DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL

BALANCE ANUAL 2024

CENTRO CIBERNÉTICO POLICIAL

A medida que el uso y la dependencia de las tecnologías de la información se vuelven más generalizadas en la sociedad, las conductas delictivas relacionadas con entornos digitales han crecido de manera exponencial, tanto en número como en sofisticación. Asimismo, la falta de concientización de los usuarios en el uso adecuado de estas tecnologías, facilita que los ciberdelincuentes exploten vulnerabilidades y materialicen conductas criminales.

En los últimos años, la Policía Nacional de Colombia, ha incrementado sus esfuerzos para combatir el cibercrimen fortaleciendo las actividades de gestión comunitaria, investigación criminal y articulación con el sector público-privado; sin embargo, se identificó un aumento del 23% de denuncias para el año 2024 por delitos informáticos, en comparación con 2023.

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL
CENTRO CIBERNÉTICO POLICIAL

BALANCE ANUAL 2024

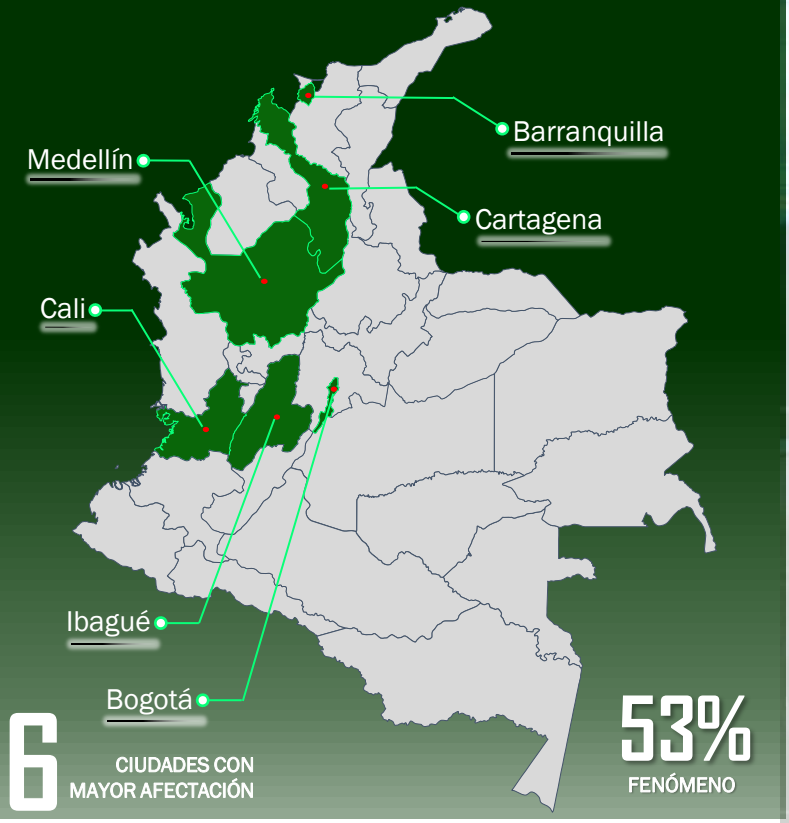
Tabla de Contenido

Pág.

BALANCE ANUAL 2024

Comportamiento del fenómeno

Las 6 ciudades que representan el **53%** del fenómeno en el país, concentraron **40.969** denuncias en el **2024**, correspondiente a un aumento del **19%** respecto del **2023** con **34.379** denuncias en las mismas ciudades.



6 CIUDADES CON MAYOR AFECTACIÓN

53% FENÓMENO

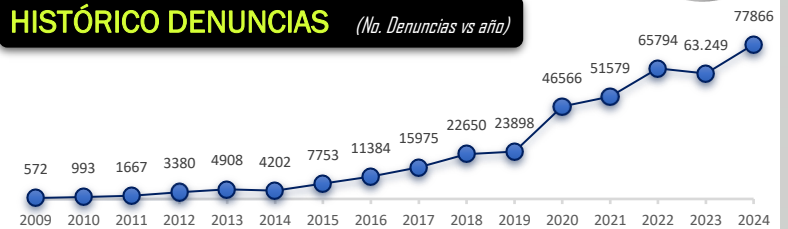
TOTAL DENUNCIAS

Ley 1273 2009

2023	2024
63.249	77.866

Incremento denuncias **23%**

HISTÓRICO DENUNCIAS *(No. Denuncias vs año)*



9 DELITOS INFORMÁTICOS

Hurto por medios informáticos y semejantes

2023	2024
31.095 DENUNCIAS	37.409 DENUNCIAS

Acceso abusivo a sistema informático

2023	2024
11.406 DENUNCIAS	16.955 DENUNCIAS

Violación de datos personales

2023	2024
10.155 DENUNCIAS	11.954 DENUNCIAS

Suplantación de sitios web

2023	2024
4.716 DENUNCIAS	6.209 DENUNCIAS

Transferencia no consentida de activos

2023	2024
3.494 DENUNCIAS	3.542 DENUNCIAS

Interceptación de datos informáticos

2023	2024
1.329 DENUNCIAS	910 DENUNCIAS

Obstaculización ilegítima de sistema informático o red de telecomunicaciones

2023	2024
319 DENUNCIAS	378 DENUNCIAS

Daño informático

2023	2024
426 DENUNCIAS	310 DENUNCIAS

Uso de software malicioso

2023	2024
309 DENUNCIAS	199 DENUNCIAS

Fuente: *Datos extraídos el día 31 de diciembre 2024.* ***Cifras sujetas a variación*** *en atención al proceso de integración y consolidación con la información de la Fiscalía General de la Nación.*

SIEDCO PLUS 2.0

BALANCE ANUAL 2024

CAI VIRTUAL

TOP 4 MODALIDADES INCIDENTES ATENDIDOS

Representación porcentual

ROBO
CUENTAS DE WHATSAPP

1.487
INCIDENTES

12%

PHISHING

1.359
INCIDENTES

11,4%

ESTAFA
POR COMPRA Y/O VENTA DE PRODUCTOS EN INTERNET

1.127
INCIDENTES

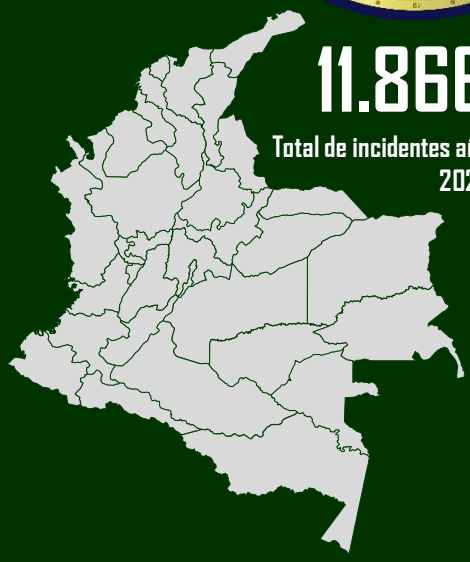
9,4%

GOTA A GOTA
VIRTUAL

1.100
INCIDENTES

9,2%

TOTAL
42%



11.866
Total de incidentes año 2024

3.656
Correos electrónicos atendidos

4.570
Chats WhatsApp atendidos

1.197
Llamadas atendidas

2.443
Chats aplicativo web

BALANCE ANUAL 2024

PRINCIPALES MODALIDADES

ROBO CUENTAS DE WHATSAPP

Conducta que permite a los ciberdelincuentes el acceso abusivo a un sistema informático, apoderándose de una cuenta de usuario, con el fin de realizar fraudes (violación de datos personales, estafas, entre otros) buscando beneficios económicos, esto es posible ya que se involucran diversas técnicas para obtener información de la víctima y vulnerar las medidas de seguridad mediante engaños.

¿Cómo funciona?

Los atacantes obtienen el número de la víctima de bases de datos filtradas, redes sociales o simplemente contactando a personas al azar.

El delincuente instala WhatsApp en un dispositivo nuevo e introduce el número de teléfono de la víctima, generando un código de verificación por SMS o llamada telefónica.

El atacante utiliza técnicas de ingeniería social para engañar a la víctima y hacer que le envíe el código de verificación, generalmente, suplantando al soporte técnico, alegando un intento no autorizado de acceder a la cuenta.

Una vez recibe el código, puede acceder a la cuenta y tomar control total sobre ella, permitiendo comunicarse con los contactos de la víctima y materializar estafas solicitando dinero en nombre del usuario.

¿Cómo evitar ser víctima?

- **Activar**: Verificación en dos pasos
- **Desconfiar**: De mensajes sospechosos
- **Evitar**: Compartir información por medios digitales

BALANCE ANUAL 2024

PRINCIPALES MODALIDADES

UTILIZACIÓN DE INTELIGENCIA ARTIFICIAL PARA LA COMISIÓN DE CONDUCTAS DELICTIVAS

Los ciberdelincuentes han integrado el uso de la IA para mejorar los ataques maximizando las oportunidades de obtener ganancias a corto plazo, explotando nuevas vulnerabilidades y modelos de negocios criminales más innovadores, teniendo en cuenta que, evaden la seguridad de los sistemas, creando así cambios constantes en el panorama cibercriminal a nivel internacional, así como desafíos importantes para las fuerzas del orden y la ciberseguridad en general.

DEEPFAKE
¿Cómo funciona?

Es una modalidad de cibercrimen, que consiste en crear archivos de vídeo manipulados mediante un software de inteligencia artificial de modo que parezcan reales. La finalidad es inducir al error a las personas receptoras mediante la facilitación de la difusión en masa de desinformación, afectando la credibilidad de la ciudadanía.

UTILIZACIÓN POR LOS CIBERDELINCUENTES

01 **Reemplazo de rostros**: consiste en el intercambio de caras de una persona con otra.

02 **Recreación gestual:** manipulan las características faciales de una persona con el fin de aparentar que está diciendo algo que no ha mencionado.

03 **Generación de rostros:** creación de imágenes sintéticas convincentes de personas inexistentes.

COMO IDENTIFICAR UN DEEPFAKE

Características de relevancia: movimientos bruscos, cambios de iluminación de un fotograma al siguiente, parpadeo extraño o ausencia de los mismos, cambios en el tono de la piel y aparición de elementos o aplicaciones digitales en la imagen.

BALANCE ANUAL 2024

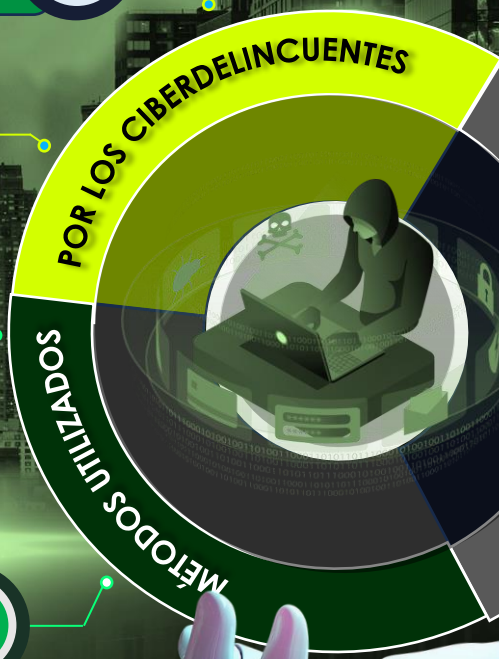
PRINCIPALES MODALIDADES

DEEPVOICE

¿Cómo funciona?

Consiste en suplantar la voz de las personas, mediante el uso de inteligencia artificial la cual permite modular la entonación original, para producir contenidos o mensajes falsos de modo que parezcan auténticos.

MÉTODOS UTILIZADOS POR LOS CIBERDELINCUENTES



1. El ciberdelincuente toma un audio como muestra de la voz de la persona a la que va a suplantar.
2. Ingresa los contenidos que se quieren producir a partir de la suplantación de voz, en aplicaciones y servicios de inteligencia artificial.
3. Somete la muestra de voz (audio) a herramientas de prueba para determinar las diferentes cualidades acústicas (*timbre, volumen, tono, duración o velocidad, y ritmo*).
4. Inducen al error mediante a través de los contenidos falsos, para afectar la credibilidad de la ciudadanía y suplantar personas con fines económicos o extorsivos.

BALANCE ANUAL 2024

OPERACIONES MÁS RELEVANTES

"ISERVER"

En trabajo de cooperación con EUROPOL y AMERIPOL se logró desarticular una Red Criminal Internacional (*Argentina*, *Ecuador*, *España*, *Perú* y *Colombia*) cuyo accionar consistía en el uso de una plataforma virtual para desbloquear los terminales Móviles (celulares) que eran hurtados en los diferentes países, para llevar a cabo diversos delitos cibernéticos (acceso abusivo, filtración de datos, extorsión y fraudes), en un escenario de Crimen como Servicio (Crime as a Service).

Capturas **3** | Allanamientos **9** | Incautación **123**

"CRIPTOESPAÑA – CANMONEY"

En una operación conjunta de la Fiscalía, Guardia Civil de España, DIPOL e INTERPOL, se materializó notificación roja a un colombiano requerido por extradición y se capturó a otro en flagrancia por porte ilegal de armas. Se realizaron allanamientos en Cúcuta y Bogotá, mientras que en España se detuvieron a tres colombianos y un español. Esta operación desarticuló una red criminal que cometió 240 fraudes informáticos en Europa por 6 millones de euros, transferidos a Colombia mediante criptoactivos y 12 billeteras virtuales.

Capturas **1** | Allanamientos **3** | Incautación **250**

BALANCE ANUAL 2024

OPERACIONES MÁS RELEVANTES

"LOS CRIPTOCITAS"

Se logró la desarticulación de una organización criminal, la cual creaba perfiles falsos en aplicaciones de citas, para contactar ciudadanos en su mayoría extranjeros. Las personas involucradas ganaban la confianza de sus víctimas, proponían encuentros físicos y por medio de sumisión con sustancias químicas (escopolamina) desorientaban a los ciudadanos con el fin de obtener acceso a sus billeteras virtuales, hurtando criptoactivos mediante transferencias no autorizadas, recaudando más de 200 millones de pesos en cripto.

Capturas **3** | Allanamientos **2** | Incautación **9**

"RESERVE"

Tras varios meses de investigación, se logró capturar a alias "*Insider*" en la ciudad de Armenia, quien habría transferido 1.25 millones de la criptomoneda Tether (equivalente a la misma cantidad en dólares), de una empresa estadounidense. El fraude se realizó entre el año 2021 y 2023, mediante 80 transacciones fraudulentas que el capturado realizaba a 05 billeteras virtuales administradas por él, así como la eliminación de los registros en los sistemas de la empresa, para evitar ser descubierto.

Capturas **1** | Allanamientos **2** | Incautación **1**

BALANCE ANUAL 2024

"FENIX"

Se logró desarticular la organización criminal que durante 5 años, participó en la expedición de más de 11.638 libretas militares de manera fraudulenta, representando una afectación al recaudo nacional de 22.000 millones de pesos. Se generó Extinción del Derecho de Dominio a 41 bienes inmuebles por un valor de $17 mil millones de pesos.

"HACKER REMOTO"

En la ciudad de Medellín y Valledupar se realizó la desarticulación de la mayor estructura criminal de distribución de software malicioso en Colombia "Virus informático", los cuales generaban diariamente más de 10.000 correos y/o mensajes de texto falsos, suplantando instituciones públicas y privadas, tales como la Fiscalía General de la Nación, Secretarías de Tránsito, DIAN, INTERPOL y bancos.

BALANCE ANUAL 2024

OPERACIONES MÁS RELEVANTES

"SKYPE"

En Norte de Santander, se logró desarticular una organización criminal que mediante la plataforma de mensajería instantánea Telegram, ofrecía material de abuso sexual infantil a extranjeros, a cambio de dádivas. La información fue obtenida en coordinación con EUROPOL e INTERPOL. Adicionalmente, durante el allanamiento, se capturó a un colombiano de 48 años en flagrancia por fabricación, tráfico y tenencia de armas.

Capturas **3**

Allanamientos **2**

BALANCE ANUAL 2024

RESULTADOS ESTRATÉGICOS

Medios de comunicación

Impacto en redes sociales

140.583
Interacciones

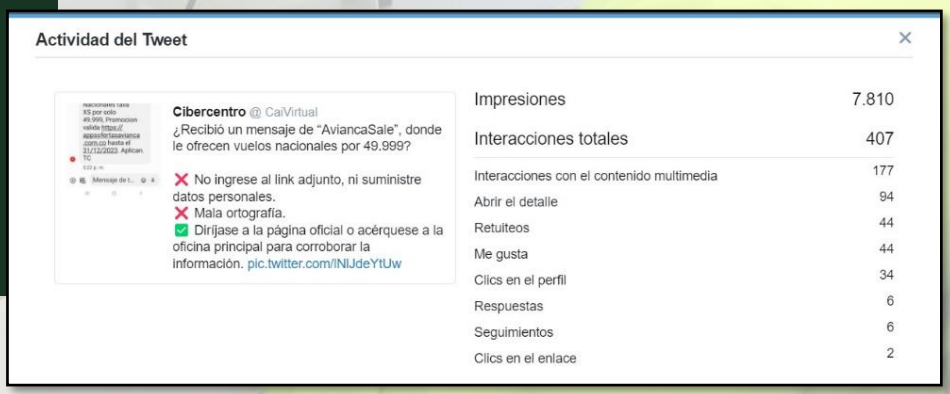
SEGUIDORES

61.440 | 11.656

8%

5.554
NUEVOS SEGUIDORES
Redes Sociales
CAI Virtual.

Publicación de Mayor Impacto



BALANCE ANUAL 2024

RESULTADOS ESTRATÉGICOS

CHARLAS DE PREVENCIÓN Y CONCIENCIACIÓN

El Centro Cibernético Policial, realizó charlas de prevención y concienciación en instituciones educativas públicas y privadas sobre el uso adecuado de las TIC´S, responsabilidad penal para adolescentes y riesgos en las redes sociales, reduciendo el riesgo en los niños, niñas y adolescentes (N.N.A) de ser víctimas de modalidades como el grooming, ciberbullying, sexting, ciberacoso, entre otros; impactando a estudiantes, padres de familia, cuidadores y directivas de las instituciones educativas.

CHARLAS REALIZADAS

144

IMPACTADOS

13.451

BALANCE ANUAL 2024

RESULTADOS COP16

15 Reuniones de Seguimiento

12 Boletines Estratégicos

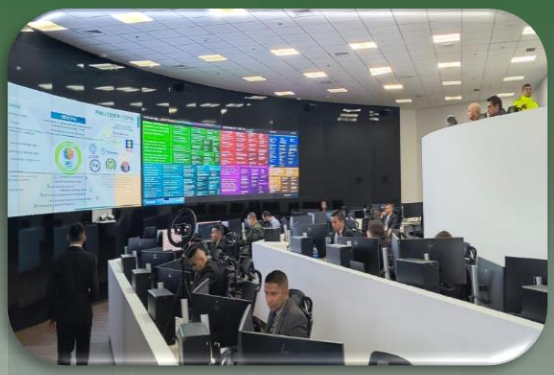
10 Análisis de Vulnerabilidades
Página COP16 – Página Ministerio Ambiente.

118 Hashtags Identificados
895 Millones de interacciones.

Capacidades:

- 25 Analistas destacados.
- Creación del protocolo para atención de incidentes de seguridad digital.
- Cooperación internacional e intercambio de información a través de los canales I-24/7 y canal de Budapest.
- Generación de alertas de ciberseguridad.
- Laboratorios de informática forense.

PMU CIBER



INTEGRANTES PMU CIBER

1. Presidencia de la República.
2. Ministerio de Ambiente y Desarrollo Sostenible
3. MINTIC (CSIRT GOBIERNO y COLCERT).
4. Fiscalía General de la Nación.
5. Dirección Nacional de Inteligencia –DNI.
6. Ministerio de Defensa Nacional (CSIRT Defensa).
7. Comando Conjunto Cibernético (CCOCI).
8. Policía Nacional.

Presidencia

COP16 COLOMBIA Paz con la Naturaleza

Fuente: Centro Cibernético Policial

BALANCE ANUAL 2024

GESTIÓN Y RESULTADOS

CAPTURAS

362 Realizadas en todo el territorio nacional en articulación con la Estrategia Integral de Ciberseguridad (**ESCIB**).

313 Delitos informático Ley 1273.

49 Material de Abuso Sexual Infantil.

29 Operaciones

16 Nivel Central

13 Nivel Desconcentrado

Resultados Estratégicos

PÁGINAS BLOQUEADAS
30.165

23.409 Material de Abuso Sexual Infantil.

6.756 Juegos ilegales de azar.

INCIDENTES ATENDIDOS
11.866

ALERTAS PREVENTIVAS
424

CHARLAS DE PREVENCIÓN
144

13.451 Impactados.

MENSAJES INTERCAMBIADOS MEDIANTE COOPERACIÓN INTERNACIONAL
396

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL
CENTRO CIBERNÉTICO POLICIAL