así como, las medidas correctivas adoptadas;

e) Analizar la información que le remita la Unidad de Administración de Riesgos sobre el cumplimiento de las políticas y procedimientos aprobados, así como evaluar las causas de los incumplimientos que hubiere, y proponer al Consejo las acciones a adoptar con relación a dichos incumplimientos;

f) Analizar los reportes que le remita el centro o área de monitoreo y prevención del riesgo de fraude, a que se refiere el artículo 13 de este reglamento, sobre los fraudes cometidos en contra de la institución o de sus usuarios de productos y servicios financieros, las distintas tipologías y su evolución en el tiempo, así como las medidas adoptadas por dicho centro o área; y, cuando corresponda instruir sobre la adopción de medidas adicionales;

g) Analizar los reportes que le remita la Unidad de Administración de Riesgos, sobre las inconformidades presentadas por los usuarios de productos y servicios financieros que puedan afectar el prestigio de la institución; las distintas tipologías y su evolución en el tiempo; así como el seguimiento y respuesta correspondiente; y, cuando corresponda instruir sobre la adopción de medidas adicionales;

h) Reportar al Consejo, al menos semestralmente o cuando la situación lo amerite, el resultado de los análisis descritos en los incisos anteriores de este artículo; e,

i) Otras funciones relacionadas que le asigne el Consejo.

Las sesiones y acuerdos del Comité deberán constar en acta suscrita por quienes intervinieron en la sesión, haciendo referencia a los antecedentes, fundamentos y demás consideraciones para la toma de decisiones.

Artículo 6. Responsabilidad de la Unidad de Administración de Riesgos. La Unidad de Administración de Riesgos apoyará al Comité, para lo cual tendrá las funciones siguientes:

a) Someter al Comité las políticas y procedimientos establecidos en los incisos a) y c) del artículo 3, de este reglamento, así como revisarlas al menos anualmente y proponer las actualizaciones correspondientes;

b) Analizar la información proporcionada por el Centro de Operaciones de Seguridad Cibernética de las vulnerabilidades y amenazas que puedan comprometer la seguridad en canales electrónicos y mantener los registros históricos correspondientes;

c) Analizar las vulnerabilidades y amenazas asociadas a la seguridad en los canales electrónicos previo a su implementación y cuando se produzcan cambios sustanciales en los mismos;

d) Verificar e informar al Comité, al menos trimestralmente y cuando la situación lo amerite, sobre el nivel de cumplimiento de las políticas y procedimientos aprobados;

e) Identificar las causas del incumplimiento de las políticas y procedimientos aprobados, determinar si los mismos se presentan en forma reiterada e incluir sus resultados en el informe indicado en el inciso anterior y proponer las medidas correctivas, debiendo mantener registros históricos sobre tales incumplimientos;

f) Analizar los reportes que le remita la unidad o área de atención de usuarios de productos y servicios financieros, a que se refiere el artículo 14 de este reglamento, sobre las inconformidades presentadas por los usuarios de productos y servicios financieros que puedan afectar el prestigio de la institución, las distintas tipologías y su evolución en el tiempo;

g) Reportar al Comité, al menos trimestralmente o cuando la situación lo amerite, el resultado de los análisis descritos en los incisos anteriores de este artículo; y,

h) Otras funciones relacionadas que le asigne el Comité.

CAPÍTULO III
ADMINISTRACIÓN DE LA SEGURIDAD EN CANALES ELECTRÓNICOS

Artículo 7. Requisitos previos a la implementación de servicios en canales electrónicos. Previo a la implementación de servicios en canales electrónicos o de sus cambios sustanciales, adicional a los requerimientos que se establecen en el Reglamento para la Administración del Riesgo Tecnológico, las instituciones deben realizar y documentar lo siguiente:

a) El análisis de vulnerabilidades y amenazas, incluyendo las pruebas de penetración correspondientes;

b) Las pruebas de código seguro, dinámico y estático;

c) Las pruebas de funcionalidad;

d) El plan de retorno al estado funcional anterior del canal electrónico; y,

e) El modelo del servicio en canales electrónicos o sus modificaciones sustanciales aprobadas por el Consejo, de acuerdo con las políticas aprobadas por este.

Artículo 8. Modelo del servicio en canales electrónicos: El modelo o sus modificaciones sustanciales indicados en el inciso e) del artículo anterior debe incluir, como mínimo, lo siguiente:

a) Esquema operativo de los servicios que contemple el flujo de información;

b) Diagrama de interrelación entre los diferentes componentes tecnológicos;

c) Mecanismos de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información;

d) Descripción de la plataforma tecnológica, interfaces, hardware y software a utilizar; y,

e) Manual de usuario final.

Artículo 9. Medidas para la administración de la seguridad en canales electrónicos. Las instituciones, para fortalecer la administración de la seguridad en canales electrónicos, a excepción de los cajeros automáticos y puntos de venta en los que se utilicen tarjetas de crédito o de débito (*PoS*, por sus siglas en inglés), deben establecer medidas que contengan, como mínimo, los aspectos siguientes:

a) Implementar múltiples factores de autenticación de usuario de productos y servicios financieros, para los diferentes canales electrónicos a través de métodos de autenticación.

   Los métodos indicados en el párrafo anterior pueden ser, entre otros, basado en el perfil transaccional; por dispositivo autorizado; o, el permanente por solicitud, entendiéndose por este último método que, el factor de autenticación será necesario para cada actividad que realice el usuario de productos y servicios financieros.

   Los métodos de autenticación, utilizados para verificar la identidad de un usuario de productos y servicios financieros, deberán solicitarse principalmente en los casos siguientes:

   1. Solicitud de afiliación o desafiliación de productos y servicios financieros, así como la aceptación de estas condiciones de uso;

   2. Modificaciones a la información del usuario de productos y servicios financieros;

   3. Cambios en los parámetros relacionados con el perfil transaccional;

   4. Creación, habilitación y rehabilitación de los factores de autenticación;

   5. Adición de cuentas para transferencias;

   6. Confirmación de operaciones que se desvíen del perfil transaccional, de acuerdo con las políticas aprobadas; y,

   7. Otros que la institución estime pertinente que puedan afectar la seguridad de los canales electrónicos.

b) Utilizar canales de comunicación cifrados para proteger la comunicación de los usuarios de productos y servicios financieros y de los componentes lógicos que soportan canales electrónicos;

c) Requerir al usuario de productos y servicios financieros la adopción de contraseñas complejas y sistematizar su cambio periódico, o bien, requerir otro factor de autenticación que permita verificar la identidad del usuario;

d) Implementar protocolos para garantizar que los correos electrónicos enviados desde el dominio de la institución sean auténticos y seguros;

e) Mantener todos los sistemas y software con sus respectivas actualizaciones de seguridad estables para mitigar vulnerabilidades, o en su defecto, implementar temporalmente controles compensatorios; en este último caso, la institución deberá asegurarse que se implementen oportunamente dichas actualizaciones de seguridad;

f) Implementar medidas de bloqueo temporal de acceso a uno o más canales electrónicos del usuario de productos y servicios financieros cuando:

1. Existan varios intentos de acceso fallidos;

2. Se identifique que las credenciales de acceso o información de sus usuarios de productos y servicios financieros puedan estar comprometidas derivado de un ataque cibernético, suplantación de identidad u otras causas;

3. Se detecte comportamiento inusual o irregular de acuerdo con el perfil transaccional; o,

4. Otras que la institución considere.

Cuando la situación lo amerite, la institución deberá tomar medidas adicionales como inhabilitar temporalmente todos los canales electrónicos del usuario de productos y servicios financieros hasta que confirme la identidad de este y la autenticidad de sus acciones;

g) Implementar sistemas de alertas que permitan identificar oportunamente movimientos inusuales de acuerdo con el perfil transaccional;

h) Implementar mecanismos para proteger los canales electrónicos contra ataques cibernéticos que pretendan afectar la confidencialidad, disponibilidad e integridad de la información, considerando tecnologías que permitan la prevención y/o bloqueo de intrusiones, código malicioso y conexiones no autorizadas, entre otras;

i) Restringir conexiones hacia los canales electrónicos desde dispositivos o redes identificadas previamente como fuentes de actividad maliciosa;

j) Segregar los componentes tecnológicos de los canales electrónicos, en redes perimetrales independientes de las redes internas de la institución;

k) Contar con bitácoras que permitan la trazabilidad de las actuaciones realizadas por los usuarios de productos y servicios financieros en canales electrónicos de la institución, que incluyan, como mínimo, los campos siguientes:

1. Identificador del usuario;

2. Hora y fecha;

3. Identificación del origen de la sesión, que incluya al menos, la dirección *IP*, la dirección *MAC* del dispositivo y tipo de aplicativo (web o móvil);

4. Tipo de actividad;

5. Monto; y,

6. Destino de transacción.

El período de conservación de estas bitácoras deberá ser definido de acuerdo a las políticas de la institución, de manera que la información almacenada permita ser utilizada para dar respuesta a las inconformidades de usuarios de productos y servicios financieros con relación al uso de canales electrónicos;

l) Implementar protocolos para identificar dominios de Internet, páginas web, aplicaciones móviles u otras plataformas que suplanten la identidad de la institución, así como gestionar la baja de estos; y,

m) Implementar procedimientos y mecanismos para monitorear y detectar información sensible de la institución o de sus usuarios de productos y servicios financieros comprometida en redes externas identificadas previamente como fuentes de actividad maliciosa.

Artículo 10. Medidas para la administración de la seguridad en cajeros automáticos y puntos de venta. Las instituciones deberán establecer las políticas y procedimientos que contengan las medidas para fortalecer la seguridad de los cajeros automáticos y puntos de venta en los que se utilicen tarjetas de crédito o de débito (*PoS*, por sus siglas en inglés).

Dichas políticas deberán contener, como mínimo, los controles transaccionales de seguridad exigidos por las marcas internacionales de tarjetas de crédito y de débito con las que opera la institución.

Artículo 11. Enrolamiento digital. Cuando las instituciones permitan la identificación de potenciales usuarios de productos y servicios financieros en forma digital y no presencial, deberán diseñar procesos para comprobar la veracidad de los datos o elementos requeridos al potencial usuario que se pretende identificar.

Durante el proceso de identificación, la institución deberá aplicar controles para determinar, como mínimo, lo siguiente:

a) Validación de la presencia real del potencial usuario con prueba de vida;

b) Confirmación de los medios de contacto y del dispositivo móvil declarados por el potencial usuario;

c) Validación de los elementos biométricos; y,

d) Validación de la identidad con la información inscrita en la entidad pública responsable del registro nacional de identidad de las personas.

Se podrán utilizar controles complementarios para verificar la identidad del potencial usuario en el proceso de enrolamiento digital, de acuerdo con la efectividad de los controles implementados.

Artículo 12. Responsabilidad de terceros. Sin perjuicio de lo establecido en el Reglamento para la Administración del Riesgo Tecnológico, cuando se trate de contrataciones con terceros relacionadas con canales electrónicos o la prestación de servicios a personas individuales o jurídicas que utilicen interfaces de conexión con los sistemas de información de la institución, esta última estará obligada a realizar la debida diligencia a efecto de cerciorarse que dichos terceros o personas apliquen medidas de seguridad, tomando en cuenta lo dispuesto en este reglamento, debiendo establecerlo en las cláusulas pertinentes de los contratos que para el efecto se celebren.

CAPÍTULO IV
FRAUDES Y ATENCIÓN DE INCONFORMIDADES DE USUARIOS DE PRODUCTOS Y SERVICIOS FINANCIEROS

Artículo 13. Centro o área de monitoreo y prevención del riesgo de fraude. El centro o área de monitoreo y prevención del riesgo de fraude, instituido por el Consejo, deberá contar con personal capacitado y competente, así como disponer

de medios y procedimientos para prevenir el riesgo de fraude y gestionar los fraudes cometidos.

El centro o área de monitoreo y prevención del riesgo de fraude dependerá de la gerencia que el Consejo designe, para lo cual tendrá, como mínimo, las funciones siguientes:

a) Proponer al Comité de Gestión de Riesgos u otro comité que el Consejo designe las políticas y procedimientos para la prevención del riesgo de fraude y gestión de fraudes cometidos en contra de la institución o de sus usuarios de productos y servicios financieros;

b) Reportar al Comité de Gestión de Riesgos u otro comité que el Consejo designe, de forma mensual o cuando la situación lo amerite, sobre el resultado de su labor;

c) Monitorear las actividades y transacciones de los usuarios de productos y servicios financieros a fin de detectar aquellas fuera de los parámetros de su perfil transaccional con el propósito de prevenir el riesgo de fraude;

d) Establecer parámetros a efecto de requerir al usuario de productos y servicios financieros factores de autenticación adicionales que le permitan acceder y operar en canales electrónicos cuando se detecte una actividad inusual de acuerdo con su perfil transaccional;

e) Establecer sistemas de alertas que permitan identificar, prevenir y reducir oportunamente el riesgo de fraude en contra de la institución o de sus usuarios de productos y servicios financieros;

f) Actualizar periódicamente los parámetros de monitoreo con base en los patrones de fraude ocurridos y otras fuentes externas;

g) Notificar al Oficial de Seguridad de la Información acerca de los eventos de fraude detectados en canales electrónicos;

h) Notificar a los usuarios de productos y servicios financieros, por los medios que estime pertinentes, ante la sospecha de una actividad fraudulenta;

i) Analizar, investigar, documentar y dar respuesta a los casos relacionados con fraudes, que le remita la unidad o área de atención de usuarios de productos y servicios financieros;

j) Proponer al Comité de Gestión de Riesgos u otro comité que el Consejo designe, las medidas preventivas y correctivas aplicables que permitan proteger las cuentas de los usuarios de productos y servicios financieros ante la ocurrencia de fraudes;

k) Llevar un registro de fraudes ocurridos clasificados por tipología;

l) Documentar cada caso atendido; y,

m) Otras atribuciones que le asigne el Consejo o la gerencia de la cual depende.

La institución podrá utilizar la infraestructura organizacional necesaria que le permita dar cumplimiento a lo establecido en este artículo.

Artículo 14. Unidad o área de atención de usuarios de productos y servicios financieros. La unidad o área de atención de usuarios de productos y servicios financieros, instituida por el Consejo, deberá contar con personal capacitado y competente para atender al usuario de productos y servicios financieros.

Dicha unidad dependerá de la gerencia que el Consejo designe, será la encargada, principalmente, de la recepción, análisis y respuesta a las inconformidades presentadas por los usuarios de productos y servicios financieros de la institución, en los plazos definidos por dicho Consejo; y, tendrá, como mínimo, las funciones siguientes:

a) Proponer a la Unidad de Administración de Riesgos las políticas y procedimientos para la atención de las inconformidades presentadas por los usuarios de productos y servicios financieros que puedan afectar el prestigio de la institución;

b) Reportar a la Unidad de Administración de Riesgos, de forma mensual o cuando la situación lo amerite, sobre el resultado de su labor de los aspectos que puedan afectar el prestigio de la institución;

c) Trasladar al centro o área de monitoreo y prevención del riesgo de fraude, para su investigación y respuesta, los casos relacionados con este;

d) Documentar cada caso atendido y llevar un registro de las inconformidades clasificadas por tipología;

e) Coadyuvar a la implementación y mejora continua de los programas de educación y divulgación de información para usuarios de productos y servicios financieros, que incluya entre otros aspectos, la seguridad de la información en el uso de sus canales electrónicos y otra información relacionada con el registro de inconformidades atendidas con la finalidad de disminuir la cantidad de estas; y,

f) Otras atribuciones que le asigne el Consejo o la gerencia de la cual depende, relacionadas con la atención de usuarios de productos y servicios financieros.

CAPÍTULO V
OTRAS DISPOSICIONES

Artículo 15. Funciones de la auditoría interna. Sin perjuicio de las funciones establecidas en el Reglamento de Gobierno Corporativo, la auditoría interna verificará, por lo menos una vez al año, el cumplimiento de lo establecido en el presente reglamento, debiendo realizar principalmente auditorías para evaluar la eficacia de los procesos en la administración de las medidas de seguridad implementadas en canales electrónicos.

Artículo 16. Funciones del Oficial de Seguridad de la Información. Sin perjuicio de las funciones establecidas en el Reglamento para la Administración del Riesgo Tecnológico, el Oficial de Seguridad de la Información debe coordinar el cumplimiento de las políticas y procedimientos de seguridad en canales electrónicos, así como tomar las acciones correspondientes de las notificaciones que reciba del centro o área de monitoreo y prevención del riesgo de fraude, en el ámbito de su competencia.

Artículo 17. Envío de información a la Superintendencia de Bancos. Las instituciones deberán enviar a la Superintendencia de Bancos información

relacionada con este reglamento conforme a las instrucciones generales que el órgano supervisor les indique.

El envío de información establecido en el párrafo anterior no exime a la institución de cumplir con otras disposiciones legales o normativas aplicables.

CAPÍTULO VI
DISPOSICIONES TRANSITORIAS Y FINAL

Artículo 18. Transitorio. Las instituciones deberán enviar a la Superintendencia de Bancos, a más tardar el 28 de febrero de 2025, el Manual para la Administración del Riesgo Tecnológico y el Manual para la Administración del Riesgo Operacional, ambos actualizados conforme lo dispuesto en este reglamento.

Artículo 19. Transitorio. Las instituciones deberán ajustarse a lo establecido en los incisos a), f) y g) del artículo 9 de este reglamento a más tardar el 16 de febrero de 2026.

Artículo 20. Casos no previstos. Los casos no previstos en este reglamento serán resueltos por la Junta Monetaria, previo informe de la Superintendencia de Bancos.