



DENUNCIA DE CODIGOS CORTOS

Asunto: Uso indebido códigos cortos asignados a HÁBLAME. Detección ataque phishing vía SMS.

1. ANTECEDENTES:

En los meses de abril, mayo de 2025, Colombia Móvil S.A. E.S.P. recibió reportes de usuarios de telefonía móvil, suscriptores de nuestra red PCS, en el cual denuncia un ataque de phishing vía SMS, a través del código corto listado a continuación:

PCA Y/O INTEGRADOR TECNOLÓGICO	CÓDIGO CORTO	Número Contrato de Acceso	Fecha de suscripción del contrato	Asignatario del código corto	Resolución CRC	Cuenta SMPP
HABLAME	85617	CMOV-161	24/03/2017	A2P COLOMBIA S.A.S.	Asignación 5347 de 2017 Recuperación 7718 de 2025	PCA_HABLM_B
HABLAME	85999	CMOV-161	24/03/2017	PACIFIC TELECOM GROUP S.A.	7144 de 2017	PCA_HABLM_B
HABLAME	890133	CMOV-161	24/03/2017	HABLAME COLOMBIA SA ESP	5127 de 2017	PCA_HABLM_B
HABLAME	899773	CMOV-161	24/03/2017	A2P COLOMBIA S.A.S.	5347 de 2017	PCA_HABLM_B
HABLAME	85882	CMOV-161	24/03/2017	AIRTIME TECHNOLOGIES CHILE SPA	7235 de 2023	PCA_HABLM_B
HABLAME	890176	CMOV-161	24/03/2017	A2P COLOMBIA S.A.S.	5298 de 2018	PCA_HABLM_B

A continuación, se presenta la explicación de los campos del cuadro:

Proveedor de Contenidos y Aplicaciones - PCA: El agente responsable directo por la producción, generación y/o consolidación de contenidos y aplicaciones a través de redes de telecomunicaciones. Resolución CRC 5050 de 2016.

Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505



Integrador Tecnológico: Una empresa o profesional que actúa como intermediario técnico y/o comercial entre los Proveedores de Contenidos y Aplicaciones (PCA) y los Proveedores de Redes y Servicios de Telecomunicaciones (PRST o "operadores"). Su función principal es facilitar la conexión tecnológica, la gestión de la mensajería (SMS/USSD).



Código corto: Es el tipo de numeración asignada por la CRC para la prestación de servicios de contenidos y aplicaciones basados en el envío o recepción de mensajes cortos de texto (SMS) y/o mensajes a través del Servicio Suplementario de Datos No Estructurados (USSD). Resolución CRC 5050 de 2016.

Asignatario de código corto: La persona o entidad (PCA, Integrador Tecnológico o incluso un Proveedor de Redes y Servicios de Telecomunicaciones - PRST en su condición de PCA) a la que la CRC le ha otorgado el derecho de uso de uno o varios códigos cortos para la provisión de contenidos y aplicaciones a través de SMS y/o USSD. Resolución CRC 5050 de 2016.

Resolución CRC: Un acto administrativo formal expedido por la Comisión de Regulación de Comunicaciones (CRC) que otorga o revoca el derecho de uso de uno o varios códigos cortos a una persona natural o jurídica. Cuando la CRC emite una resolución de asignación, significa que un código corto específico (por ejemplo, 85858) es formalmente asignado a un **Proveedor de Contenidos y Aplicaciones (PCA)**. Esta resolución detalla las condiciones de uso, los servicios para los cuales se puede utilizar el código y las obligaciones del asignatario. Por el contrario, una resolución de retiro significa que la CRC formalmente recupera el derecho de uso de un código corto previamente asignado. Esto suele ocurrir si el asignatario incumple los términos de la asignación, si el código no se utiliza para el fin previsto dentro de un plazo determinado.

Cuenta SMPP: Es un conjunto de credenciales y configuraciones que permiten a una aplicación o sistema (conocido como External Short Messaging Entity o ESME) conectarse a un Short Message Service Center (SMSC) o a una plataforma de gateway SMS (como la que podría operar un Integrador Tecnológico) para enviar y recibir mensajes de texto (SMS).

2. REPORTE

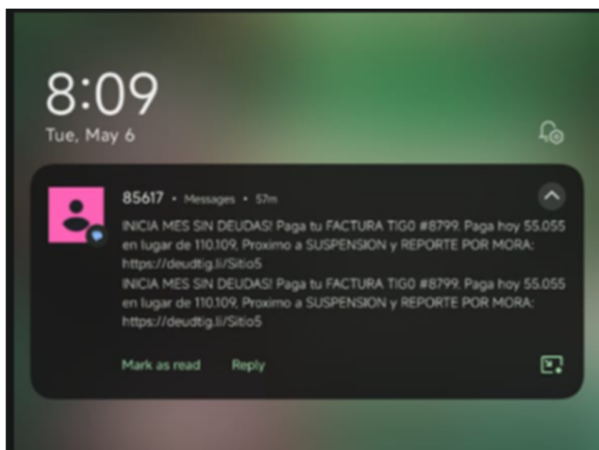
Presentamos a continuación la captura de pantalla del mensaje recibido en el equipo móvil del suscriptor y algunos ejemplos de los SMS recibidos por los usuarios:

CÓDIGOS CORTOS HABLAME

Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505





Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505





Se generan requerimientos internos al área de Seguridad de la información de Tigo, solicitando el bloqueo en nuestra red de los links maliciosos y para que gestione el bloqueo con el Hosting que aloja los portales falsos de pago.

Request #	Status	Open Date	Prio	Request Area	Type	Summary
12561112	En Proceso	6/05/2025 21:08	2 Baja	Seguridad.Re	Requerimiento	Análisis y bloqueo de sitios web fraudulentos.
12551850	Duplicado	30/04/2025 12:51	None	Seguridad.Md	Requerimiento	Buenas tardes. Se presenta nuevo incidente de smishing c...
12551314	Cerrado-Resu	30/04/2025 10:03	2 Baja	Seguridad.Re	Requerimiento	Análisis y bloqueo de sitios web fraudulentos.
12543162	Cerrado-Resu	24/04/2025 17:53	None	Seguridad.Re	Requerimiento	Análisis y bloqueo de sitio web fraudulento.

Listado de Portales identificados.

Se identifican en total 180 links cortos que redireccionaban a los siguientes 11 portales falsos

URL Bloqueadas:

- <https://express-tigo.portal-beneficios.com/index.php?sid=a0NHdUhCc3hteHhHOVZ6Q0MwekJXcm1aMHRWZWxYSnZqWEJ4WkU3RE0zRT0>
- <https://express-tigo.portal-beneficios.com/index.php?sid=cVvkVXZGVHE3eEdOUVBZMXg4VTdUZHIEMzd4N0pxQjIBbENVM2pGaVZkQT0=>
- <https://express-tigo.portal-beneficios.com/index.php?sid=WjZFN3RoZDZKMzJDNVI0SGtrejBRWDdrSEdja3l3Z3FhbG1UdjIUZktOND0=>
- <https://factura-tigo.com/index.php?sid=a1QrR0JLMEE3K21xNzZldUhCam5UZm42M3d4RzkzM0ZnMnB3Sk03YVVLND0>

Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

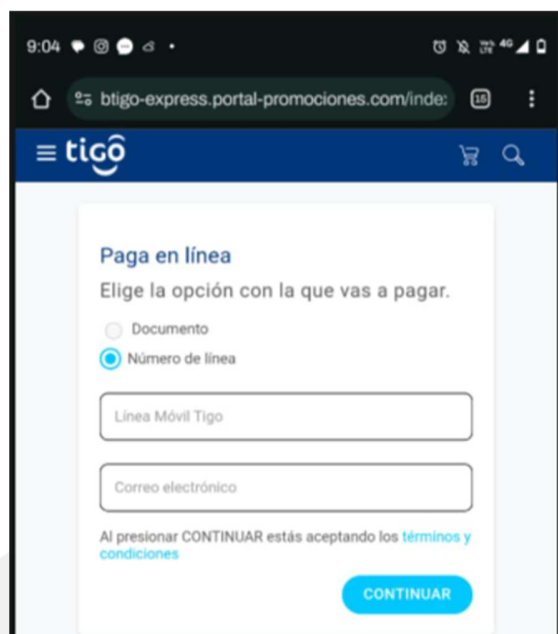
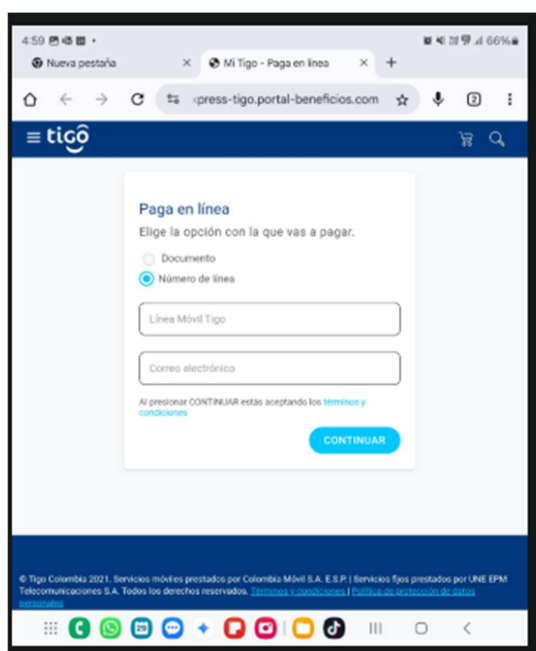
Bogotá
Conmutador (+57) 604 325 1505





- <https://pago-fact-claro.com/index.php?sid=bGRTcDhDeS9kQWxOTlhCaitxYWUrR1BVakN3SkN4T3l0NnJHNvpjOWFnWT0=>
- <https://portalpagosdescuentos.store/index.php?sid=NG54M01sQ0VlbFlqWTg0YXM4YWYvUmplVFBYs1pyRUTxc253aytZeTdFWT0=>
- <https://portal-tigo.com/index.php?sid=b1hRjQ5eDNpUnFXeTRSOWNXQ2FmeG85enJLa3pXM0pWMkhHUGJIMEY2OD0=>
- <https://portal-tigo-50off.site/index.php?sid=ekVscC9LOElxTm1Xak00S21vNTN0NDE1Q3k0WFFYTFppdnRGTIVZMXZ4Zz0=>
- <https://tigodescuentos.online/index.php?sid=dWlzZFpKbW9aL0hxUGdWY2xBRWhTcmVMektYSm9PSXF4YmxBZDFZSFRnaz0=>
- <https://tigodescuentos.online/index.php?sid=ZGh0YkVlL1JMbUJ5RlVNRWdlQ05DcFF3QkwzbTZ5QTJaeE9kL3pXK1VVT0=>

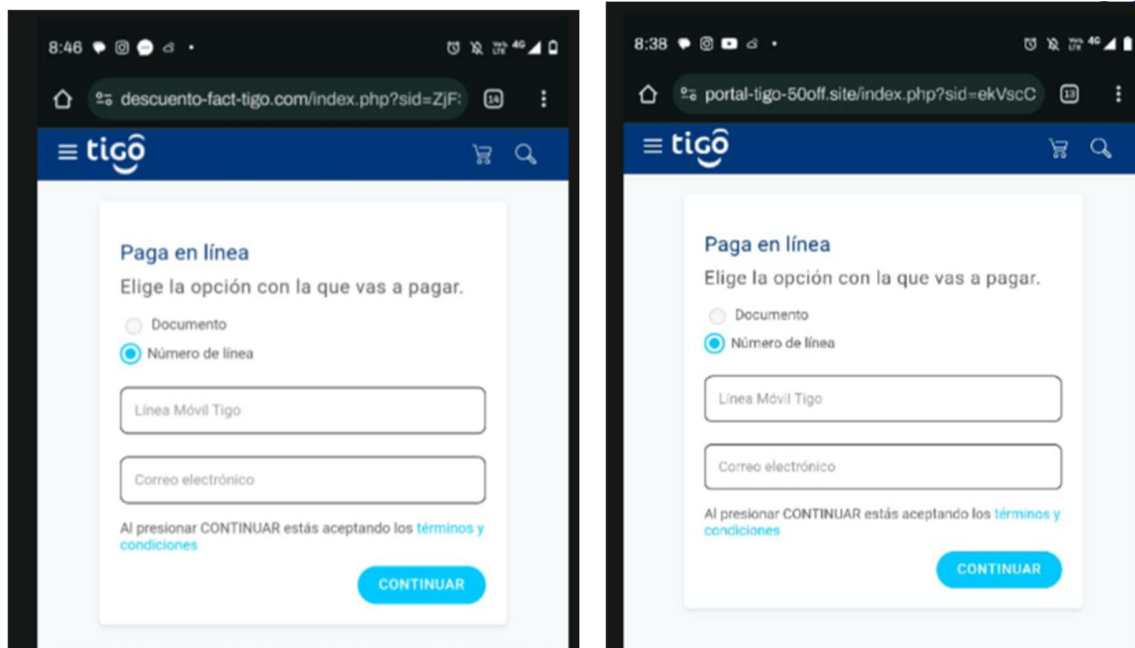
Capturas de los portales falsos.



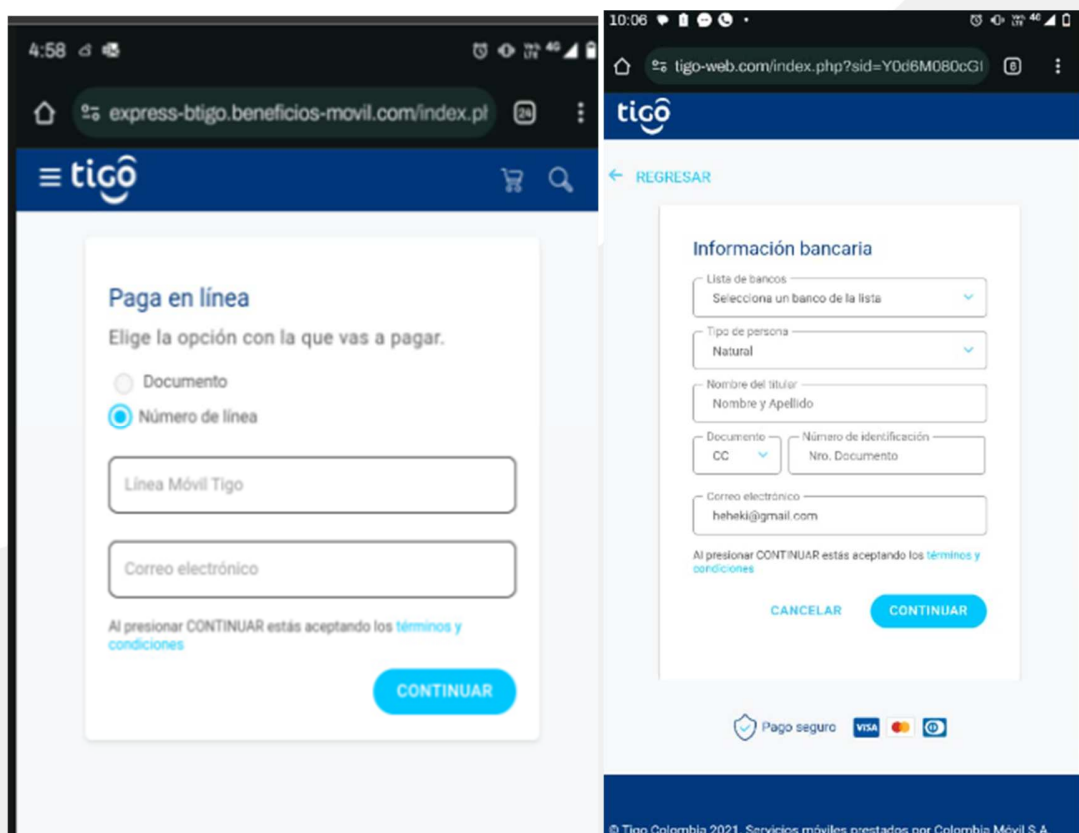
Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505





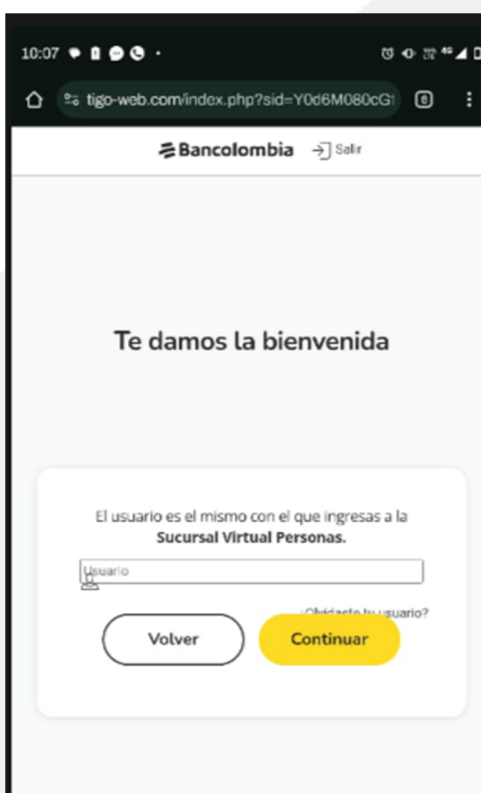
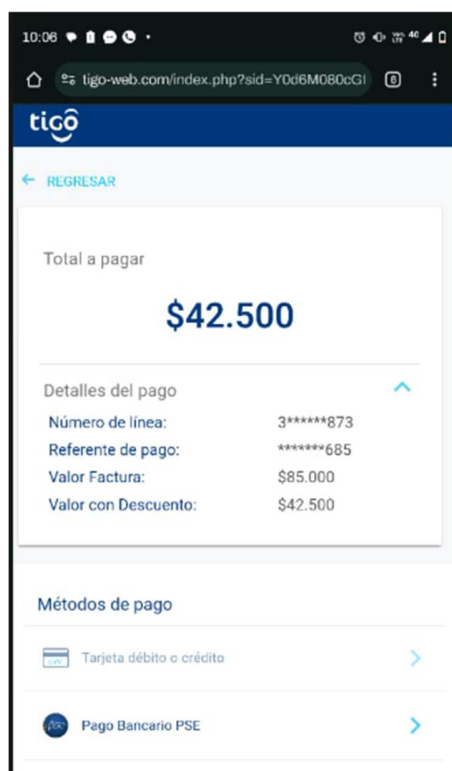
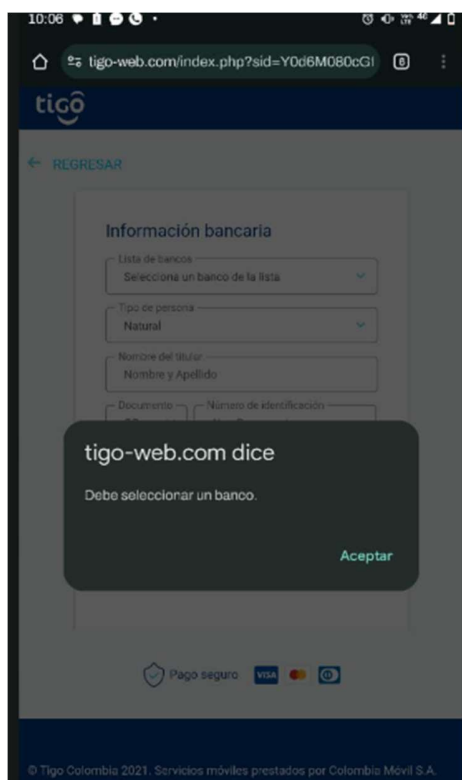
Proceso de pagos falso simulado por los links maliciosos.



Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505

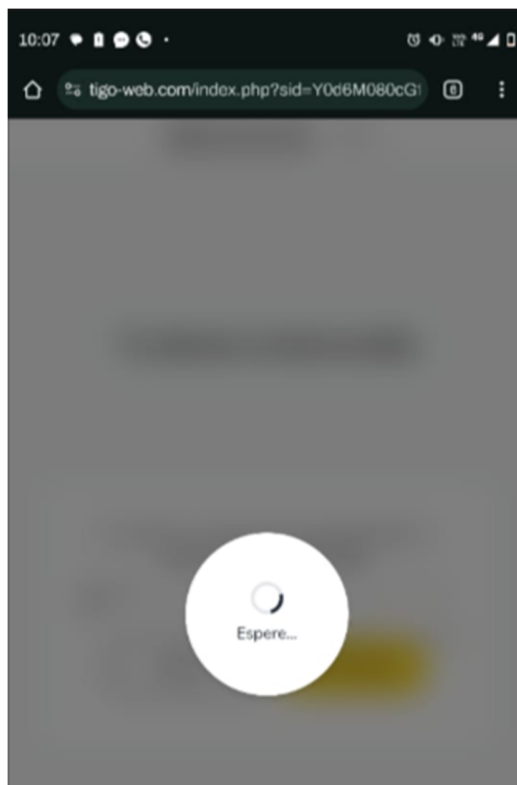
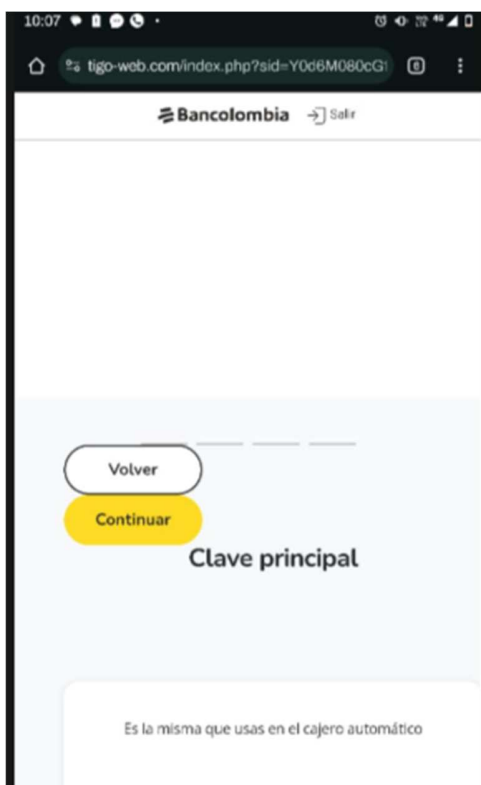




Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505





Colombia Móvil S.A. E.S.P.
Carrera 50 #96-12

Bogotá
Conmutador (+57) 604 325 1505



3. INVESTIGACIÓN

En el análisis realizado a los portales se logra evidenciar que simulan una transacción legítima de pago de factura, guiando a los usuarios por un portal de pagos (PSE) falso, el cual pedía la autenticación con sus credenciales bancarias y una vez obtenida la información emitía un mensaje de ***“Error en la transacción, inténtalo más tarde”***. La información captada era almacenada para posteriormente saquear las cuentas bancarias.

Mediante PQRS algunos de nuestros clientes indicaron ser víctimas de robo en sus cuentas (105 PQRS).

En el análisis de los SMS bloqueados se identifica que poseían información privilegiada del cliente: Nombre del titular, número de la línea, plan de facturación, valor de la factura y fecha límite de pago, facilitando la confusión en el usuario y permitiendo ser víctima de esta estafa.

Dentro del marco investigativo que se adelanta al interior de la compañía se busca siempre proteger al cliente utilizando mecanismos y plataformas de control de fraude con el fin de mitigar el impacto que pueda tener la llegada de estas comunicaciones, empleando toda la experiencia del mercado y frenando desde nuestro alcance la proliferación de los fraudes de Smishing, Vishing y Phishing.

Con las herramientas antifraudes utilizadas en TIGO se generaron acciones de identificación y bloqueo de los SMS que cumplieran con los patrones de fraude configurados.

Fruto de esto se detectaron 86492 SMS fraudulentos suplantando la gestión de cobro de TIGO y 25589 SMS fraudulentos soplando otras entidades (Bancolombia, banco de Bogotá, Claro, Latam).

4. AFECTACIÓN

Se generó afectación al buen nombre de la empresa TIGO por robo de la información comercial de nuestros usuarios, insatisfacción en los clientes que fueron víctimas de robo en sus cuentas bancarias, costos adicionales por campañas preventivas de comunicación al cliente para contrarrestar la desinformación generada por el fraude y costos operacionales en la detección y control del incidente.

5. CONCLUSIONES

Después de adelantar la investigación correspondiente a esta modalidad de fraude, la compañía dispuso de mecanismos de control de Smishing para frenar en lo posible la proliferación del envío masivo de SMS con el ánimo de unirse a la lucha contra este flagelo que afecta a los usuarios. De esta manera y en línea con lo anterior se pone en conocimiento a las autoridades competentes como mecanismo de control y transparencia de los casos de fraude reportados o conocidos por la compañía.

6. OBLIGACIONES del PCA

El contrato de acceso indica las siguientes obligaciones del PCA:

El PCA y/o Integrador Tecnológico se obliga a:

(...)

(ix) Responsabilizarse por la información transportada a través de los SMS que originen con ocasión del presente contrato y que sean enviados (o vayan a ser enviados) a los Usuarios.

(xvi) Mantener control sobre la información transportada en los SMS enviados y responder por las infracciones a la ley derivadas de la falta de control."

"ARTÍCULO 2.1.19.9. IDENTIFICACIÓN DEL PCA. En el envío de mensajes a través de SMS o USSD, con fines comerciales o publicitarios, se deberá informar a los usuarios el nombre, la marca o la razón social del PCA responsable de la provisión de contenidos y aplicaciones. El cumplimiento de esta obligación deberá hacerse al principio o al final de cada sesión, mensaje o un grupo de mensajes concatenados según lo que aplique."

"ARTÍCULO 2.1.18.4. PREVENCIÓN DE FRAUDES DE LOS PCA E INTEGRADORES TECNOLÓGICOS ASIGNATARIOS DE CÓDIGOS CORTOS. Los PCA e integradores tecnológicos que sean asignatarios de códigos cortos deberán hacer uso de herramientas tecnológicas para prevenir fraudes a través del envío de mensajes SMS o USSD y efectuar controles periódicos respecto de la efectividad de los mecanismos dispuestos para tal fin."

La regulación vigente que aplica a los PCA está contenida en las Resoluciones CRC 3501 de 2011, 5050 de 2016, 5111 de 2017 y 6522 de 2022.



Especialista Riesgos
Dirección Control de Negocio y seguramiento de Ingresos
John.restrepo@tigo.com.co
Teléfono: Celular: (57)3128874769
Dirección: Cra. 48 #20-45, Edificio Rivana
Medellin - Colombia