SUPERINTENDENCIA DE BANCOS

Circular Nro. SB-DS-2026-0011-C

Quito D.M., 19 de mayo de 2026

Asunto: Medidas preventivas ante amenazas cibernéticas difundidas por redes sociales y canales digitales

Entidades de los Sistemas Financieros Privado, Público y de Seguridad Social

De mi consideración:

Un cordial saludo desde la Superintendencia de Bancos

En atención al artículo 60 del Código Orgánico Monetario y Financiero, que establece como finalidad de la Superintendencia de Bancos: *"(…) velar por la estabilidad, solidez, solvencia y seguridad de los sectores financieros público y privado nacional y de las entidades que lo conforman. Para ello, efectuará la vigilancia, auditoria, intervención, control y supervisión de las actividades financieras que ejercen las entidades del sistema financiero nacional, con el propósito de que estas actividades atiendan al interés general, se sujeten al ordenamiento jurídico, y de evitar, prevenir y desincentivar prácticas fraudulentas y prohibidas con el fin de proteger los derechos de los usuarios y/o clientes del sistema financiero nacional."*

Ante el incremento de amenazas cibernéticas que circulan actualmente a través de redes sociales, aplicaciones de mensajería, correos electrónicos, sitios web falsos y otros canales digitales, se dispone a las entidades bancarias privadas, públicas, fondos complementarios cerrados e institutos de seguridad social adoptar medidas inmediatas de prevención, monitoreo y protección de sus sistemas tecnológicos, plataformas transaccionales e información sensible.

Estas amenazas pueden incluir campañas de phishing, suplantación de identidad institucional, enlaces maliciosos, ingeniería social, malware, ransomware, difusión de noticias falsas, perfiles falsos, mensajes fraudulentos dirigidos a clientes y funcionarios, así como intentos de acceso no autorizado a sistemas internos.

En tal virtud, se solicita implementar y reforzar, de manera prioritaria, las siguientes acciones:

1. **Fortalecer el monitoreo permanente de redes sociales y canales digitales**, a fin de identificar publicaciones, mensajes, perfiles o enlaces que suplanten la identidad de la institución o busquen inducir a error a clientes y usuarios.
2. **Reforzar la seguridad de los sistemas críticos**, incluyendo banca en línea, aplicaciones móviles, sistemas de pagos, plataformas de atención al cliente, bases de datos, redes internas, servidores y servicios expuestos a internet.
3. **Garantizar la protección de la información de clientes y de la institución**, aplicando controles de acceso, cifrado, segmentación de redes, autenticación multifactor, gestión segura de credenciales y revisión continua de privilegios.
4. **Actualizar de forma inmediata sistemas operativos, aplicaciones, firewalls, antivirus, herramientas EDR/XDR, plataformas de monitoreo y demás componentes tecnológicos**, aplicando parches de seguridad conforme a la criticidad de las vulnerabilidades identificadas.
5. **Activar o reforzar los centros de monitoreo de seguridad**, incluyendo equipos SOC, SIEM, análisis de logs, alertas tempranas, detección de comportamientos anómalos y respuesta ante incidentes.
6. **Realizar campañas urgentes de concienciación dirigidas a clientes, funcionarios y proveedores**, advirtiendo sobre mensajes falsos, enlaces sospechosos, solicitudes de claves, códigos de verificación, transferencias inusuales o descargas no autorizadas.
7. **Verificar la autenticidad de las comunicaciones institucionales**, utilizando únicamente canales oficiales y evitando la difusión de información no confirmada que pueda generar confusión, pánico financiero o exposición reputacional.
8. **Revisar y actualizar los planes de respuesta ante incidentes cibernéticos**, asegurando la disponibilidad de equipos técnicos, jurídicos, comunicacionales y ejecutivos para actuar oportunamente ante cualquier evento.
9. **Ejecutar respaldos seguros, cifrados y probados**, garantizando que la información crítica pueda ser

Circular Nro. SB-DS-2026-0011-C

Quito D.M., 19 de mayo de 2026

recuperada en caso de ataques de ransomware, sabotaje, pérdida de datos o indisponibilidad de servicios.

10. **Reportar de manera inmediata cualquier incidente, intento de ataque, campaña fraudulenta o vulnerabilidad relevante** a las autoridades competentes y a las áreas internas responsables de seguridad de la información, cumplimiento y gestión de riesgos.

Se recuerda que la protección de la infraestructura tecnológica y de la información financiera constituye una responsabilidad prioritaria para preservar la confianza del público, la continuidad operativa, la estabilidad del sistema financiero y la seguridad de los clientes.

Las máximas autoridades de cada institución deberán disponer la ejecución inmediata de las medidas antes señaladas, así como mantener vigilancia permanente sobre nuevas amenazas que pudieran afectar la integridad, disponibilidad y confidencialidad de los servicios financieros.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Econ. Roberto José Romero von Buchwald
SUPERINTENDENTE DE BANCOS

Copia:

Magister
Francisco Xavier Garzón Cisneros
Intendente General

Magister
Jessenia Marlene Cazco Arízaga
Intendente Nacional de Riesgos y Estudios

Magister
Delia María Peñafiel Guzmán
Secretaria General

Master
Patricio Chanabá Paredes
Director Ejecutivo
ASOCIACIÓN DE INSTITUCIONES DE MICROFINANZAS / ASOMIF

Doctor
Marco Antonio Rodríguez Proaño
Presidente Ejecutivo
ASOCIACIÓN DE BANCOS PRIVADOS DEL ECUADOR - ASOBANCA

Doctora
María de los Angeles Haro Jaramillo
Asesor 2

jc/fg

SUPERINTENDENCIA DE BANCOS
Documento Firmado electrónicamente por ROBERTO JOSE ROMERO VON BUCHWALD