Centro Cibernético Policial

Informe Cibercrimen 2020

SOMOS UNO.
SOMOS TODOS.

Las tecnologías de la información y las comunicaciones se han convertido en parte fundamental en la vida cotidiana de la ciudadanía, permitiendo con esto un aumento significativo en su utilización en el transcurrir de los años. De igual forma, los ciberdelincuentes han aprovechado esto como una brecha de vulnerabilidad para migrar de lo físico a lo digital y de esta manera realizar un actuar delincuencial polimórfico con el fin de obtener beneficios para sí mismos. Motivo por el cual ha sido necesario analizar y entender los diferentes fenómenos criminales que utilizan las redes de la información y las comunicaciones de manera prospectiva, aplicando herramientas de hiperconvergencia y Big Data, lo que permite optimizar los procesos administrativos y operativos que adelanta la Policía de Colombia en entornos nacionales e internaciones.

CENTRO CIBERNÉTICO POLICIAL

BALANCE **CIBERCRIMEN**

En Colombia se evidenció un incremento en los delitos cibernéticos de un **89%** respecto al año anterior. El delito que registró el mayor número de denuncias fue el "**Hurto por medios informáticos"** con **16.654** casos, sin embargo, es importante destacar que por motivo de la pandemia del COVID-19, los delitos de mayor incremento fueron: **suplantación de sitios web**, **violación de datos personales** y **interceptación de datos informáticos** .

Ley 1273
09 delitos

PERIODO 2020				PERIODO COVID-19 25 de marzo/31 de dic.		
Variación	2019	2020		2019	2020	Variación
37%	12.114	16.654	Hurto por medios informáticos y semejantes	9.593	13.529	41%
174%	3.457	9.487	Violación de datos personales	2.646	8.218	211%
89%	3.689	6.985	Acceso abusivo a un sistema informático	2.814	5.841	108%
303%	1.350	5.440	Suplantación de sitios web	1.126	4.429	305%
86%	1.806	3.355	Transferencia no consentida de activos	1.371	2.757	96%
192%	545	1.594	Interceptación de datos informáticos	429	1.332	210%
31%	503	661	Uso de software malicioso	367	542	48%
105%	307	629	Daño informático	237	284	120%
119%	136	289	Obstaculización ilegitima de sistema informático o red de telecomunicación	101	255	152%
+89%	23.907	45.104	TOTAL	18.717	37.550	+101%

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 **14.072** incidentes, siendo el sector de mayor afectación el **FINANCIERO** ***(87,3%)***, seguido del sector de **MEDIOS DE COMUNICACIÓN** ***(66.3%)*** y **GOBIERNO** ***(38%)***. Por otra parte, presentó disminución el sector **CUIDADANO** ***(-29%)*** y el **TECNOLÓGICO** ***(-0.5%)***.

FINANCIERO

2019 1,076
2020 2,016
+87.3%

GOBIERNO

2019 462
2020 639
+38%

MEDIOS DE COMUNICACIÓN

2019 425
2020 707
+66.3%

CIUDADANO

2019 11,612
2020 8,239
-29%

TECNOLOGÍA

2019 701
2020 697
-0,5%

PREVENCIÓN

Instagram
Seguidores: 2.990

Twitter
Seguidores: 54.163

Facebook
Seguidores: 14.547

ALERTAS PREVENTIVAS

494 Contexto NATURAL

582 Periodo COVID-19

Modalidades

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

SUPLANTACIÓN DE IDENTIDAD

	2019	2020
+35.2%	1,585	2,144

PHISHING

	2019	2020
+6.3%	2,188	2,326

ESTAFA POR VENTA Y COMPRA DE PRODUCTOS ONLINE

	2019	2020
+4%	2,691	2,800

VISHING

	2019	2020
-30.3%	1,688	1,176

MALWARE

	2019	2020
-50%	2,288	1,141

SE LOGRARON IDENTIFICAR **162** NOTICIAS FALSAS DURANTE LA PANDEMIA

OBSERVATORIO DEL CIBERCRIMEN

- EXPLOTACIÓN **SEXUAL INFANTIL EN LÍNEA**
- **ALTA TECNOLOGÍA**
- **SEGURIDAD CIUDADANA**
- **FRAUDE**

EXPLOTACIÓN 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.

MODALIDADES

7.139 URL´S BLOQUEADAS EN **2020**
4.163 URL´S BLOQUEADAS EN **2019**

GROOMING

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

Fueron reportados al CAI Virtual **225** incidentes.

SEXTORSIÓN

Chantaje realizado de forma virtual, a quienes han enviado fotos o videos eróticos, con la finalidad de obtener dinero, solicitar encuentros sexuales u obtener mayor contenido sexual.

Fueron reportados al CAI Virtual **637** incidentes.

CIBERBULLYING

Situación en donde un niño o adolescente es molestado, amenazado, acosado, humillado o avergonzado, a través de Internet u otros medios tecnológicos.

Fueron reportados al CAI Virtual **50** incidentes.

Top 5 de países consumidores de Material de Explotación Sexual Infantil

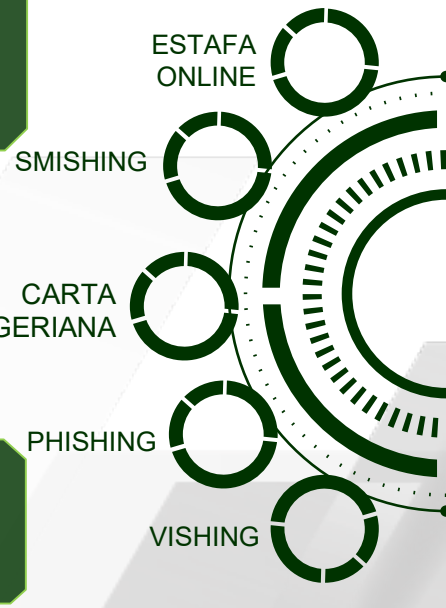
Fuente: Te Protejo ONG

FRAUDE A TRAVÉS **DE MEDIOS ELECRÓNICOS**

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.



FALSA ENCOMIENDA

Mediante ingeniería social el cibercriminal identifica una persona que se encuentra en el exterior, la cual será suplantada por medio de redes sociales y escribe a sus allegados solicitando recibir una encomienda que enviará al país. Posteriormente, se hace pasar por un funcionario de aduanas, manifestando que la encomienda se encuentra retenida y exige un pago.

VENTA DE DÓLARES

A raíz de la suplantación de una persona por medio de redes sociales y aplicaciones de mensajería instantánea, buscan ofrecer divisas extranjeras a muy bajo precio a los allegados de la víctima, con el fin de estafarlos.

SOLICITUD DE PRESTAMOS

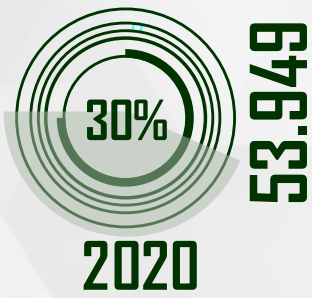
Por medio de la suplantación de una persona, solicitan préstamos de dinero a los allegados de la víctima, supuestamente para solucionar calamidades familiares, prometiendo devolverlo en un tiempo no mayor a 48 horas.

Normalmente, utilizan aplicaciones de mensajería instantánea y configuran los números telefónicos para desviar llamadas o mensajes entrantes, de esta forma la víctima no tiene otros medios con los cuales tomaría contacto con el cibercriminal.

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.



ALTA **TECNOLOGÍA**

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

ACCESO ABUSIVO A SISTEMA INFORMÁTICO

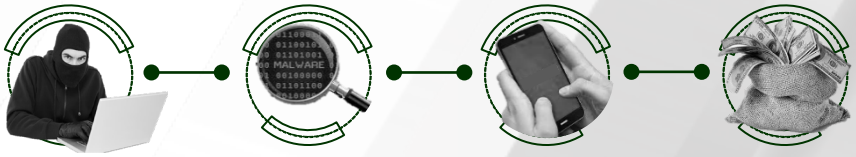
OBSTACULIZACIÓN ILEGÍTIMA

DAÑO INFORMÁTICO

PRINCIPALES **MODALIDADES**

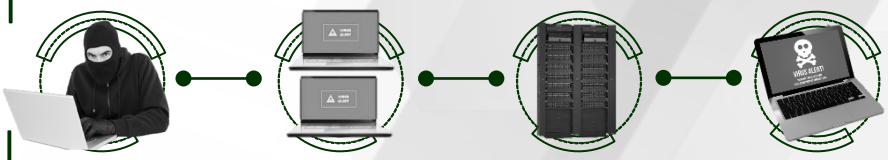
MALWARE

Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.



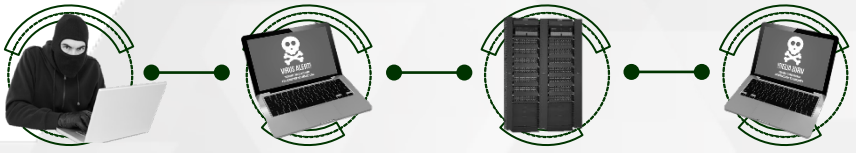
DDoS

Ataque distribuido de denegación de servicio, se realiza utilizando múltiples puntos de ataque simultáneamente sobre un servidor para que deje de funcionar.



DEFACEMENT

Ataque sobre un servidor web, como consecuencia se cambia su apariencia. El cambio puede ser a beneficio del atacante o buscando generar propaganda.



SEGURIDAD **CIUDADANA**

Durante el año 2020, el Centro Cibernético Policial realizó actividades de ciberpatrullaje en diferentes fuentes abiertas de información, con el fin de identificar posibles delitos que afecten la seguridad ciudadana en internet.

Estadística de las Modalidades

TERRORISMO

2019	2020	
184	369	+101%

INJURIA

2019	2020	
13,303	7,794	-41%

CALUMNIA

2019	2020	
16,508	10.230	-38%

ESTUPEFACIENTES

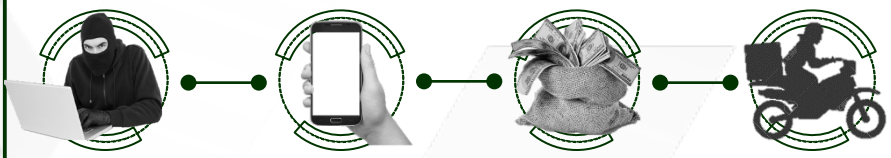
2019	2020	
66,208	43,724	-34%

AMENAZAS

2019	2020	
48,679	39,740	-18%

¡ DROGAS EN INTERNET !

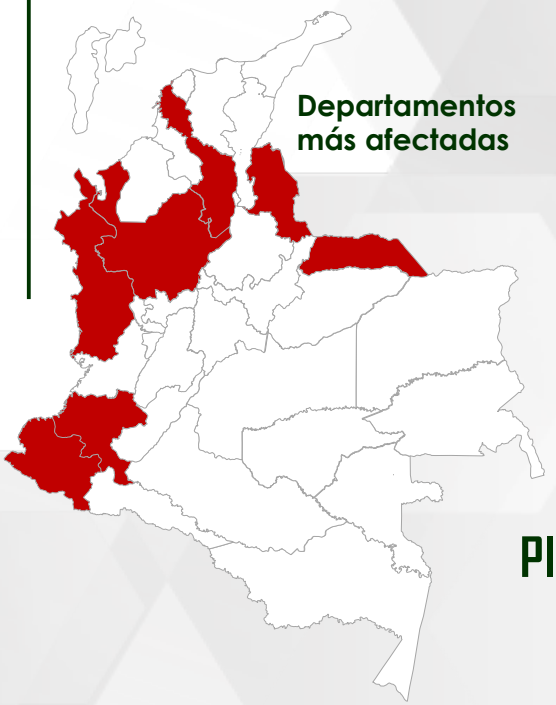
Modus Operandi

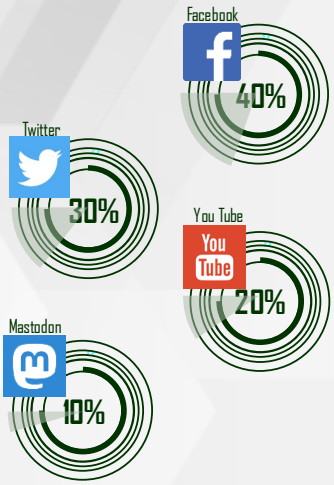


Ofrecimiento en Redes sociales — Contacto por RRSS — Transferencias Bancarias — Entrega a domicilio

GRUPOS ARMADOS ORGANIZADOS

Con relación a Grupos Armados Organizados, se identificaron un total de 58 cuentas y portales web, pertenecientes al Ejército de Liberación Nacional (ELN), Grupos Armados Organizados Residuales (estructuras de las extintas FARC-EP que no se acogieron al proceso de paz) y Clan del Golfo, 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 acciones terroristas, como también buscar adeptos a sus ideologías.





Plataformas virtuales con mayor interacción

GRUPOS ARMADOS

COOPERACIÓN **INTERNACIONAL**

Desde el 16/03/2020, el Consejo de Europa avaló el ingreso de Colombia al Convenio de Budapest, primer y único instrumento de cooperación internacional en materia de cibercrimen. Esto permitió desde el día 01/07/2020, la entrada en funcionamiento del Punto de Contacto (PoC) 24/7, del cual el Centro de Capacidades para la Ciberseguridad de Colombia (C4) se encuentra como responsable, estableciendo las siguientes funciones:

EUROPOL

Se generó el intercambio de **1.028** comunicaciones entre el Centro Cibernético Policial y la Oficina Europea de Policías, en las siguientes temáticas:

- Fraude informático.
- Material de abuso sexual infantil.
- Nuevas modalidades de malware y alta tecnología.

INTERPOL

Con la Organización Internacional de Policía Criminal, se realizó el intercambio de **56** comunicaciones, la apertura de **06** casos investigativos, realización de cursos en línea de la Academia Global, cruce de información con las **17** bases de datos y la recepción de nuevas modalidades delictivas por parte de los **194** países miembros.

INTERCAMBIO DE INFORMACIÓN JUDICIAL

SOLICITUD DE CONSERVACIÓN DE DATOS

ASISTENCIA TÉCNICA A LOS MIEMBROS DEL CONVENIO

Se recepcionaron **02** requerimientos en marco del **Convenio de Budapest** por parte de las autoridades de **Chipre** y **Chile**, a fin de apoyar procesos investigativos en dichos Estados.

Balance Operacional

En el 2020 la Estrategia Integral de Ciberseguridad, logró la desarticulación de **14 organizaciones** delictivas y la captura de **219 actores criminales**, así mismo, la ejecución de **32 operaciones** priorizadas, de las cuales **16** fueron desplegadas por el Centro Cibernético Policial.

Resultados CECIP

16 Operaciones

6 Operaciones internacionales

- Los Moldavos (Fraude Bancario)
- Operación nacional (Material de abuso sexual infantil - **MASI**)
- Intervención nacional (**MASI**)
- La depredadora (**MASI**)
- Endurence (portales fraudulentos)
- IOS (cibercontrabando)

28 Capturas

10 Escritos de acusación

164 Procesos investigativos

710 OPJ ejecutadas

Operaciones ESCIB

2019	2020	
23	32	+39%

Operaciones CECIP

2019	2020	
12	16	+33%

Organizaciones desarticuladas

2019	2020	
7	14	+100%

¡ Operaciones de Impacto !

Los Moldavos

Desarticulación de una organización internacional, dedicada a la clonación de productos bancarios, donde se capturó a **02 ciudadanos Rumanos**, catalogados como unos de los cibercriminales más buscados a nivel mundial.

La Depredadora

Operación trasnacional en articulación con la Agencia Europea de Policía – EUROPOL, logrando la Captura de alias “la Depredadora”, quien distribuía material de explotación sexual infantil de sus hijas menores de 14 años, a nivel mundial.

Hijackers

Desarticulación de una organización criminal (03 capturas), que secuestraba portales web de empresas nacionales e internacionales, aprovechando el incremento tecnológico a razón de la pandemia COVID 19.

Dollar´s Scam

Desarticulación de una organización criminal asociada a la nueva modalidad cibercriminal de suplantación de WhatsApp, en la cual se logró la captura de cuatro (04) personas.

Centro Cibernético Policial

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

@CaiVirtual

3202948647

(1) 5159727

CaiVirtual

ANTE CUALQUIER SITUACIÓN CONTÁCTENOS EN: