

Respetado Doctor
Cesar Ovidio Tellez García
Fiscal 425 Local
Unidad de Investigación Judicial y Protección de la Información y de los Datos
Bogotá D.C.

Asunto: Segunda Ampliación de Denuncia

Referencia: 110016000050202492413

Punible: Suplantación de sitios web para capturar datos personales (Art. 269G C.P.) y demás que se lleguen a establecer

Víctima: COLOMBIA MÓVIL S.A. E.S.P.

Respetados Señores,

FELIPE JIMÉNEZ GUACANEME, identificado como aparece al pie de mi firma, obrando como Apoderado Suplente para Asuntos Penales de **COLOMBIA MÓVIL S.A. E.S.P.**, respetuosamente me dirijo ante ustedes con el fin de **AMPLIAR LA DENUNCIA**, de conformidad con el artículo 69º del Código de Procedimiento Penal.

Lo anterior, con base tanto en los derechos como en los deberes que por medio de la Constitución Política de Colombia¹, la Ley 906 de 2004 y demás disposiciones legales le son reconocidos a mi prohijada.

I. ANTECEDENTES

- i. **COLOMBIA MÓVIL S.A. E.S.P.**, es una empresa cuyo objeto social es la prestación de servicios de telecomunicaciones, tecnologías de la información y las comunicaciones, servicios de información y actividades complementarias relacionadas y/o conexas con ellos. Tiene como nombre comercial **TIGO**.

¹ Cabe destacar artículos como el 95º, que en su numeral séptimo impone el deber de “Colaborar para el buen funcionamiento de la administración de la justicia”; disposición que se complementa con el artículo 229º que reconoce el derecho de cada ciudadano a acceder a la administración de justicia.

- ii. Para el desarrollo de su actividad, **COLOMBIA MÓVIL S.A. E.S.P.** cuenta con una amplia red distribuida a lo largo del territorio nacional, así como diferentes puntos de atención destinados a prestar servicios de tecnología y telecomunicaciones a sus usuarios.
- iii. El artículo 4.2. de la Resolución No. 3501 de 2011 de la Comisión de Regulación de Comunicaciones, establece lo siguiente con relación a las obligaciones de los proveedores de redes y servicios de telecomunicaciones móviles respecto del acceso a sus redes para la provisión de contenidos y aplicaciones a través de SMS/MMS:

“[...] 4.2. Permitir el acceso a sus redes por parte de los PCA e integradores tecnológicos siempre que sea técnica y económicamente viable y en ningún caso podrán cobrar a dichos agentes por considerar o tramitar su solicitud de acceso. De acuerdo con lo anterior, los PSRT sólo podrán oponerse al acceso solicitado cuando demuestren fundada y razonablemente que el mismo causa daños a la red, a sus operaciones o perjudica los servicios que dichos proveedores deben prestar. En su argumentación, el PSRT deberá presentar las propuestas para evitar los daños alegados y los responsables sugeridos para adelantar las acciones. (Subrayado, negrillas y cursivas fuera del texto).

De acuerdo con lo anterior, **COLOMBIA MÓVIL S.A. E.S.P.** en calidad de Proveedor de Redes y Servicios de Telecomunicaciones (en adelante PRST), se encuentra obligado a permitir el acceso a sus redes a otros sujetos a fin de que éstos brinden servicios de telecomunicaciones, quienes adquieren la calidad de Proveedores de Contenidos y Aplicaciones (en adelante PCA).

- iv. Por otro lado, el artículo 2.1.18.4 de la Resolución 5050 de 2016 de la Comisión de Regulación de Comunicaciones, dispone que los PCA deberán poner en práctica los medios idóneos para la prevención de fraudes por medio de SMS/MMS. De manera concreta indica:

“ARTÍCULO 2.1.18.4. . 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.**” (Subrayado, negrillas y cursivas fuera del texto).

- v. Atento a la normativa antes indicada, la relación entre mi poderdante y los PCA se encuentra regulada por contratos de acceso o de prestación de servicios de red a fin de que los PCA envíen SMS -a través de código cortos- de sus diferentes clientes. De tal suerte, también es necesario recalcar que los PCA cuentan con la obligación de velar por el adecuado uso de los servicios de telecomunicaciones prestados mediante el uso de las redes de telecomunicaciones de **COLOMBIA MÓVIL S.A. E.S.P.**

- vi. **COLOMBIA MÓVIL S.A. E.S.P.** ha suscrito diversos contratos con **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.** para que fungiera como PCA de Códigos Cortos, entre estos se destaca lo siguiente:

PCA	CÓDIGO CORTO	Número Contrato de Acceso	Fecha de suscripción del contrato	Resolución CRC	Cuenta SMPP
HABLAME	85301	CMOV-161	24/03/2017	5298 de 2018	PCA_HABLM_B

- vii. Es menester resaltar que dentro de dichos contratos de acceso consta la siguiente cláusula:

“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” (Subrayado, negrillas y cursivas fuera del texto).

- viii. Al respecto, y en virtud de la administración que la empresa **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.** realiza sobre una diversidad de códigos cortos, se han presentado múltiples incidentes de fraudes **sistemáticos y generalizados** en detrimento de **COLOMBIA MÓVIL S.A. E.S.P.** y sus clientes.
- ix. De hecho, el suscrito formuló una denuncia que fue asignada ante su Honorable Despacho en donde se daba cuenta de cómo terceros indeterminados estarían utilizando los códigos cortos asignados a **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.** para suplantar sitios web para capturar datos personales (Art. 269G C.P.).
- x. Incluso, el pasado **15 de octubre de 2024**, se radicó una ampliación de denuncia por conducto de la cual se allegabas información a su Honorable Despacho sobre otros **cinco (05) hechos punibles** que habrían sido propiciados con el uso de códigos cortos administrados y gestionados por **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.**
- xi. Ahora bien, este fenómeno delictivo sigue en crecimiento, y se han presentado más eventos con la instrumentalización de códigos cortos asignados a **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.**, los cuales se expondrán a continuación:

- I. El **28-08-2024** un usuario recibió un mensaje presuntamente fraudulento enviado desde el código corto 85301, a través del cual se envió el siguiente mensaje: **“APRECIADO CONTRIBUIDOR: El plazo para saldar tu mora fiscal vence el 30/08/24, se procederá al congelamiento de sus activos. Mas informacion: u.to/dyXYIA”**. (Subrayado, negrillas y cursivas fuera del texto). Tal y como podrá evidenciarse con la imagen aportada por el usuario que presentó la mencionada alerta, y que se encuentra en el informe “*Uso indebido códigos cortos asignados a HABLAME. Detección ataque phishing vía SMS*” suscrito por Especialistas de Riesgos de la Dirección Control de Negocio y Aseguramiento de Ingresos de **COLOMBIA MÓVIL S.A. E.S.P.**

De acuerdo con las validaciones realizadas por los servidores en materia de seguridad informática de **COLOMBIA MÓVIL S.A. E.S.P.:**

“El mensaje incluye un link que lleva a una página supuestamente de la DIAN, el otro enlace acertado ya no se encuentra disponible. Las campañas de smishing lideradas por ciberdelincuentes experimentados, suelen usar servicios de almacenamiento en la nube para ocultar malware o engañar a las víctimas para que revelen información personal.

Hay que notar que los enlaces mostrados en los mensajes parecen ser links acertados; en el caso del que aún está disponible hxxps://u[.]to/dyXYIA, al visitarlo redireccionan hacia el sitio hxxps://dianimpuestosonline[.]com/pagorapido; Al validar el dominio dianimpuestosonline[.]com se evidencia que tu registrad hace/dias, algo común en las campañas maliciosas. Cabe resaltar que es un dominio completamente diferente a la página real de la DIAN. lo cual aumenta la sospecha.

Aparte de lo anterior, al validar la url hxxps://u[.]to/y2LWIA, no se encontraba disponible sin embargo se identifica que resuelve la dirección IP 195.216.243[.]J155 y se encuentra ubicada en Rusia. Además, al validar dicha IP en herramientas de seguridad se encuentra que 2 de 94 proveedores de seguridad la consideran como maliciosa. Cabe anotar que el servicio de u.to que ofrece acortar url's es conocido por ser usado por ciberdelincuentes para abreviar sus enlaces. además de estar relacionado con otras campañas de smishing anteriores” (Subrayado, negrillas y cursivas fuera del texto).

- xii. Tomando en cuenta lo anterior, de conformidad con las labores investigativas adelantadas por funcionarios de mi poderdante, se determinó que los códigos cortos asignados a **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.** habrían sido utilizados para un presunto fraude de modalidad

Phishing, ya que los links relacionados en los SMS podrían descargar y activar algún tipo de software malicioso que pueda infectar equipos electrónicos.

- xiii. Vale decir que esta clase de afectaciones ya ha sido expuesta por funcionarios de mi prohijada a la empresa **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.**, que estaría representada por el **Sr. DIEGO DAMIAN VALDIVIESO PINILLA**, sin que a la fecha se hayan realizado labores concretas por parte de tale sociedad para evitar y/o mitigar los incidentes que ponen en riesgo los datos personales de los usuarios de **COLOMBIA MÓVIL S.A. E.S.P. – Tigo**.
- xiv. A su turno, también se ha informado de esto a la Comisión de Regulación de Comunicaciones, para que se tomen las medidas tendientes a proteger a los usuarios del servicio público esencial de las telecomunicaciones.
- xv. Se aclara que las identidades de los sujetos responsables de los hechos aquí expuestos no son conocidas por mi cliente. Lo anterior, como consecuencia de que no se ha tenido contacto directo con los mismos, ni oportunidad de aprehenderlos o identificarlos por medio de los artefactos tecnológicos destinados para tal efecto.
- xvi. Igualmente, al suscrito le merece el deber de aclarar que, al ser un tercero contratado por **COLOMBIA MÓVIL S.A. E.S.P.** para asuntos penales, la única información que se tiene sobre los hechos acaecidos es aquella que se ha plasmado con anterioridad.

II. SUGERENCIAS INVESTIGATIVAS AL AL PROGRAMA METODOLÓGICO DE LA INVESTIGACIÓN

En aras de coadyuvar el desarrollo del Programa Metodológico de Investigación, respetuosamente solicito a la Fiscalía General de la Nación que se ordenen las siguientes actividades investigativas:

1. Se cite a diligencia de entrevista a **JAIRO FIGUEROA**, Especialista de Fraudes de la Dirección Control de Negocio y Aseguramiento de Ingresos de **COLOMBIA MÓVIL S.A. E.S.P.**, quien puede ser contactado en el correo electrónico Jairo.Figueroa@tigo.com.co, al teléfono celular (57) 3002290822 o en la Calle 127A # 53A – 45, Edificio We Work, Piso 5 de Bogotá D.C.
2. Se cite a diligencia de entrevista a **DIEGO DAMIAN VALDIVIESO PINILLA**, Gerente de **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.**, o a quien haga sus veces, quien puede ser contactado al abonado telefónico (1) 8845634 y a los correos electrónicos d.valdiviesco@hablame.co o notificacionesjudiciales@hablame.co.

3. Se requiera a **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.**, con notificaciones en notificacionesjudiciales@hablame.co, para que exponga qué labores ha adelantado para mitigar los incidentes que ponen en riesgo los datos personales de los usuarios de **COLOMBIA MÓVIL S.A. E.S.P. – Tigo**.
4. Se requiera a la Comisión de Regulación de Comunicaciones para que exponga qué labores ha adelantado para mitigar los incidentes que ponen en riesgo los datos personales de los usuarios de **COLOMBIA MÓVIL S.A. E.S.P. – Tigo**. En especial aquellos que se han configurado desde los Códigos Cortos asignados a **HÁBLAME COLOMBIA LDI S.A.S. E.S.P.**

III. ANEXOS

Para que sean tenidos en cuenta por la Fiscalía General de la Nación, se anexan al presente escrito el siguiente documento:

- A. Informe “*Uso indebido códigos cortos asignados a HÁBLAME. Detección ataque phishing vía SMS*” suscrito por **JAIRO FIGUEROA**, Especialista de Fraudes de la Dirección Control de Negocio y Aseguramiento de Ingresos de **COLOMBIA MÓVIL S.A. E.S.P.**

IV. NOTIFICACIONES

Para tales efectos, el suscrito podrá ser notificado en el correo electrónico felipe@casasyescobar.com y/o al teléfono celular 3046419036.

Cabe resaltar que el suscrito únicamente representará a COLOMBIA MÓVIL S.A. E.S.P. dentro para la interposición de la denuncia, para notificaciones en sede de conocimiento, por favor dirigirse al correo notificacionesjudiciales@tigo.com.co.

No siendo más el objeto del presente, agradezco su amable atención.

Cordialmente,



FELIPE JIMÉNEZ GUACANEME

C.C. No. 1.015.406.601 de Bogotá D.C.

T.P. No. 360.225 del C. S. de la J.



DENUNCIA DE CODIGOS CORTOS

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

1. ANTECEDENTES:

En el mes de agosto de 2024, 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	CÓDIGO CORTO	Número Contrato de Acceso	Fecha de suscripción del contrato	Resolución CRC	Cuenta SMPP
HABLAME	85301	CMOV-161	24/03/2017	5298 de 2018	PCA_HABLM_B

Se detalla la información del PCA asignatario del código corto, número de contrato de acceso, fecha de suscripción del contrato, número de resolución de la CRC y la cuenta SMPP a la cual está asociado el código.

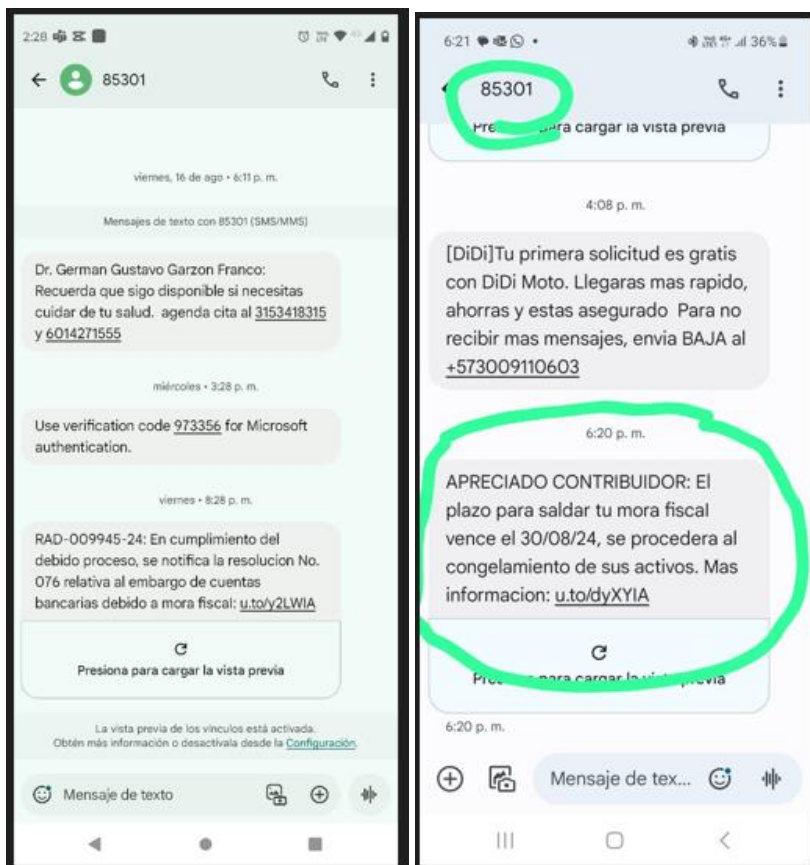
2. REPORTE

Presentamos a continuación la captura de pantalla del mensaje recibido en el equipo móvil del suscriptor:

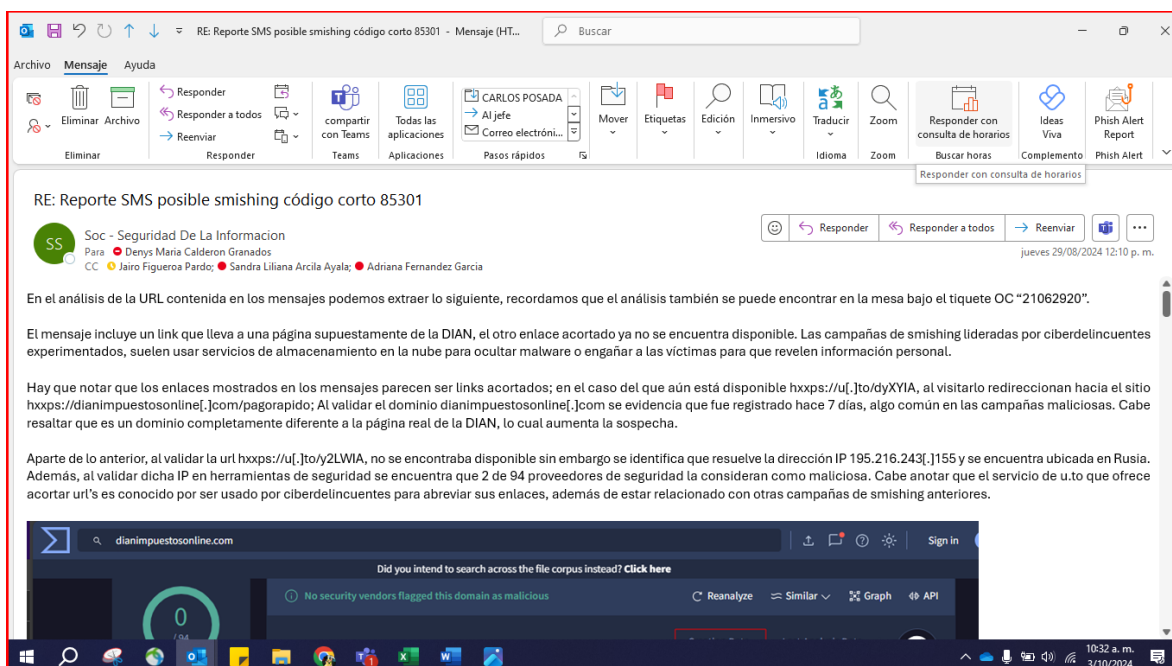


CÓDIGOS CORTOS HABLAME

28-08-2024



Anexo. Análisis de Smishing código 85301



3. INVESTIGACIÓN

No se acceden a los links dado que podría en determinado momento descargar y activar algún tipo de software malicioso que pueda infectar equipos electrónicos como tablets, smartphones o computadores. Uno de los factores predominantes a la hora de identificar este tipo de actuar de los ciberdelincuentes es la redacción en la escritura de los mensajes y la ortografía usada que en la mayoría de los casos que es precaria.

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.

4. AFECTACIÓN

No es posible cuantificar las pérdidas económicas, de datos personales, financieros o cualquier otro aspecto en este tipo de actuar fraudulento entendiendo que no hay una estadística o reporte de casos de los clientes o cantidad de mensajes detectados con este tipo de contenido

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

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.”

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.

7. FIRMANTE



Jairo Figueroa Pardo

Especialista Riesgos

Dirección Control de Negocio y seguramiento de Ingresos

Jairo.Figueroa@tigo.com.co

Teléfono: Celular: (57)300 229 0822

Dirección: Calle 127A # 53A – 45

Edificio We Work • Piso 5

Bogotá - Colombia