CRC
COMISIÓN DE REGULACIÓN DE COMUNICACIONES

16º CAMP

Aso Ban Caria

Identificación de medidas para mitigar el fraude a través de servicios móviles

CLAUDIA XIMENA BUSTAMANTE O.
Comisionada – Directora Ejecutiva (E)
Comisión de Regulación de Comunicaciones

USD $23B

pérdidas globales estimadas por fraude digital

Crowdstrike 2026
Global Threat Report

Fraude como industria global

El panorama actual muestra una evolución hacia ataques combinados que mezclan ingeniería social, robo de credenciales y herramientas basadas en inteligencia artificial.

Modalidades de fraude cibernético

Phishing

Apropiación de información confidencial de los usuarios sin autorización.

Smishing

Phishing por medio de SMS

Vishing

Phishing por medio de llamadas de voz

Spoofing

Suplantación de identidad del remitente del mensaje de correo electrónico, IP o cualquier otra app.

Fraude cibernético por SMS o llamadas de voz

SMS con enlaces falsos

SMS con malware

Llamadas extorsivas desde centros penitenciarios

Enmascaramiento del CLI.

16º CAMP

Cifras globales del fraude

27 segundos
Ataque más rápido registrado

34% ataques
originados en redes sociales

82% ataques
ya no usan malware

+400%
Crecimiento del Vishing

Crowdstrike 2026 Global Threat Report

16º CAMP

Cifras Colombia

11%
CAGR
Delitos informáticos 2020-2024

99M
Intentos de phishing
Kaspersky Panorama de Amenazas Latam

49.5%
denuncias
Hurto por medios infromáticos

20.8%
>Crecimiento Denuncia Acceso abusivo a stm informático

Observatorio DDHH y Defensa Nacional - MinDefensa

16º CAMP

Problemática

El phishing es el principal punto de entrada al fraude financiero en la región.

Rápida evolución de vectores de ataque

El teléfono móvil es la principal puerta de entrada al fraude digital.

16º CAMP

Marco de acción TIC

- Ley 1341/09 TIC
- Ley 2300/ 23 RNE
- Resolución CRC 5050/16
- Estrategia Nal. Seguridad Digital
- CONPES SD -Institucionalidad

- Gestión de riesgos de seguridad digital
- Enfoque de prevención y pedagogía
- Gestión de recurso de indentificación y actualización regulatoria

ASÍ SE PROTEGEN LAS COMUNICACIONES MÓVILES EN COLOMBIA:

Marco Normativo Vigente

Estas son las normas y las entidades que trabajan juntas para fortalecer la seguridad, prevenir fraudes y garantizar la correcta identificación de los usuarios en los servicios móviles.

CRC
COMISIÓN DE REGULACIÓN DE COMUNICACIONES

www.crcom.gov.co

1. Resolución DIJIN 912 de 2008

- Registro de usuarios.
- Operadores registran datos completos de usuarios.

2. Artículo 95 del Código Nacional de Seguridad y Convivencia Ciudadana

- Activación de líneas sin información de los usuarios afecta la seguridad.

3. Ley 1266 de 2008

- Verificación de identidad del titular.
- Lucha contra la suplantación.

4. Decreto 4768 de 2011 (MinJusticia y MinTIC)

- Autoriza al INPEC a bloquear o inhibir la señal en cárceles.
- MinTIC puede ordenar a los PRST restricciones de dicha señal.

5. Resolución CRC 5050 de 2016

art 2.1.10.7

- **Operadores:** implementación de herramientas contra el fraude.
- **Usuarios:** entregan datos veraces.

6. Resolución CRC 5050 de 2016

art 2.7.1.1

- Obliga a identificar y bloquear equipos hurtados, extraviados o con IMEI adulterado.
- Reduce el mercado ilegal de celulares.
- Uso de bases de datos positivas y negativas con el listado de los IMEI que se encuentran habilitados.

7. Decreto 857 de 2024

- Acción interinstitucional en cárceles.
- Control operativo del crimen organizado.

8. Resolución CRC 5050 de 2016

art 2.1.3.3.

- Actualiza y refuerza la verificación de identidad en líneas móviles, especialmente prepago.
- Prohíbe registrar SIM a comercializadores.
- **Exige:** verificación en tiempo real de documentos.
- Cierra vacíos de identificación y mejora la seguridad.

16º CAMP

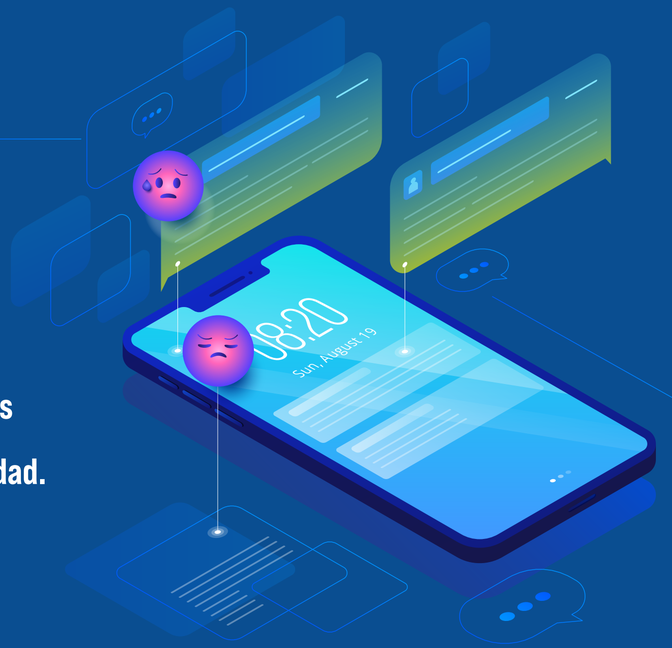
ASÍ FUNCIONA

REGISTRO DE NÚMEROS EXCLUIDOS

- La CRC lo administra
- La SIC vigila y sanciona
- Las empresas deben cumplir

1.

Te registras.
Ingresas tus datos y los canales por los que no quieres recibir publicidad.



2.

Tu información se guarda en una base nacional.
No se comparte con empresas: solo saben si pueden o no contactarte.

3.

Las empresas consultan.
Antes de enviar mensajes o hacer llamadas, deben verificar si estás inscrito.

4.

Si lo hacen igual...
Están incumpliendo la Ley 2300 de 2023 y pueden ser sancionadas por la SIC.

Inscrito en el RNE
NO deben llamarte

No inscrito
pueden contactarte

Si no respetan tu decisión, repórtalo Ante la SIC
Ley 2300 de 2023

Prevención Spam telefónico y Mensajes No Deseados

EJE 1

SMS

EJE 2

Mitigación de fraude de Voz

EJE 3

Acciones Educativas

EJE 4

Simplificación

Proyecto regulatorio contra el Fraude

- Prevención, Detección, respuesta y Pedagogía
- Análisis de alternativas publicadas
- Mesas de articulación intersectorial
- Propuesta normativa 2T

Participar en: www.crcom.gov.co

Prevención Spam telefónico y Mensajes No Deseados

EJE 1

SMS

Alternativas propuestas

- Registro nacional de remitentes (centralizado y DLT) con bloqueo o marcado
- Formalización y conocimiento del cliente (KYC)
- Categorización del tipo de contenido y consentimiento del cliente
- Monitoreo proactivo del tráfico
- Asignación de CC o números 940 a cada marca para identificación exclusiva
- Códigos Alfanuméricos y controles a patrones anómalos de tráfico P2P

Prevención Spam telefónico y Mensajes No Deseados

EJE 2

Mitigación de fraude de Voz

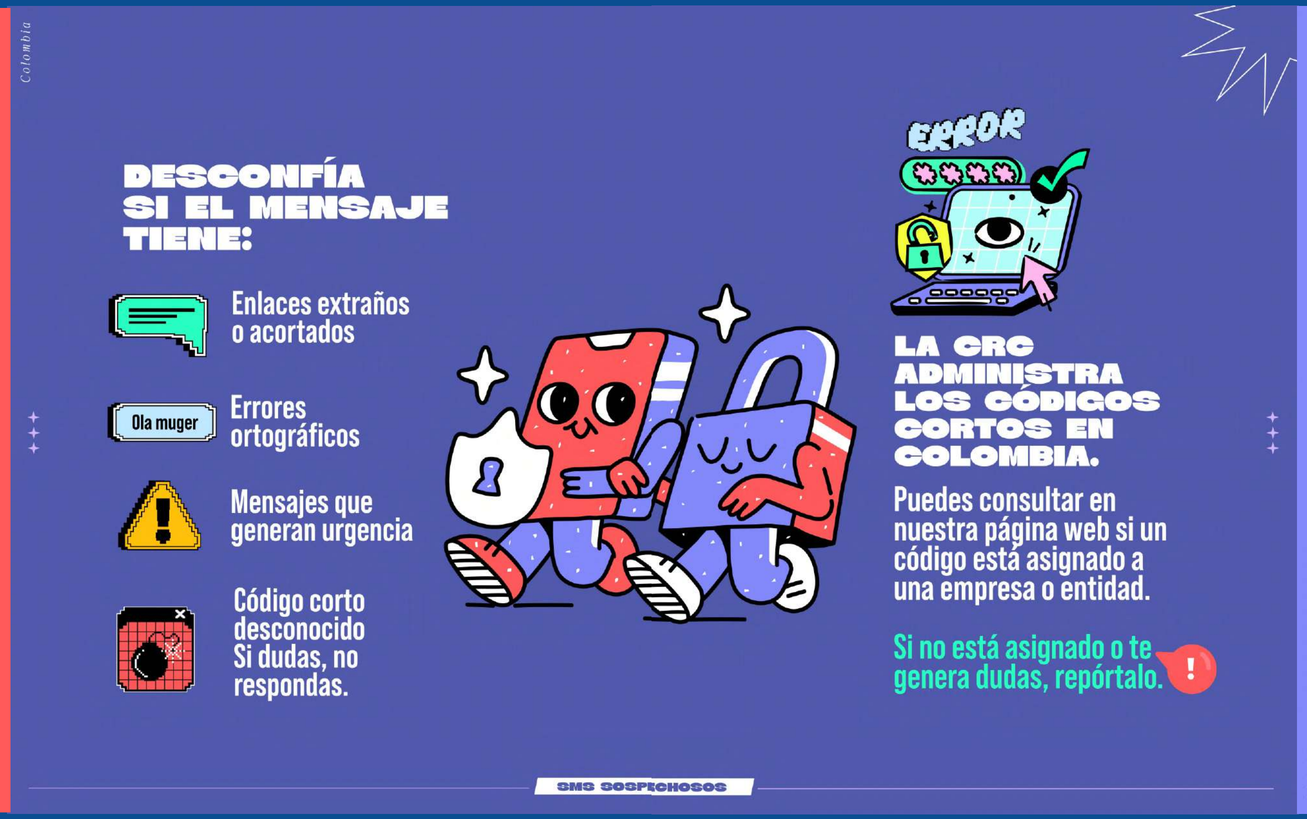
Alternativas propuestas Servicios de voz

- Bloqueo de llamadas internacionales con CLI nacional
- Listas DNO (Do Not Originate)
- Validación de origen de llamadas Stir/Shaken/RCD
- Monitoreo de tráfico coordinado

Prevención Spam telefónico y Mensajes No Deseados

16º CAMP

EJE 3
Acciones Educativas

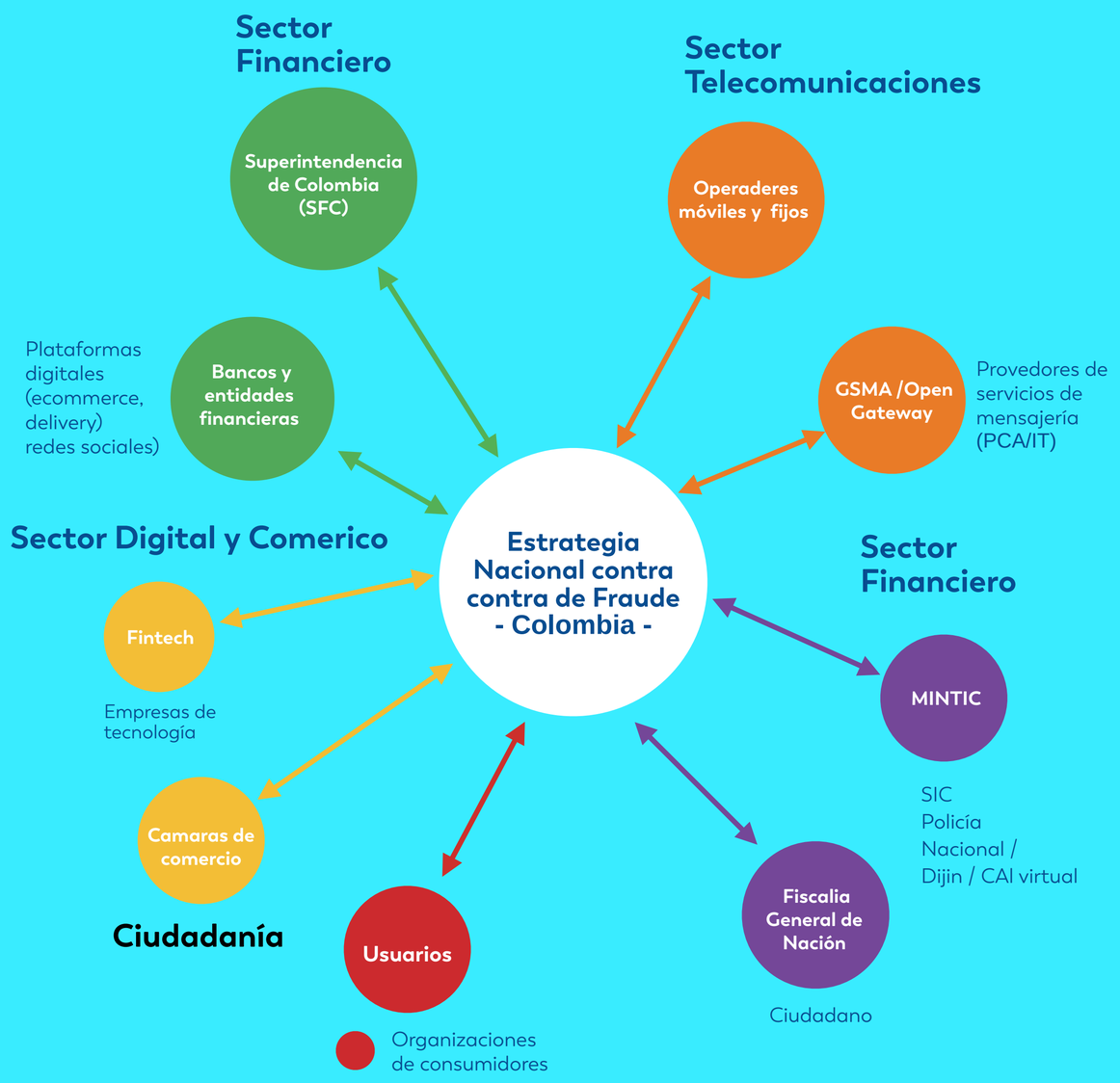


Prevención Spam telefónico y Mensajes No Deseados

EJE 4

Simplificación

- Revisión del régimen de administración de recursos de identificación bajo enfoque de simplificación



Articulación institucional es necesaria para disminuir:

- Duplicidad de esfuerzos
- Brechas de trazabilidad y atención efectiva
- Reacción tardía ante nuevas amenazas

Acciones requeridas

El sector financiero es un actor determinante en:

- Participación Mesas Técnicas intersectoriales
- Intercambio de alertas con entidades seguridad
- Proponer protocolos y uso de estándares comunes
- Inversión en sistemas de prevención y respuesta
- Pedagogía clara y permanente a usuarios

16º CAMP

Proteger al usuario es proteger la confianza

Confianza en los sistemas de pago y en canales de comunicaciones

Aso Ban Caria

16º CAMP

Gracias