



CENTRO CIBERNÉTICO POLICIAL

INFORME CIBERCRIMEN 2021



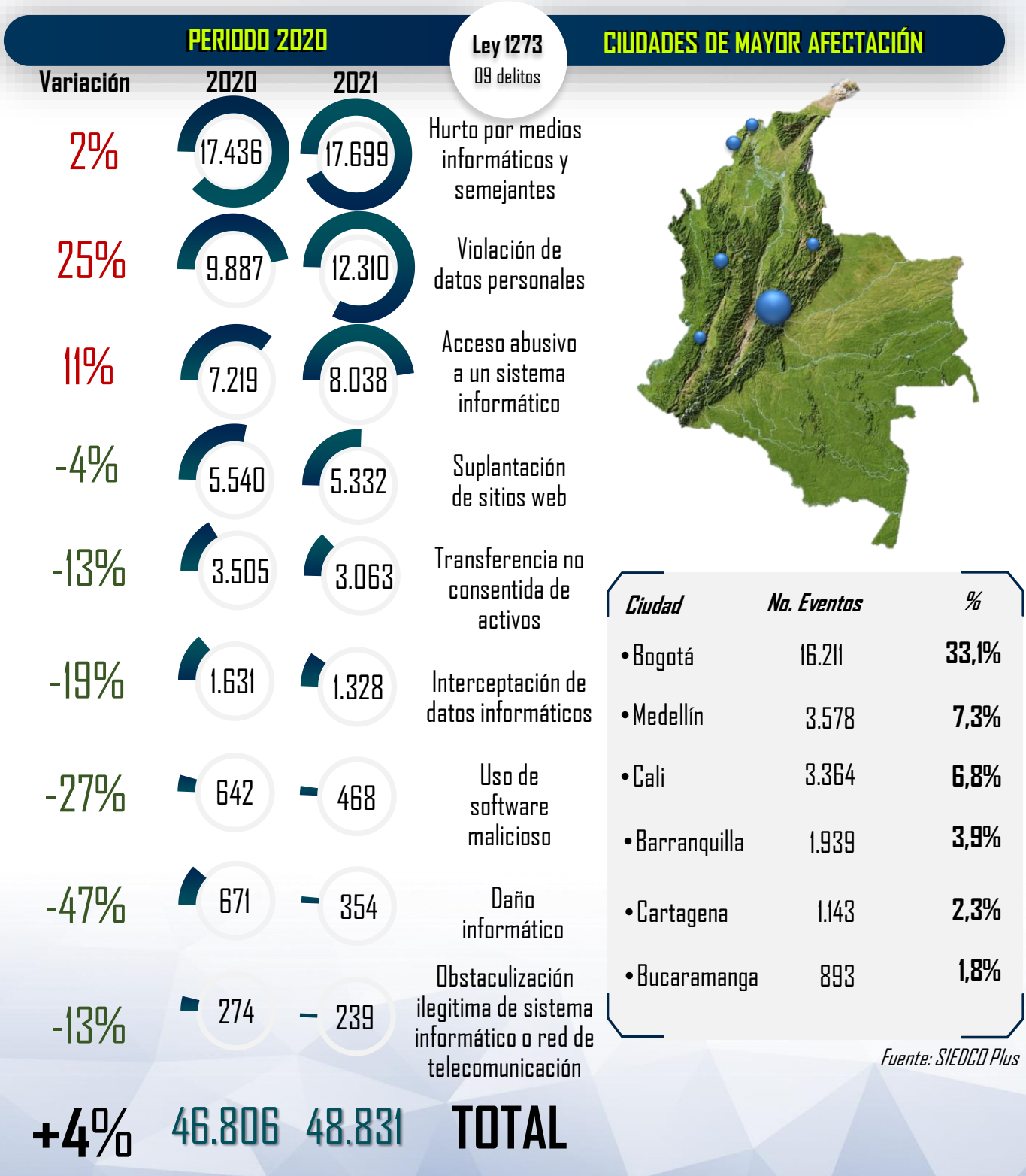
Las tecnologías de la información y las comunicaciones en el mundo han tenido gran acogida, evidenciando que diferentes actividades del entorno cotidiano están migrando a la Web. Aspecto que ha sido explotado por parte de los ciberdelincuentes, quienes mejoraron su actuar criminal para lograr un mayor alcance con mejores beneficios y menos exposición. Este cambio ha planteado nuevos retos a las agencias de aplicación de la ley, quienes han tenido que evolucionar para mitigar las acciones criminales que pretenden afectar el bien jurídico tutelado de la información y los datos.

CENTRO CIBERNÉTICO POLICIAL

BALANCE CIBERCRIMEN



En Colombia se registró el mayor número de denuncias frente al delito "Hurto por medios informáticos" con **17.699** casos y una variación del **2%** en comparación al año **2020**, por otra parte, las ciudades de mayor afectación fueron Bogotá, Medellín, Cali y Barranquilla.



CAI VIRTUAL



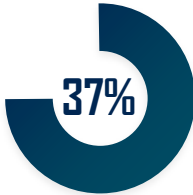
Es el servicio especializado de atención 24/7, brindado por la Policía Nacional de Colombia a través del Centro Cibernético Policial de la Dirección de Investigación Criminal e INTERPOL; mediante el cual las víctimas de los delitos cibernéticos pueden acceder y poner en conocimiento la información correspondiente al delito que les está afectando, donde se les brinda toda la asesoría correspondiente, informándoles los pasos a seguir para solucionar su incidente o instaurar la denuncia ante las autoridades pertinentes.

SECTORES AFECTADOS

A través de este servicio se recibieron **15.479** incidentes, siendo el sector de mayor afectación el **GOBIERNO (37%)**, seguido del sector **CIUDADANO (13%)**. Por otra parte, presentó una disminución el sector **MEDIOS DE COMUNICACIÓN (-66%)** y el sector **TECNOLOGÍA (-40%)**.

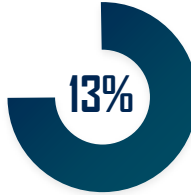
GOBIERNO

2020 567
2021 777



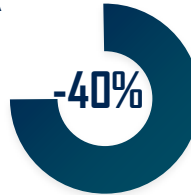
CIUDADANO

2020 7.802
2021 8.860



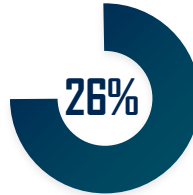
TECNOLOGÍA

2020 674
2021 407



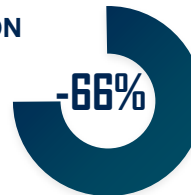
FINANCIERO

2020 1.874
2021 2.372



MEDIOS DE COMUNICACIÓN

2020 703
2021 246



PREVENCIÓN



INSTAGRAM

Seguidores: 5.836



TWITTER

Seguidores: 56.740



FACEBOOK

Seguidores: 14.695

ALERTAS



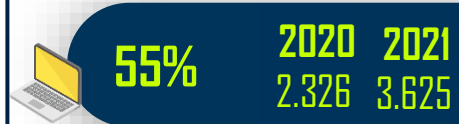
CHARLAS PREVENTIVAS



Modalidades

Las principales modalidades reportadas a nuestra plataforma por parte de la ciudadanía fueron las siguientes:

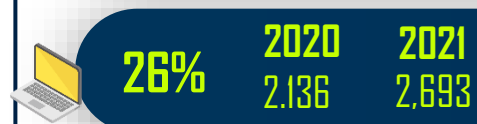
PHISHING



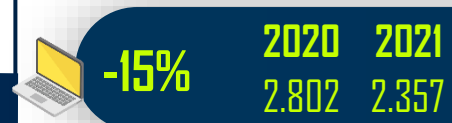
SMISHING



SUPLANTACIÓN DE IDENTIDAD



ESTAFA POR VENTA Y COMPRA DE PRODUCTOS ONLINE



MALWARE



ACTIVIDADES DE PREVENCIÓN EN CANALES NACIONALES DE TELEVISIÓN

CENTRO DE CAPACIDADES PARA LA CIBERSEGURIDAD DE COLOMBIA C4

**MATERIAL DE ABUSO
SEXUAL INFANTIL**

ALTA TECNOLOGÍA

SEGURIDAD CIUDADANA

FRAUDE

ABUSO SEXUAL INFANTIL EN LÍNEA



El abuso sexual infantil implica la transgresión de los límites íntimos y personales de los niños, niñas o adolescentes (NNA). Supone la imposición de comportamientos de contenido sexual por parte de una persona (un adulto u otro menor de edad) hacia un NNA, realizado en un contexto de desigualdad o asimetría de poder, habitualmente a través del engaño, la fuerza, la mentira o la manipulación.

MODALIDAD



7.139 URL'S BLOQUEADAS EN 2020
20.025 URL'S BLOQUEADAS EN 2021

GROOMING

Estrategia utilizada por un adulto a través de un perfil falso, para ganar la confianza de un menor a través de internet con fines sexuales.

Fueron reportados al CAI Virtual **516** incidentes.



En muchos casos a través de sobornos o engaños el agresor contacta al NNA y establece un vínculo de confianza. Normalmente finge otra edad, empatizando a un nivel profundo con los niños, niñas y/o adolescentes, simulando escuchar sus problemas y aprovecha esa información para manipular después.



En esta fase el ciberdelincuente pretende arrancar la red de apoyo natural del menor (familiares, amistades, docentes, etc.) dejándolo desprotegido, de esta manera insiste en la necesidad de mantener todo en secreto.



El delincuente suele preguntar a la víctima si alguien más conoce su relación e intenta averiguar quién más tiene acceso al ordenador o dispositivo que utiliza el menor.



En esta última fase el cibercriminal utiliza la manipulación, las amenazas, el chantaje o la coerción para que el NNA le envíe material sexual o la relación culmine con un encuentro físico.

Dentro de los delitos de cibercrimen con mayor impacto en relación a ciberataques contra las infraestructuras críticas del Estado, se encuentran:

PRINCIPALES MODALIDADES

CORREO
ELECTRÓNICO



REDES
SOCIALES



SUPLANTACIÓN
BANCARIA



PHISHING

Modalidad que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario suplantando una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información personal o realizar un cargo económico e infectar el dispositivo.

El ciberdelincuente envía correos de manera masiva con el fin de llamar la atención de incautos.

Si el ciudadano llegase a ingresar los datos personales en la página suplantada, el ciberdelincuente se apodera de la información personal.

Con la información personal puede suplantar al ciudadano por redes sociales, mensajería instantánea o realizar compras electrónicas.

Afecta a los contactos, patrimonio económico, honra y buen nombre del ciudadano afectado.



SEGURIDAD CIUDADANA



Durante el año 2021, el Centro Cibernético Policial realizó búsquedas de información pública en internet (Ciberpatrullaje), con el fin de identificar posibles delitos que afecten la seguridad ciudadana en internet.

Denuncias Estadística de las Modalidades

CALUMNIA

Año	Denuncias	%
2020	10,923	17%
2021	12,823	

AMENAZAS

Año	Denuncias	%
2020	35,699	28%
2021	45,682	

INJURIA

Año	Denuncias	%
2020	8,325	7%
2021	8,949	

TERRORISMO

Año	Denuncias	%
2020	301	52%
2021	457	

ESTUPEFACIENTES

Año	Denuncias	%
2020	44,019	11%
2021	48,769	

GRUPOS ARMADOS



CUENTAS BLOQUEADAS **281**

¡ DROGAS EN INTERNET !

Modus Operandi



Ofrecimiento en Redes sociales



Contacto privado



Negociación

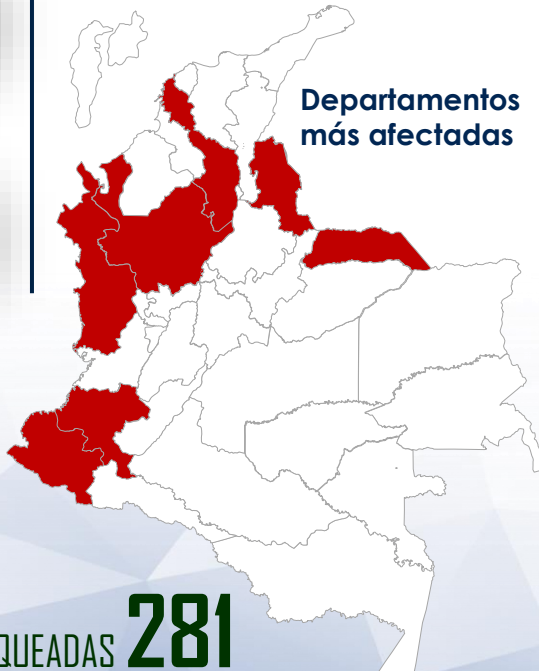


Entrega del estupefaciente

Páginas bloqueadas **104**

GRUPOS ARMADOS ORGANIZADOS

Con relación a grupos armados organizados y residuales, se identificaron y bloquearon un total de **281** cuentas y portales, alusivas a Grupos Armados Organizados (GAO) y grupos radicales, usadas con el fin de generar temor en la población mediante la difusión de panfletos amenazantes, comunicados a la opinión pública y atribución de atentados o ataques, como también buscar adeptos a sus ideologías.



Facebook **125**
 Ivoox **15**
 Telegram **10**
 Otras **13**

Sitios o Redes Sociales con mayor interacción

FRAUDE A TRAVÉS DE MEDIOS ELECTRÓNICOS



Los ciberdelincuentes implementaron nuevos métodos para la captura y hurto de información personal, que posteriormente usaron para llevar a cabo la suplantación de identidad, fortaleciendo la capacidad de ganar la confianza de personas incautas y materializar estafas.

PRINCIPALES MODALIDADES DE FRAUDE

La migración de actividades cotidianas al entorno digital, permitió que los cibercriminales se aprovecharan de las vulnerabilidades y la falta de conocimiento de las personas, empleando métodos y engaños con el objetivo de inducir a las personas al error y así robar la información personal o buscar fines lucrativos para sí o un tercero.

ESTAFA TURÍSTICA

Modalidad bastante común, en donde las principales fechas de acción de estos delincuentes es la temporada vacacional, es decir, días en los cuales las personas salen a vacaciones y el estafador obtiene un provecho económico ilícito a costas de las personas que inocentemente se fían de falsas propuestas que se ven en la web.

FALSA OFERTA LABORAL



El ciberdelincuente publica todo tipo de ofertas de empleo en plataformas digitales, suplantando la identidad de compañías reconocidas o firmas especializadas en reclutamiento de personal.

SOLICITUD DE PRESTAMOS

Por medio de la suplantación de una persona, solicitan préstamos de dinero a los allegados de la víctima, supuestamente para solucionar calamidades familiares, prometiendo devolverlo en un tiempo no mayor a 48 horas.

Normalmente, utilizan aplicaciones de mensajería instantánea y configuran los números telefónicos para desviar llamadas o mensajes entrantes, para que la víctima no tenga más medios para tomar contacto con el cibercriminal.

ESTAFA ONLINE



SMISHING



PHISHING



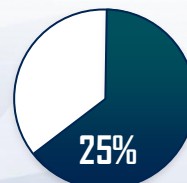
VISHING



ESTADÍSTICA

ART: 246 ESTAFA

El que obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños.



2020

52.863
Denuncias



2021

66.215
Denuncias

Balance Operacional



En el 2021 se realizaron **293** capturas, de las cuales **242** fueron por los delitos contemplados en la Ley 1273 de 2009 y **51** por explotación sexual infantil en Internet.

Resultados CECIP

12 Operaciones

21 Capturas

04 Escritos de acusación

OPERACIONES ESCIB

2020 32

2021 56



Se generó el intercambio de **520 comunicaciones** entre el Centro Cibernético Policial y la Oficina Europea de Policías.

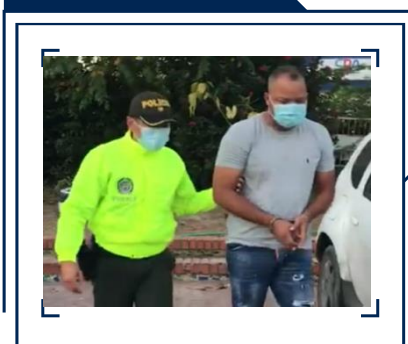


Con la Organización Internacional de Policía Criminal, se ejecutaron **02 procesos investigativos**, se realizaron seminarios y cursos con el Centro de Innovación de INTERPOL, **cruce de información con las 17 bases de datos** y la recepción de nuevas modalidades delictivas por parte de los 194 países miembros.

Operaciones de Impacto !

OPERACIÓN BLUENET BEC

A través de maniobras engañosas de BEC (Business E-mail Compromise) la líder de la organización logró suplantar a los representantes legales de 02 empresas, con el fin de aperturar el portal transaccional (banca virtual), canal por el cual, finalmente se realizarían las transferencias, materializándose el hurto por 1.900 millones de pesos.



RED OSCURA



Primera Operación a nivel nacional contra la DarkNet, capturando los responsables de la producción de más de 380 imágenes de abuso sexual infantil. Rescate de 01 niña quien era sometida a vejámenes por parte de sus progenitores.

OPERACIÓN BECKING

Modalidad de suplantación de correos empresariales (BEC), los cuales generaron fraudes financieros superiores a los 1.100 millones de pesos, la modalidad la realizaban a través de la compra de dominios de correos electrónicos enmascarados para generar la credibilidad en el engaño.





CENTRO CIBERNÉTICO POLICIAL



<https://caivirtual.policia.gov.co/>



@CaiVirtual



3202948647



(1) 5159727



Caivirtual

ANTE CUALQUIER SITUACIÓN CONTÁCTENOS EN: