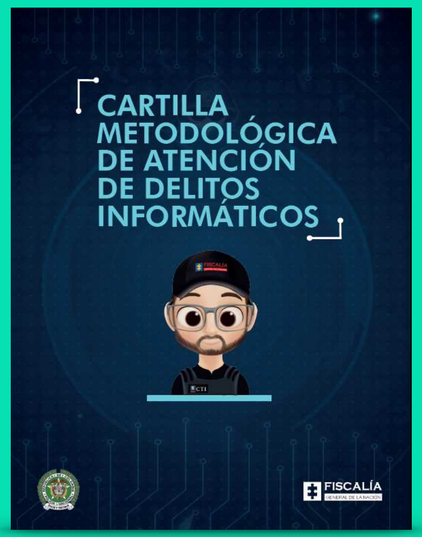
Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles

Contexto de la problemática

Mecanismos utilizados para Fraude cibernético



Modalidades de fraude

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

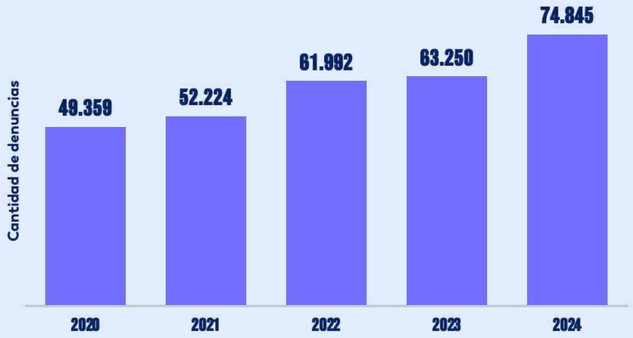
Llamadas extorsivas desde centros penitenciarios

Enmascaramiento del CLI.

Contexto de la problemática

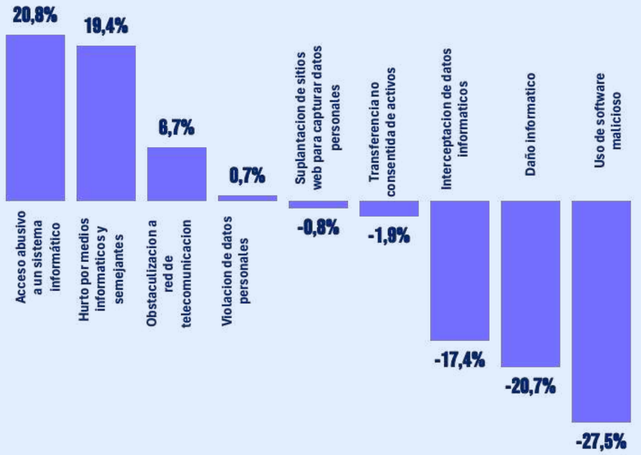
Denuncias sobre conductas asociadas a delitos informáticos

Según el Observatorio de Derechos Humanos y Defensa Nacional del MinDefensa



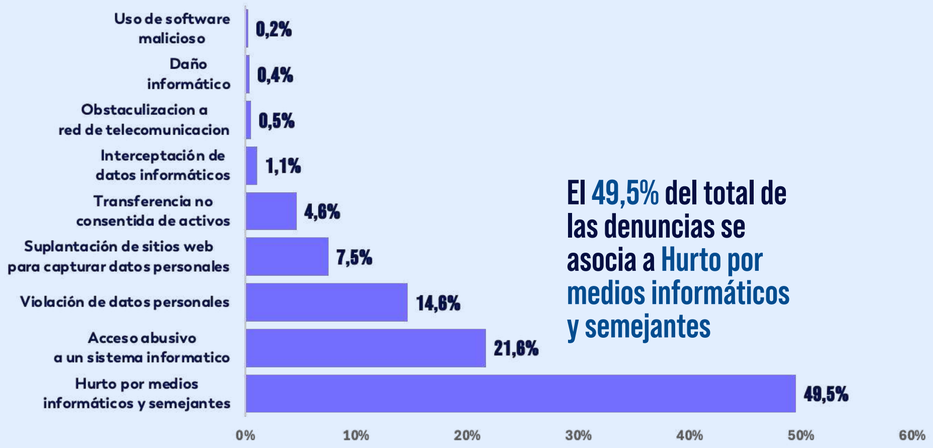
11.0% tasa de crecimiento promedio anual entre 2020 y 2024 de delitos informáticos

Tasa crecimiento anual 2020-2024



Acceso abusivo a un sistema informático crece de forma acelerada 20,8%

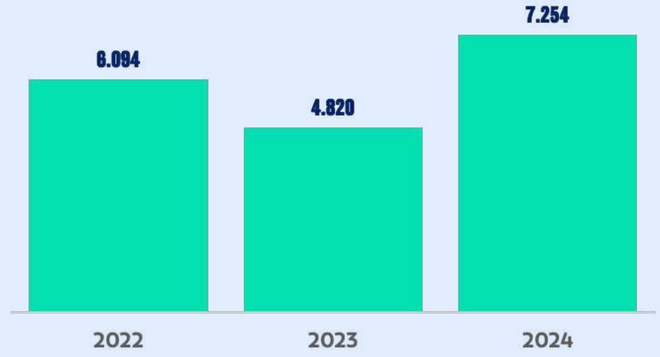
Distribución de denuncias por tipificación de la conducta en 2024



El 49,5% del total de las denuncias se asocia a Hurto por medios informáticos y semejantes

Quejas sobre posibles vulneraciones al tratamiento de datos personales

De acuerdo con la Delegatura para la Protección de Datos Personales de la SIC



Persistencia de las tácticas de ingeniería social dado el crecimiento del 19% en PQR

2025

Contexto de la problemática

Requerimiento de información CRC sobre el fraude cibernético por medio del servicio de llamadas de voz y SMS

1 de cada 3 empresas detectó incidentes de fraude cibernético en los últimos 3 años.

El **65,1% No cuenta con procedimientos** para intercambio de alertas.

Comportamiento de incidentes entre 2023 y 2024

Smishing creció un **119,3%** en llegando a **570mil incidentes detectados en 2024**

37,2% enfrenta dificultades para mantener o fortalecer sus medidas antifraude.

Vishing creció un **390,7%** en llegando a **17mil incidentes detectados en 2024**

El **principal método implementado es responder a incidentes.**

Es un **método** que se **activa** de forma **posterior a** la identificación del **incidente.**

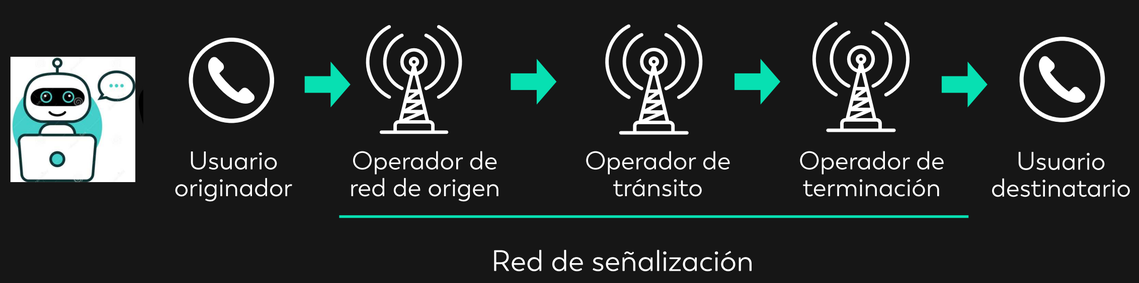
16% de las empresas cuenta **datos sobre costos**

$2.700 millones
promedio por empresa en 2024

Contexto de la problemática

Cadenas de valor desde el flujo de la comunicación

Servicio de llamadas de voz



Servicio de mensajes cortos de texto

Recursos de identificación críticos:

- **Numeración E.164**
- Identificador del abonado (caller ID)
- Puntos de señalización/red (como puntos de interconexión)

Recursos de identificación críticos:

- **Códigos cortos y numeración E.164**
- Identificadores de aplicación o remitente alfanumérico
- Numeración E.164 / número de destino
- Dirección IP (si se usa interfaz de red)

20
25

Árbol del problema

Consecuencias

- Trasgresión de los derechos de los usuarios de los servicios de telecomunicaciones
- Afectaciones a empresas y organismos públicos
- Aumento de casos de uso indebido de códigos cortos con fines fraudulentos
- Pérdida de confianza en los servicios de telecomunicaciones

Problema

Ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto

Causas

- Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso
- Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes
  - Dificultad en la identificación y rastreo de ataques cibernéticos
- Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos
- Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto

Objetivos del proyecto

Diseñar la estrategia de la CRC para la prevención del contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto

Evaluar las posibles herramientas de prevención teniendo en cuenta su viabilidad técnica y económica.

Acciones educativas que aumenten el conocimiento de los usuarios en la prevención de fraudes.

Identificar aspectos del RRI susceptibles de adecuación desde la perspectiva de prevención.

- Líneas de acción de la CRC.
- Recomendaciones a otras autoridades.
- Construcción conjunta de una estrategia nacional de prevención.

2025

Cronograma del proyecto y consulta pública

Julio 4

Publicación Documento Formulación Problema

Julio 28

FINALIZA término de la consulta pública

IVT 2025

Publicación propuesta regulatoria

IT-2026

Decisión regulatoria

Participa en la consulta pública aquí:

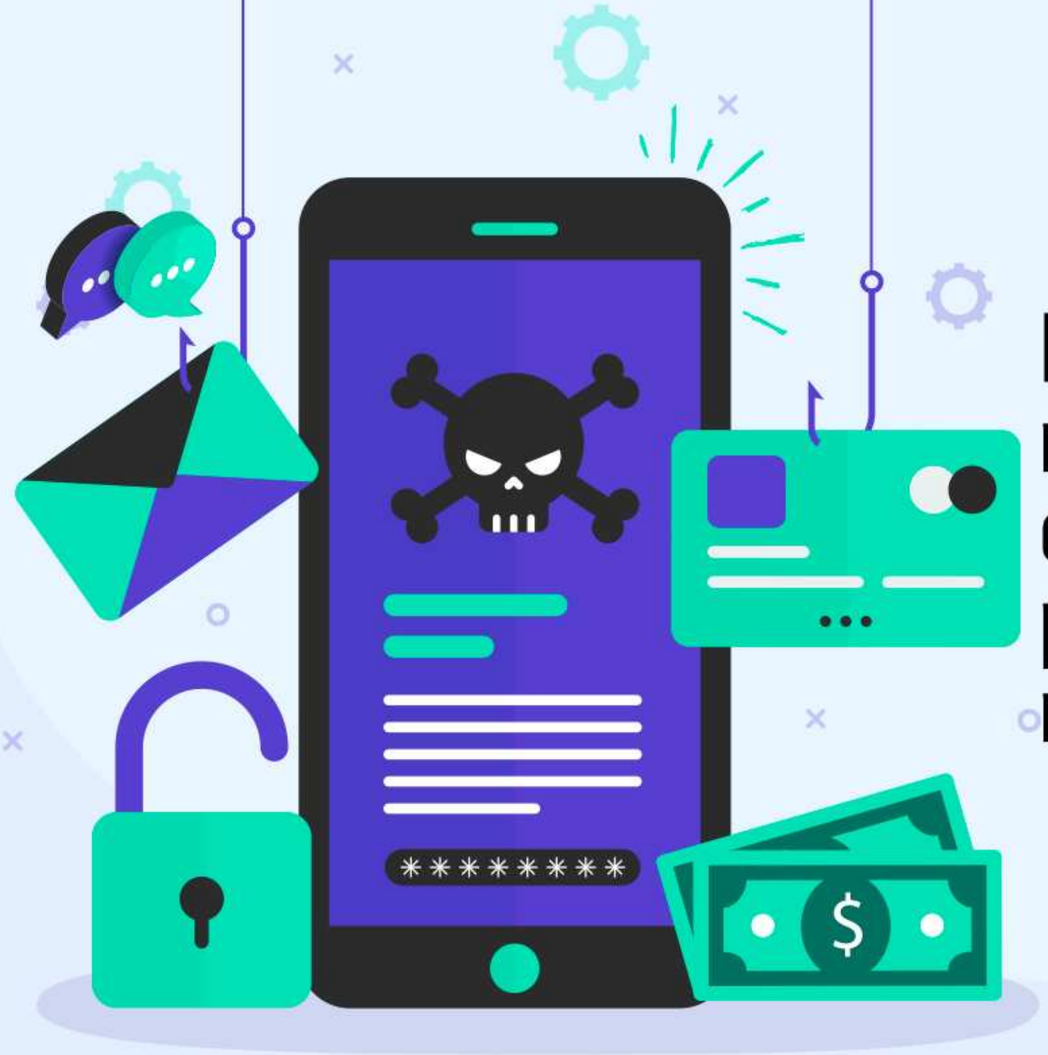
2025

¿Por qué nos encontramos aquí?

- MinJusticia
- MinDefensa
- INPEC + Gaulas
- Fiscalía
- DIJIN – Policía
- MinTIC – ColCert
- SIC
- Superfinanciera
- Entidades financieras
- PRSTM
- PCA
- IT
- CRC

Es un problema transversal que requiere:

- La materialización de una estrategia nacional efectiva.
- Disponibilidad de información oficial a nivel nacional.
- Coordinación entre entidades para prevenir y controlar.
- Articulación entre el sector público y el sector privado que generen soluciones efectivas.



Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles