Señores
COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC
Ciudad

Asunto: Observaciones Proyecto CRC Identificación medidas mitigación fraude cibernético por servicios móviles

Respetados señores:

Encontrándonos en término, en atención a su solicitud, de manera atenta nos permitimos remitir observaciones al Proyecto CRC "*Identificación medidas mitigación fraude cibernético por servicios móviles",* para los fines pertinentes, las cuales enfocan en la necesidad de fortalecer las medidas propuestas para mejorar la seguridad de las comunicaciones móviles, especialmente en un contexto donde los usuarios reciben información sensible y realizan transacciones a través de estos canales.

1. Se sugiere que el proyecto de circular incluya medidas concretas que mejoren la seguridad de los mensajes de texto (SMS), muchas entidades aún utilizan este canal para enviar claves temporales o notificaciones importantes, es clave asegurar que estos mensajes no puedan ser interceptados o falsificados. Es necesario implementar mecanismos que aseguren que el mensaje que recibe el usuario realmente proviene de una fuente confiable como cifrado punto a punto, autenticación del emisor y monitoreo del tráfico.

2. Es fundamental que se exija a los proveedores de servicios móviles implementar mecanismos de autenticación del origen de los mensajes y llamadas, siguiendo modelos internacionales como STIR/SHAKEN.

3. El documento se enfoca principalmente en los operadores de telecomunicaciones, pero debería también considerar a las empresas que usan estos servicios para comunicarse con sus clientes. Es importante que estas entidades tengan claro qué deben exigir a sus proveedores para garantizar comunicaciones seguras, incluyendo guías de mejores prácticas y responsabilidades compartidas con los PRSTM, PCA e IT.

4. Se recomienda que se establezca un protocolo nacional de notificación a entidades financieras y otras entidades críticas cuando se detecten recursos de identificación (línea, número, etc.) involucrados en campañas fraudulentas. Esto permitiría actuar con mayor rapidez y evitar que más usuarios sean engañados.

5. En lo relativo al tema de que las empresas contratan a terceros para enviar mensajes a sus clientes, se sugiere incluir recomendaciones explicitas para que estas contrataciones incluyan condiciones claras de seguridad, que los mensajes no puedan ser modificados y que no se usen números sin control, requisitos explícitos para la administración y uso de numeración asignada (outsourcing de mensajería A2P) tales como validación del uso autorizado y control de integridad del contenido transmitido.

6. Aunque los mensajes de texto se siguen usando mucho, ya no son el canal más seguro para enviar claves o códigos de acceso. Se recomienda en consecuencia que el

documento invite (o exija) a las entidades a usar otras formas más seguras de autenticar a los usuarios, como aplicaciones móviles que generan códigos, envían notificaciones seguras o autenticadores físicos.

7. Se solicita incluir en la estrategia de mitigación una obligación de trazabilidad técnica detallada de los mensajes y llamadas, con acceso en línea a registros por parte de entidades afectadas como mecanismo de respuesta ante incidentes, de esta manera seria de gran ayuda para investigar más rápido y proteger a los usuarios.

Agradecemos la atención prestada y quedamos atentos

Cordialmente,

FINAGRO
Santiago Espinosa Romero
despinosa@finagro.com.co
Director
Dirección Juridica
Teléfono en Bogotá +57 601 3203377 - Ext: 292
Carrera 13 No 28-17 Bogotá, Colombia, Suramérica