

**DIRECCIÓN DE INVESTIGACIÓN  
CRIMINAL E INTERPOL  
CENTRO CIBERNÉTICO POLICIAL  
BALANCE DE CIBERSEGURIDAD  
2023**



# BALANCE DE CIBERSEGURIDAD 2023



## Tabla de Contenido

	Pág.
❖ Introducción.....	3
❖ Comportamiento del fenómeno.....	4
❖ CAI Virtual.....	5
❖ Gestión y resultados.....	9
❖ Operaciones.....	10
❖ PMU Ciberelectoral 2023.....	14
❖ Comunicaciones estratégicas.....	15
❖ Resultados estratégicos.....	16



**BG. José Luis Ramírez Hinestroza**

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, logrando una reducción histórica para el año 2023 del -10% de denuncias por delitos informáticos.

# DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL

## CENTRO CIBERNÉTICO POLICIAL

# BALANCE DE CIBERSEGURIDAD 2023

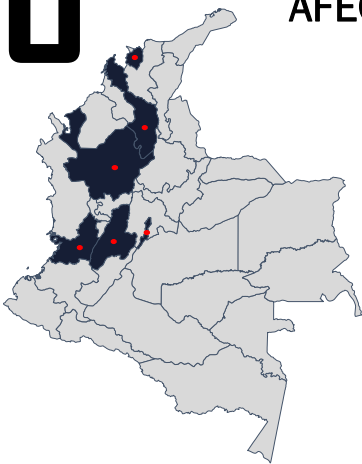


## Comportamiento del fenómeno

En el año 2023 se reportaron **59.033** denuncias por delitos informáticos, representando un **decremento** del **-10%** respecto del año 2022 con **65.794** denuncias.

Por otra parte, las ciudades con mayor afectación fueron Bogotá, Medellín, Cali, Barranquilla, Cartagena e Ibagué.

## 6 CIUDADES CON MAYOR AFECTACIÓN



**54%**  
FENÓMENO

Denuncias % Fenómeno

Bogotá	19.542	33%
Medellín	5.144	9%
Cali	3.230	5%
Barranquilla	1.694	3%
Cartagena	1.238	2%
Ibagué	1.096	2%

## 9 DELITOS INFORMÁTICOS DENUNCIAS

2022 | 2023

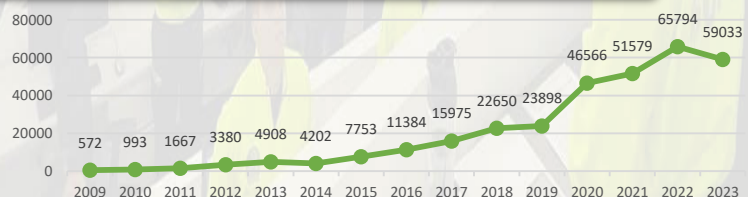
Hurto por medios informáticos y semejantes	26.366	28.512	+8%
Acceso abusivo a un sistema informático	13.081	10.883	-17%
Violación de datos personales	13.588	9.639	-29%
Suplantación de sitios web	5.751	4.393	-24%
Transferencia no consentida de activos	3.578	3.303	-8%
Intercepción de datos informáticos	1.989	1.311	-34%
Daño informático	631	397	-37%
Uso de software malicioso	418	299	-29%
Obstaculización ilegítima de sistema informático o red de telecomunicación	392	296	-25%

**59.033**  
TOTAL  
DENUNCIAS

**-10%** Decremento denuncias.

Fuente: SIEDCO PLUS 2.0

## EVOLUCIÓN HISTÓRICA (No. Denuncias vs año)



Ley 1273  
2009

# BALANCE DE CIBERSEGURIDAD 2023



## CAI VIRTUAL

TOP 4 MODALIDADES  
INCIDENTES ATENDIDOS

Variación 2022 y  
2023

PHISHING



6.804  
INCIDENTES

106%

ESTAFA

POR COMPRA Y/O VENTA DE PRODUCTOS  
EN INTERNET



2.035  
INCIDENTES

-12%

FALSEDAD  
PERSONAL EN ENTORNOS  
DIGITALES



875  
INCIDENTES

-64%

AMENAZAS  
A TRAVÉS DE REDES  
SOCIALES



806  
INCIDENTES

-16%

El CAI Virtual, es la primera plataforma en Iberoamérica que brinda un servicio dedicado a la prevención, sensibilización y atención de incidentes cibernéticos, dirigido a la ciudadanía contra los delitos cibernéticos.

El lanzamiento de la segunda versión del CAI Virtual, permitió focalizar la atención al ciudadano, destacando de manera diferencial el servicio en línea 24/7, orientado a dar respuestas a los incidentes cibernéticos reportados por los ciberciudadanos. Asimismo, a través de la plataforma se pueden consultar los balances y boletines en materia de ciberseguridad, los cuales incluyen noticias de interés, alertas preventivas, estadísticas de cibercriminalidad y resultados estratégicos.



**El lanzamiento de la segunda versión del CAI virtual fue el 22 de febrero de 2023.**

# BALANCE DE CIBERSEGURIDAD 2023



## PRINCIPALES MODALIDADES

### PHISHING

#### ¿Cómo funciona?

Es una técnica de ingeniería social que consiste en el envío de correos electrónicos fraudulentos que suplantan la identidad de empresas o instituciones legítimas, con el objetivo de engañar a los usuarios para que proporcionen información personal o financiera, como contraseñas, números de tarjeta de crédito o información bancaria, entre otros.

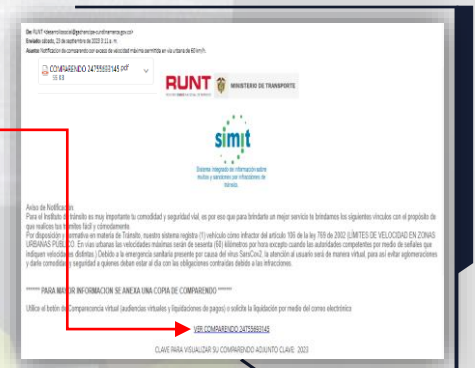
#### ¡ Campaña notificación de comparendo!

Esta campaña consistió en suplantar a plataformas de las autoridades de tránsito, con el fin de ejecutar actividades maliciosas en el sistema y/o comprometer información personal de la víctima, relacionando el siguiente asunto: ***“Notificación de comparendo por exceso de velocidad máxima permitida en vía urbana de 60 km/h”.***

El correo allegado solicita al usuario dar clic en [VER COMPARENDO 24755693145](#) el cual contiene una URL oculta.

Asimismo, es adjuntado un archivo en formato PDF del supuesto comparendo, que lo invita a dar clic el enlace.

Una vez ejecutado el archivo, requiere una contraseña de acceso que es suministrada en el mismo correo y PDF, donde iniciará la ejecución del software malicioso para infectar el dispositivo y/o la captura de información confidencial.



PDF

# BALANCE DE CIBERSEGURIDAD 2023



## PRINCIPALES MODALIDADES

### ESTAFA

#### POR COMPRA Y/O VENTA DE PRODUCTOS EN INTERNET

#### ¿Cómo funciona?

Se caracteriza por el hurto al patrimonio económico a través de la compra y/o venta de productos, ofertas de servicios de hospedaje, arrendamiento de inmuebles y planes vacacionales a lugares turísticos, por medio de plataformas o perfiles en redes sociales.

#### ¡ Características!

- ✓ **Suplantán** a propietarios reales para generar estafas.
- ✓ **Ofrecen** descuentos entre el 40 y 60% o por debajo del valor real.
- ✓ **Crean** cuentas y páginas falsas de supuestos promotores de agencias turísticas.

#### ¿Cómo identificar páginas falsas?



1 Consulte si tiene Registro Nacional de Turismo en la página web [www.rues.org.co/rnt](http://www.rues.org.co/rnt), puede consultar.

2 Asegúrese que la página web utilice protocolos seguros de comunicación.

3 Verifique que esté agremiada a la Asociación Colombiana Hotelera (COTELCO) y/o la Asociación Colombiana de Agencias de Viajes y Turismo (ANATO).

4 Verifique que la página web tenga un certificado SSL válido.

5 Revise la página web y no caiga en los trucos de formularios de solicitud.

6 Verifique que la página web tenga perfiles en redes sociales y que la información sea consistente y verificable.

7 Estas páginas web suelen tener errores en la gramática, estilo de redacción o uso del lenguaje.



# BALANCE DE CIBERSEGURIDAD 2023



## PRINCIPALES MODALIDADES

### FALSEDAD PERSONAL EN ENTORNOS DIGITALES

#### ¿Cómo funciona?

Se refiere a la actividad de usar la identidad de otra persona sin consentimiento, con el objetivo de causar daño o perjuicio a terceros. Este tipo de conducta puede incluir la creación de perfiles falsos en redes sociales, el uso de fotos o datos personales, con el fin de cometer fraudes o generar ciberacoso.

#### ¿Cómo evitar ser suplantado en Internet?



No publique información personal sensible, como direcciones o documentos valiosos.



Sea selectivo al aceptar solicitudes de amistad y elimine perfiles que ya no se utilizan.



Esté atento a la creación de perfiles falsos que puedan suplantar la identidad.



No comparta contraseñas personales.



Procure configurar la privacidad de sus redes sociales.



# BALANCE DE CIBERSEGURIDAD 2023



## Gestión y Resultados

### Variación 2022

**38.801** PÁGINAS BLOQUEADAS

**56%**  
(24.875)

35.104 Contenido explotación sexual Infantil.

3.697 Juegos ilegales en línea.

**16.597** INCIDENTES  
atendidos CAI Virtual.

(16.909)

**581** ALERTAS PREVENTIVAS  
redes sociales CAI Virtual.

**53%**  
(379)

**223** ANÁLISIS  
muestras de software maliciosos.

**160** CHARLAS DE PREVENCIÓN

22.509 personas informadas y sensibilizadas.

**14%**  
(140)

**766** MENSAJES INTERCAMBIADOS

SIENA de EUROPOL con 27 países

**138%**  
(321)

# 352 CAPTURAS

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

**277** DELITOS INFORMÁTICOS  
LEY 1273 DEL 2009.

**75** EXPLOTACIÓN SEXUAL  
INFANTIL EN INTERNET.

## 28 Operaciones

**16** Nivel Central

**12** Nivel Desconcentrado

## 03 OPERACIONES

Trasnacionales



EUROPEAN CYBERCRIME CENTRE  
**EC3**  
EUROPOL



**100%** Cumplimiento  
operacional

- 16 DIJIN
- 02 MEVAL
- 02 MECAL
- 01 MEBAR
- 01 DECUN
- 02 DEQUI
- 01 MEBUC
- 01 MEVIL
- 01 METIB
- 01 MECAR

# BALANCE DE CIBERSEGURIDAD 2023



## Operaciones más relevantes



### ACCUSER

El 10/02/2023, gracias a información suministrada por el Organismo de Investigación Judicial de Costa Rica remitida por el canal oficial de INTERPOL, se logró la captura por orden judicial de un individuo que contactaba a una niña costarricense (10 años), exigiéndole contenido sexual mediante amenazas por medio de las plataformas OMEGLE (plataforma de chat en vivo) y WhatsApp, simulando ser un menor de edad (modalidad Grooming).

### PANZERFAUST

El 27/03/2023, se logró efectuar diecinueve capturas por orden judicial por el hurto de 2.775 millones de pesos a los fondos del municipio de Nocaima (Cundinamarca). Esta estructura se dedicaba al hurto por medios informáticos y uso de software malicioso.



### DOS CARAS

El 19/04/2023 se logró la captura de una persona que contactaba y acosaba a una niña de 13 años, a través de las redes sociales, Facebook y WhatsApp, ofreciéndole entre 100.000 y 130.000 pesos a cambio de tener relaciones sexuales. En el análisis realizado a la evidencia, se identifica las conversaciones y las peticiones que el victimario le hacía a la menor de edad.



# BALANCE DE CIBERSEGURIDAD 2023



## Operaciones más relevantes

### EL COLECCIONISTA

El 02/05/2023 se materializó la captura en Candelaria -Valle del Cauca, por el delito de Pornografía con Persona Menor de 18 años, contra un individuo que distribuía Material de Abuso Sexual Infantil (MASI) en la Darknet, miembro de 250 grupales (más de 3.500 usuarios a nivel mundial), identificando mas de 450 mil imágenes y videos que datan desde el año 2012. A su vez, se dejan fuera de servicio dos servidores online donde compartía este contenido.



### ANONYMOUS

El 08/05/2023 se materializó una orden de captura contra el actor criminal autodenominado OrgOn perteneciente a la estructura cibercriminal internacional ANONYMOUS en el Municipio de Aguazul, Casanare, quien habría realizado ataques a más de 500 sitios web y sería el reclutador de nuevos integrantes de esta estructura en Colombia.



### MERCURIO

El 05/06/2023 en la ciudad de Barranquilla, se logró la captura de catorce personas quienes realizaron fraudes informáticos por un valor de \$862'721.801 pesos. Uno de los integrantes (alias "VALLE"), era el segundo al mando de la subestructura "GERLIN PINO DUARTE" del Grupo Armado Organizado (GAO) "CLAN DEL GOLFO", encargado de realizar extorsiones en el municipio de Puerto Colombia - Atlántico.



# BALANCE DE CIBERSEGURIDAD 2023



## Operaciones más relevantes



### APOLO

El 23/08/2023, en los municipios de Bello, Itagüí, Apartadó y Medellín del departamento de Antioquia, se materializaron cuatro capturas por orden judicial, por los delitos de estafa agravada en modalidad masa y suplantación de sitios web para capturar datos personales, suplantando empresas como AMAZON y Mercado Libre para ofrecer falsos empleos e inversiones, logrando así esclarecer más de 150 denuncias.

### LOS TRADERS

El 12/09/2023 se materializaron tres ordenes de captura contra una organización delincencial, quienes citaban a sus víctimas (nacionales y extranjeras) a través de la aplicación de citas Tinder, procediendo a drogarlas con escopolamina para posteriormente con datafonos portátiles, realizar transferencias a diferentes cuentas, hasta desocupar los fondos de las tarjetas.



### PALOMA

A través de cooperación internacional con EUROPOL, la Policía de Noruega informó sobre la captura de un ciudadano Español en su territorio, quien tendría conexión con Colombia en la compra de material de explotación sexual infantil; logrando el 19/09/2023, materializar captura por orden judicial en el municipio de Pamplona - Norte de Santander, de la madre de la víctima de 3 años de edad; así como el rescate de la niña.

# BALANCE DE CIBERSEGURIDAD 2023



## Operaciones más relevantes

### PAUTA DIGITAL

El 21/09/2023 en la ciudad de Bogotá, se materializó una captura, a quien accedía abusivamente a los sistemas de información de medios de comunicación nacionales, para inyectar software malicioso y así, incluir pautas digitales que no habían sido autorizadas, cometiendo un fraude por más de 600 millones de pesos.



### PLATAFORMAS

El 09/10/2023 en la ciudad de Bogotá y Medellín, se logró la captura de nueve personas (una de nacionalidad China) e incautación de +7800 EMP a quienes generaron aplicaciones móviles, con las que accedían a datos personales (imágenes, videos, ubicaciones, contactos, entre otros); para constreñir y extorsionar a más de 1.300 víctimas. De igual forma, se generaron medidas cautelares con fines de extinción del derecho de dominio a bienes evaluados en más de 2.100 millones de pesos.

Bogotá: cayó ciudadana china que lideraba red de 'gota a gota' a través de aplicaciones

### HONOR

El 15/11/2023 en las ciudades de Riohacha y Santa Marta, se logró la captura de tres integrantes de una organización criminal, quienes realizarían fraude a las arcas de la Policía Nacional por un valor 429.586.464 pesos, mediante el acceso abusivo y modificación de información de los sistemas de SIIF Nación y SAP pertenecientes al Tesoro Público Nacional, es de anotar, que la líder de la organización, era funcionaria activa de la institución y hoy se encuentra condenada por la Justicia Penal Militar.

A cárcel tres capturados inmersos en caso de patrullera de la Policía de origen guajiro



LA PRENSA HOY

CORTINADO PROMOCIONADO

# BALANCE DE CIBERSEGURIDAD 2023



## PMU CIBERELECTORAL 2023

**16** ALERTAS PREVENTIVAS  
505 IP restringidas

**8.777** PÁGINAS VERIFICADAS  
Dominio .GOV.CO

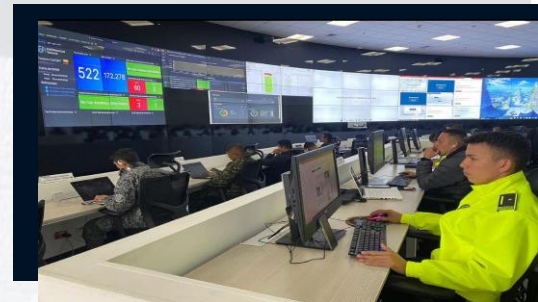
**19** INCIDENTES (PHISHING)  
Suplantación Registraduría Nacional.

**09**  
ENTIDADES

### RESULTADOS:

- 12 boletines enviados desde el PMU Ciberelectoral.
- Verificación en línea de 42 servicios productivos y 13 servicios electorales de la RNEC, sin presentar ataques cibernéticos.
- 4 alertas de seguridad digital emitidos por CSIRT Presidencia, sobre amenazas identificadas.
- 09 capturas en flagrancia por delitos electorales, 02 capturas en flagrancia por otros hechos, 90 capturas por orden en mesa y 187 denuncias recibidas a través de URIEL.
- 102 indicadores de compromiso IoC.

### PMU CIBERELECTORAL



29 octubre 2023



### INTEGRANTES PMU CIBERELECTORAL

1. Presidencia de la República.
2. Registraduría Nacional del Estado Civil.
3. Consejo Nacional Electoral.
4. MINTIC (CSIRT GOBIERNO y COLCERT).
5. Fiscalía General de la Nación.
6. Dirección Nacional de Inteligencia – DNI.
7. Ministerio de Defensa Nacional (CSIRT Defensa).
8. Comando Conjunto Cibernético (CCOCI).
9. Policía Nacional.



# BALANCE DE CIBERSEGURIDAD 2023

## Comunicaciones Estratégicas

### Medios de comunicación

### Impacto en redes sociales

122.350

Interacciones

SEGUIDORES



61.221



7.817



288

4% ↑ **3.087**  
**NUEVOS SEGUIDORES**  
 Redes Sociales  
 CAI Virtual.



DESTACADOS DE LOS POSTS

<p><b>Tweet principal</b> tuvo 23,9 mil impresiones</p> <p>#CaIVirtualAlerta.</p> <p>Correo de asunto: "Usted tiene un proceso pendiente y no se le permitirá la salida del país" es FALSO... Se trata de un engaño para difundir #Malware suplantando a @MigracionCol.</p> <p>[No de clic] pic.twitter.com/U65hpnaoY0</p>	<p><b>Tweet con contenido multimedia principal</b> tuvo 22,7 mil impresiones</p> <p>Con la modalidad de #Phishing: Este mensaje busca suplantar sitios web para extraer datos personales, información financiera y credenciales de acceso a la banca virtual, no dude en informar al @CaIVirtual.</p> <p>#DiosYPatria pic.twitter.com/BmBET5ccqj</p> <p>Tu envío asignado a 472 se encuentra pendiente del pago de distribución. Consulta: gclnk.com/ed5JT01oUE Inf: 018000111210</p>	<table border="1"> <tr> <td>Posts</td> <td>29</td> <td>Post impressions</td> <td>194 mil</td> </tr> <tr> <td>Visitas al perfil</td> <td>9.542</td> <td>Menciones</td> <td>1.037</td> </tr> <tr> <td>Nuevos seguidores</td> <td>158</td> <td></td> <td></td> </tr> </table>	Posts	29	Post impressions	194 mil	Visitas al perfil	9.542	Menciones	1.037	Nuevos seguidores	158		
Posts	29	Post impressions	194 mil											
Visitas al perfil	9.542	Menciones	1.037											
Nuevos seguidores	158													

### Publicaciones de mayor impacto

194mil impresiones  
 9.542 visitas al perfil  
 1.037 menciones  
 158 nuevos seguidores

# BALANCE DE CIBERSEGURIDAD 2023

## Resultados Estratégicos

# 247

Relacionamientos estratégicos

Visitas estratégicas que permiten referenciar, articular y generar confianza con diferentes sectores y entidades públicas y privadas (*agencias de ley internacionales, sector financiero, entre otros*), con el fin de fortalecer las capacidades institucionales para la investigación y prevención del cibercrimen, donde se resaltan las siguientes:



### SECRETARIO GENERAL INTERPOL

Visita del Secretario General de INTERPOL, Jürgen Stock, afianzando la cooperación policial internacional efectiva para hacer frente contra los desafíos de la ciberdelincuencia.



### BINANCE

Visita de referenciación y capacitación por parte del equipo de investigaciones de Binance, con el fin de articular y fortalecer la cooperación en la investigación de delitos que involucran el uso de criptoactivos.

# BALANCE DE CIBERSEGURIDAD 2023

## Resultados Estratégicos



### GRUPO DE TRABAJO CONJUNTO DE ACCIÓN CONTRA EL CIBERDELITO EUROPOL

Capacitación en técnicas de investigación de criptoactivos, dictada por Europol y la Policía Federal de Bélgica, con la participación de distintas Direcciones de la Policía Nacional de Colombia.



### ESPAÑA

Visita de oficiales de la Guardia Civil de España, para fortalecer las alianzas en la lucha frontal contra el cibercrimen y exploración de nuevas estrategias para luchar contra los delitos realizados con el uso de divisas digitales.

# BALANCE DE CIBERSEGURIDAD 2023

## Resultados Estratégicos



### EUROPOL

Visita de referenciación por parte de funcionarios del International Nuclear Security Forum, quienes se encontraban realizando el "Taller Sobre el Desarrollo de una Política Nuclear" aportando con nuestra experiencia al proceso de formación académica.

### PAÍSES BAJOS

Visita del señor Coronel Huib Zwaan, oficial de enlace de la Policía Nacional de los Países Bajos, dando a conocer las capacidades del Centro Cibernético Policial en la lucha frontal contra el cibercrimen.



### SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA SLP

Visita de la Secretaría de Seguridad y Protección Ciudadana de México, para referenciar las capacidades como actores del ecosistema de seguridad digital en Colombia.



# BALANCE DE CIBERSEGURIDAD 2023

## Resultados Estratégicos

### **POLICÍA FEDERAL DE ALEMANIA**

Visita de referenciación de la Policía Federal de Alemania, donde se abordaron aspectos importantes de prevención y buenas prácticas de ciberseguridad.



### **FUERZA AEREA DE MÉXICO**

Visita de señores Generales de México, con el propósito de intercambiar experiencias y buenas prácticas en la lucha contra el cibercrimen.

### **POLICÍA DE ECUADOR**

Visita de la Policía de Ecuador, donde se expusieron las capacidades investigativas, de cooperación internacional y estrategias orientadas a la prevención y lucha contra el cibercrimen.



## Resultados Estratégicos



### **POLICÍA JUDICIAL DE PORTUGAL Y EUROPOL**

La Policía Judicial de Portugal y Europol, unieron **||||** esfuerzos operacionales contra el cibercrimen y la persecución de este fenómeno a nivel internacional.



### **EMBAJADORA DE CIBERSEGURIDAD DEL REINO UNIDO**

Se atendió la visita de referenciación de la Embajadora **||||** de Ciberseguridad del Reino Unido, fortaleciendo la articulación y cooperación internacional con este país.

### **ESCUELA SUPERIOR DE GUERRA**

Visita por parte los estudiantes de la Maestría en **||||** Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, fortaleciendo los conocimientos y las respuestas a los incidentes cibernéticos desde la óptica de la academia.



# BALANCE DE CIBERSEGURIDAD 2023

## 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 que los niños, niñas y adolescentes (N.N.A) sean víctimas de modalidades como el grooming, cyberbullying, sexting, ciberacoso, entre otros; impactando a estudiantes, padres de familia, cuidadores y directivas de las instituciones educativas.



CHARLAS  
REALIZADAS

147

IMPACTADOS

21.506



**DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL**  
**CENTRO CIBERNÉTICO POLICIAL**  
**2023**

