# JUNTA MONETARIA
## RESOLUCIÓN JM-99-2025

Inserta en el punto noveno del acta 46-2025, correspondiente a la sesión celebrada por la Junta Monetaria el 22 de octubre de 2025.

**PUNTO NOVENO: Superintendencia de Bancos solicita a Junta Monetaria modificar el Reglamento de Medidas de Seguridad en Canales Electrónicos, emitido mediante resolución JM-91-2024.**

**RESOLUCIÓN JM-99-2025.** Conocido el oficio número 8810-2025, del 9 de octubre de 2025, del Superintendente de Bancos, al que se adjunta el dictamen número 17-2025 de la Superintendencia de Bancos, por medio del cual solicita a esta junta modificar el Reglamento de Medidas de Seguridad en Canales Electrónicos, emitido mediante resolución JM-91-2024.

### 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 el Reglamento para la Administración del Riesgo Tecnológico en relación a operaciones y servicios financieros a través de canales electrónicos, estipula que las instituciones que realicen operaciones y servicios financieros por estos medios, deben implementar, entre otros, mecanismos para la protección y control de la infraestructura de Tecnologías de Información (TI); **CONSIDERANDO:** Que esta junta mediante resolución JM-91-2024, del 24 de julio de 2024, emitió el Reglamento de Medidas de Seguridad en Canales Electrónicos, a efectos de normar las medidas mínimas que las instituciones 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; **CONSIDERANDO:** Que dada la actualización de los estándares internacionales relacionados a seguridad de la información y ciberseguridad, los cuales brindan un conjunto de mejores prácticas, directrices y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información, así como asegurar que las decisiones y acciones sean trazables, es pertinente incorporar al marco normativo tales actualizaciones; **:** Que existen limitaciones técnicas y de privacidad que impiden obtener la dirección MAC de los dispositivos de los clientes y usuarios de servicios financieros de las instituciones; no obstante, derivado de la evolución de las herramientas tecnológicas que permiten su actualización de forma constante, existen mecanismos alternativos validados que permiten contar con la trazabilidad de las actuaciones realizadas por dichos usuarios en canales electrónicos; **CONSIDERANDO:** Que el dictamen número 17-2025, de la Superintendencia de Bancos, concluye que es pertinente que se modifique el Reglamento de Medidas de Seguridad en Canales Electrónicos, en el sentido de que la identificación única del dispositivo de los clientes y usuarios pueda realizarse por un conjunto de atributos relevantes que aseguren su trazabilidad,

### 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 y 129 de la Ley de Bancos y Grupos Financieros; y tomando en cuenta el oficio número 8810-2025 y el dictamen número 17-2025, ambos de la Superintendencia de Bancos,

### RESUELVE:

1. Modificar el artículo 9 al Reglamento de Medidas de Seguridad en Canales Electrónicos, emitido en resolución JM-91-2024, en el sentido siguiente:

   **"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 única del dispositivo, conformada por un conjunto de atributos relevantes que aseguren la referida trazabilidad;
      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."

2. Autorizar a la secretaría de esta junta para que publique la presente resolución en el diario oficial y en otro periódico, la cual entrará en vigencia el día de su publicación.

BANCO DE GUATEMALA - Junta Monetaria - GUATEMALA, C. A.

Romeo Augusto Archila Navarro
Secretario
Junta Monetaria



(331522)-30 octubre