Informe:

Balance **Cibercrimen** en Colombia **2017**

CENTRO CIBERNÉTICO POLICIAL

@caivirtual

caivirtual.policia.gov.co

CENTRO CIBERNÉTICO POLICIAL

Tendencias del CIBERCRIMEN

INTRODUCCIÓN

En 2017 el cibercrimen reportó un incremento del 28.30% respecto al año anterior, consolidándose como uno de los principales retos en materia de lucha contra la criminalidad en el mundo; el modelo de crimen como servicio permitió que actividades ilícitas mutaran del escenario físico al virtual, diversificando el mercado de productos asociados al mismo.

La venta de datos personales, la oferta inusitada de malware, la comercialización de productos ilegales como armas, estupefacientes, bienes hurtados, documentos fraudulentos, entre otros, se han visto favorecidos por el afianzamiento de las criptomonedas como medio de pago predilecto para el crimen, aunado al anonimato que ofrece la Internet profunda y las rentas criminales derivadas del auge de estas conductas.

> **"Ciberataques sofisticados de afectación global impactaron infraestructuras digitales criticas en el mundo, en Colombia 446 empresas reportaron haber sido victimas.**

En el mismo sentido, el auge de las redes sociales y el uso a edad cada vez más temprana de dispositivos digitales por parte de los colombianos, facilitó el crecimiento de incidentes reportados por Gromming y Sextortion en el presente año.

NUEVAS AMENAZAS 2017

A través del ciberpatrullaje 24/7 y los reportes de los ciudadanos y sectores afectados al @caivirtual, fueron identificadas nuevas modalidades delictivas asociadas al cibercrimen, entre las que se destacan las siguientes amenazas como principales agentes desestabilizadores en el uso legal y confiable de la web:

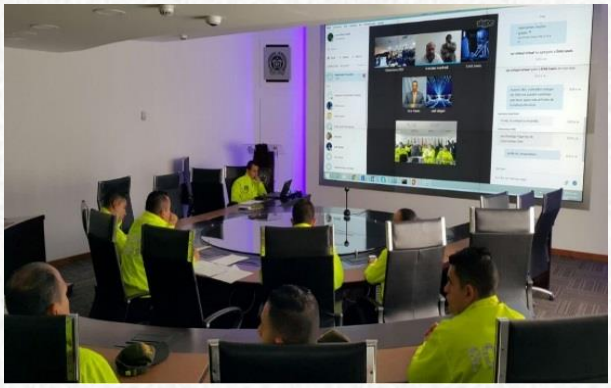
1. Ciberinducción al daño físico.

La integración digital a nivel mundial de niños, niñas y adolescentes en la web, trajo consigo un modelamiento de interacción a base de retos con fines de auto lesión. Esta acción criminal en contra de la vida y la integridad de los mismos, obligó una acción oportuna con el propósito de minimizar el impacto negativo en el uso de redes sociales; de esta actividad se destaca: **508** alertas generadas, **77.390** cuentas impactadas, **2.987** interacciones publicadas en redes sociales, **6.498.746** usuarios impactados, **83** apariciones en medios (44 publicaciones en Internet, 10 emisiones en radio, 10 publicaciones en medios impresos de comunicación, 19 emisiones en televisión), **12** casos con conexidad delictiva, **15** grupos identificados a

CENTRO CIBERNÉTICO POLICIAL

Tendencias del CIBERCRIMEN

nivel mundial en la red Facebook (ballena azul, reto del hada de fuego), **3** grupos eliminados en Colombia (Facebook), **4.123** usuarios que se les impidió acceso a estos grupos, **1** alerta mundial INTERPOL (circular morada), **coordinación** con Chile, México y Rusia, e **identificación** de perfiles provenientes de México, Argentina y Perú.



2. Estafa por suplantación de sim card.

Modalidad en la que el criminal aprovechando que el titular de un abonado telefónico se encuentra de viaje o no puede atender llamadas, se presenta en oficinas de empresas de operadores de telefonía móvil para obtener una sim card nueva a partir de la suplantación del titular.

Luego sincroniza redes sociales y productos financieros vinculados al número telefónico para validar accesos que le permiten generar transferencias no consentidas.

Por esta modalidad fueron reportados **1385** casos al @caivirtual, con perdidas que ascienden a los **$7.690.000.000,00**

3. Vishing – Tráfico de datos financieros personales.

Modalidad de estafa en la que los ciberdelincuentes aplican técnicas de ingeniería social vía telefónica, con el fin de tener acceso a información personal y financiera de sus víctimas para así lucrarse económicamente. Durante la vigencia se han recibido **1055** casos de vishing por cifras cercanas a los **$2.132.000.000,00**

CENTRO CIBERNÉTICO POLICIAL

Tendencias del CIBERCRIMEN

4. Fraude por falso WhatsApp.

La utilización de aplicaciones alojadas en las tiendas virtuales oficiales, son usadas para la creación de conversaciones falsas por parte de personas inescrupulosas que utilizan los datos públicos como la foto de perfil y el número de celular de las víctimas para simular chats y enviar pantallazos de las conversaciones para obtener información y cometer delitos vinculados a la afectación de la reputación de las personas, estafas, extorsión, entre otros.

381 casos han sido reportados al @caivirtual por víctimas principalmente Gerentes, a los cuales les han llegado falsas conversaciones entre los mismos con empleados de áreas financieras, donde se evidencia la intención de materializar estafas tipo BEC.

5. Ciberpirámides

Los delincuentes están aprovechando la incertidumbre que existe respecto a la legalidad y fluctuación de las criptomonedas, captando la atención de incautos inversionistas para hacer supuestas compras en monedas como el Bitcoin, Ripple o Ethereum, recaudando dineros para luego desaparecer estafando masivamente a los ciudadanos. La actividad investigativa en articulación con autoridades internacionales y la Fiscalía General de la Nación, logró identificar a dos de los presuntos responsables de una estafa en más de 10 países entre EE.UU y Latinoamérica, siendo el 77% de los reportes consolidados desde la parte investigativa originados desde Colombia. Las cifras del fraude reportan que hasta el momento las sumas son superiores a los **1.500** millones de pesos representados en **182** personas que en **11** ciudades informaron al @caivirtual una estafa por parte del portal web MECOIN.


Alerta por Bitcoin en Colombia
Economía 27 Mar 2014 - 8:32 AM
La Superintendencia Financiera emitió una circular en la que advierte de los riesgos de usar o transar en este tipo de monedas virtuales.

AMENAZAS PERSISTENTES 2017

1. Ransomware

WannaCry y Petya:

Entre el 12 y el 14 de mayo se registró un ataque cibernético a escala global bajo la modalidad de infección de malware conocido como Ransomware (Wannacry), el cual afectó infraestructura crítica de medios de transporte, hospitales, energía, gas, teléfono en más de 150 países. En Colombia este ataque impactó principalmente MIPYMES vinculadas al sector productivo del país.

Como parte de una respuesta integral para mitigar el impacto del secuestro de data

CENTRO CIBERNÉTICO POLICIAL

Tendencias del
CIBERCRIMEN

se dio inicio a una mesa de crisis para la atención de víctimas, recepción y análisis de malware y difusión de alertas preventivas, obteniendo los siguientes resultados:

- 160 muestras analizadas de malware
- 59 alertas generadas
- 52 víctimas atendidas
- 619.520 usuarios impactados
- 8.4 millones de cuentas impactadas en Twitter
- 3 boletines preventivos
- Coordinación con 51 empresas, 5 universidades y 6 ISP (Proveedor de Servicios de Internet).

Posteriormente se conoció dentro de la esfera investigativa otro ataque de similares características bajo la denominación PETYA.

En los dos ataques registrados se realizó mesas de crisis conjunta con el EC3 de EUROPOL para el intercambio de información, análisis de malware y búsqueda de patrones de infección de equipos tecnológicos.

2. Ataque a entes gubernamentales

Las entidades gubernamentales fueron objeto de ataques informáticos a través de “puertas traseras” gracias a la infección de malware y la utilización de RAT (Remote Access Tool) para la ejecución de software malicioso que sirve para la transferencia ilegal y no consentida de:

- Dinero
- Información del sector público
- Bases de datos

Las cifras de hurto por este delito ascienden a más de 50 mil millones de pesos solo en alcaldías a nivel nacional.


JUSTICIA | 11/8/2017 1:01:00 PM

El “regalito” de navidad que tiene sentado al alcalde de Albania en el banquillo de acusados

Aurelio Efraín Arregoces fue imputado por haber presuntamente tratado de desviar 22.000 millones de pesos del fondo de regalías a cuentas de cibermulas en el país. Su captura fue celebrada por el propio presidente Juan Manuel Santos.

El "regalito" de navidad que tiene sentado al alcalde de Albania en el banquillo de acusados *Foto: Archivo particular*

La DIJIN adelanta 15 procesos investigativos con la Fiscalía del Eje Temático de Cibercrimen, donde se evidencia el ataque a alcaldías en diferentes zonas del país.

CENTRO CIBERNÉTICO POLICIAL

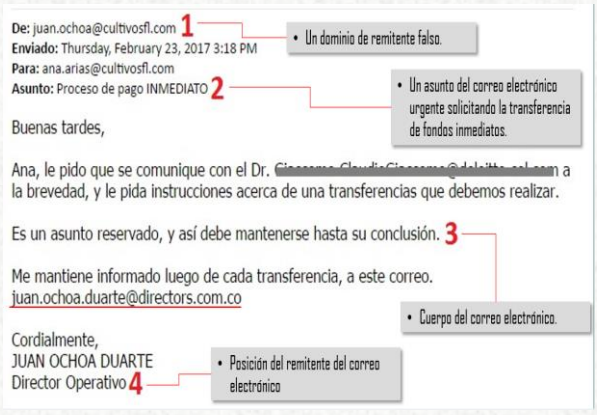
Tendencias del CIBERCRIMEN

3. BEC (Suplantación de correo corporativo):

Los ataques tipo BEC siguieron afectando a empresas del sector productivo y de retail en el país como la farmacéutica, petróleos, tecnología, transporte, comercio, entre otras.

Se estima que por cada caso de BEC que afecte en Colombia, existe una pérdida de **380** millones de pesos.

La suplantación de correo tiene dentro de sus principales objetivos a Gerentes y/o Jefes de Áreas Financieras, Ventas, Comercio, Exportaciones, Importaciones, Tesorerías, Revisorías fiscales, Contabilidad, Bancos, así como Secretarías ejecutivas, logrando mediante engaño transferir importantes sumas de dinero



El FBI considera a las estafas tipo BEC como el fraude de los 3 billones de dólares a partir del impacto negativo en la empresa y comercio de los EEUU

4. Carding

Modalidad de fraude mediante la cual los ciberdelincuentes comercializan los datos de tarjetas de crédito y débito, cuentas bancarias e información financiera sustraída a las víctimas con fines fraudulentos. Esta modalidad ha generado pérdidas anuales por **60,000** millones de pesos**.**

Los principales vectores de ataque están asociados a modalidades como: Skimming (clonación de tarjetas), intercambio de tarjetas (cambiazo), ataques en ATM, compromisos de reservas, Phishing (suplantación de sitios web para capturar datos personales) y falsos Call Center (Vishing).

En el @caivirtual se han recibido **328** incidentes por carding, destacando la afectación de tarjetahabientes en zonas de interacción como las hoteleras, comercio, turismo, pago de servicios públicos, etc.

CENTRO CIBERNÉTICO POLICIAL

5. Estafas por internet

El **55.3%** de los incidentes atendidos a través de @CaiVirtual fueron estafas en Internet, constituyéndose como el delito con mayor afectación a los colombianos. Dentro de las modalidades con mayor impacto se destacan: Compra y venta de productos en Internet, Vishing (estafas a través de llamadas telefónicas), Smishing (estafas a través de mensajes de texto SMS o chats en Whatsapp), Cartas Nigerianas (promesas de herencias o recompensas a través de correos electrónicos) y Paquetes turísticos (engaños en el alquiler de sitios de esparcimiento, generalmente en temporada de vacaciones).

Por otra parte **6372** ciudadanos han reportado este tipo de defraudaciones.

- El **60%** de las estafas corresponden al fraude por compra o venta de productos en internet: 3846 reportes
- El **16%** representan estafas por llamadas telefónicas (Vishing): 1055 reportes
- El **13%** corresponde a engaños a través de mensajes de texto o chats (Smishing): 856 reportes.
- El **8%** de las estafas están asociadas a Cartas Nigerianas: 502 reportes.
- El **2%** representan ofertas fraudulentas de arrendamientos de fincas de descanso por internet (paquetes turísticos): 113 reportes .

De igual forma, el promedio de una estafa en internet oscila entre **500.000** pesos y **20** millones de pesos, siendo así que a la fecha asciende a 15 mil millones de pesos la cuantía de las estafas en la presente vigencia.

Precisamente, la estrategia de Ciberseguridad comprende el trabajo articulado con autoridades administrativas, ASOBANCARIA, INCOCREDITO, principales pasarelas de pago y la Cámara Colombiana de Comercio Electrónico CCCE, para promover actividades de prevención e investigación.

VENTAS ILÍCITAS EN INTERNET

Durante el presente año se detectó un incremento en el número de expendios de drogas ilícitas a través de las redes sociales, este fenómeno que se ha conocido como ciberexpendios ha permitido a los delincuentes migrar el microtráfico hacia la virtualidad.

Mediante ciberpatrullaje adelantado por el @caivirtual fueron detectados al menos **55** mercados ilegales, destacando 21 grupos con

CENTRO CIBERNÉTICO POLICIAL

NARCOMENUDEO EN LA WEB

amplia interacción con usuarios (consumidores); el top **5** de las ciudades con mayor afectación por el creciente fenómeno de comercio ilegal son Bogotá, Medellín, Cali, Bucaramanga y Villavicencio.

> **Dentro de los productos que más ofertan están el Popper desde $25.000, LSD desde $30.000 y cannabis desde $15.000**

El servicio de Investigación Criminal ha afectado este tipo de ventas ilícitas mediante la realización de **5** operaciones que consolidan **47** capturas, siendo significativo haber puesto al descubierto el modo de transporte (utilizando NNyA), la comercialización a través del ocultamiento en comida como (brownies, pan, tortas, entre otros) y su venta con la utilización de nombres particulares a partir de la jerga popular de cada región del país como por ejemplo (cilantro para el cannabis).

Este tipo de economía criminal soportada mediante la utilización de las tecnologías de la información y las comunicaciones y redes sociales, tiene como fin la búsqueda de nuevos "clientes" entre los que se destacan principalmente la población estudiantil, pandillas y/o tribus urbanas.

De igual forma, los procesos investigativos advierten la conexidad delictiva con otras formas de actos ilegales tales como:

- Venta de licor adulterado
- Venta de armas
- Fiestas sexuales

Cae banda que vendía tortas y brownies con marihuana

Un total de 16 personas, señalados de pertenecer a la red criminal, fueron capturadas por las autoridades en 12 allanamientos realizados en varios puntos de la ciudad.

Las autoridades incautaron tres vehículos en los que se presume repartían el estupefacientes. Los clientes contactaban a 'Los S.S.' por páginas de Facebook y otras redes sociales. (Foto: Suministrada / VANGUARDIA LIBERAL)

RESULTADOS OPERATIVOS 2017

A través de la coordinación interinstitucional con el sector publico y privado y las agencias de ley internacionales como EUROPOL, AMERIPOL e INTERPOL, se adelantaron iniciativas operativas de alcance internacional, entre ellas se destacan las operaciones contra la pornografía infantil y el Grooming como "TANTALIO" y "DRAKAR", en las cuales fuero capturadas **17** personas en varias ciudades del país.

En el mismo sentido fueron bloqueadas **3.891** sitios en internet, por estar inmersos en estas actividades ilícitas.

En el desarrollo de diferentes investigaciones coordinadas con la Fiscalía General de la Nación, fueron capturadas **310** personas por delitos cometidos en contra de la Ley 1273/09

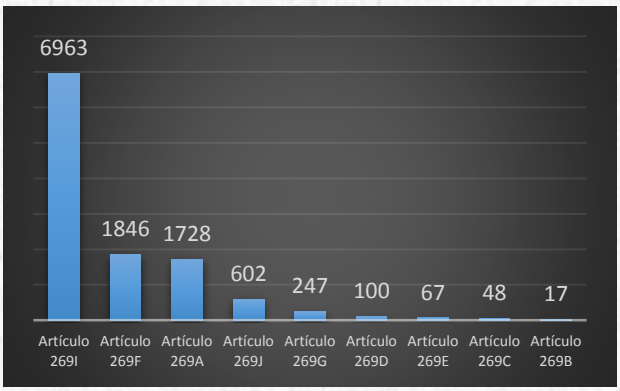
CENTRO CIBERNÉTICO POLICIAL

Tendencias del CIBERCRIMEN

generando una afectación directa a **30** organizaciones criminales.

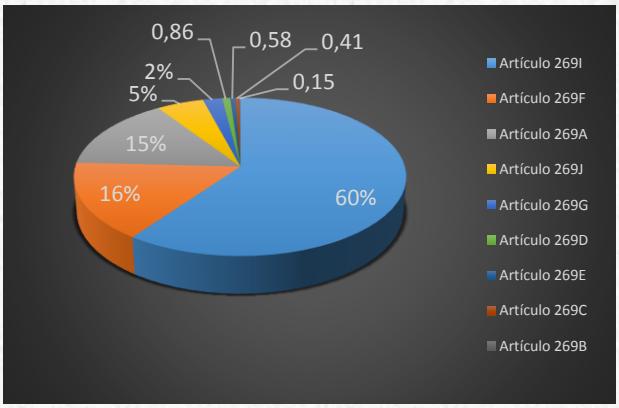
COMPARATIVO DELICTIVO

En la presente vigencia se han recibido 11.618 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país.



En cuanto a las tipologías criminales denunciadas ante la Policía Nacional en el citado periodo de tiempo, se evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades público - privadas, así como la integridad, disponibilidad y confidencialidad de la información que circula a través del ciberespacio.

Siendo el "Artículo 269I. Hurto por medios informáticos y semejantes" la tipología criminal de mayor frecuencia, equivalente al 60%, seguido del "Artículo 269F. Violación de datos personales" con 16% y "Artículo 269A. Acceso abusivo a un sistema informático" con



- Artículo 269A. Acceso abusivo a un sistema informático
- Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación
- Artículo 269C. Interceptación de datos informáticos
- Artículo 269D. Daño Informático
- Artículo 269E. Uso de software malicioso
- Artículo 269F. Violación de datos personales
- Artículo 269G. Suplantación de sitios web para capturar datos personales
- Artículo 269I. Hurto por medios

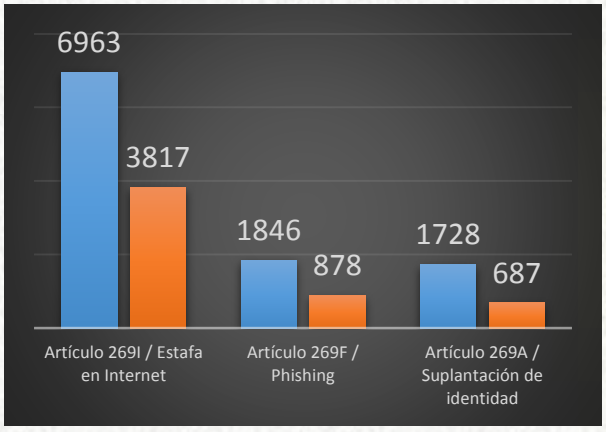
de activos

CENTRO CIBERNÉTICO POLICIAL

Tendencias del CIBERCRIMEN

> **"El crecimiento de denuncias es concordante con la masificación de medios tecnológicos para la interacción social, así como el acceso a la banca y el comercio".**

Reflejando con esto que las intenciones cibercriminales desde y hacia Colombia están ligadas principalmente a los campos comerciales y financieros, que cada vez se hacen más visibles en la cotidianidad de las personas y entidades, gracias a la masificación del uso de las tecnologías de la información y las comunicaciones a nivel nacional como se ha mencionado anteriormente, lo que proporciona una extensión de las capacidades humanas, por lo que la interacción hombre-máquina adquiere gran protagonismo, sin dejar de lado tres aspectos primordiales que soportan el e-comercio (confianza, sistemas de pago y seguridad).



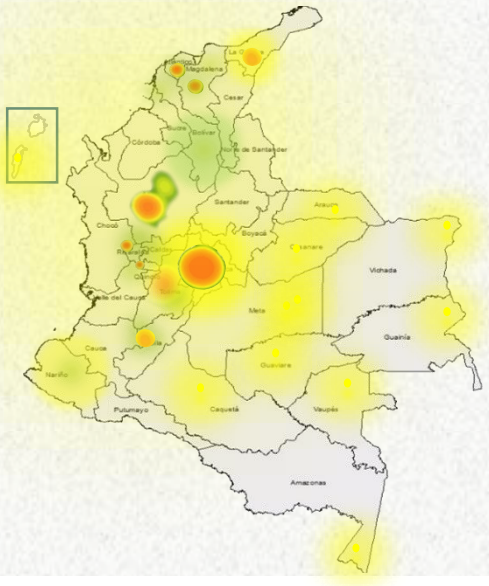
La anterior es una comparación de cifras de 3 modalidades de incidentes informáticos, con cifras de 3 delitos que se encuentran enmarcadas dentro de las conductas punibles tipificadas en Colombia, siendo concordante el crecimiento de la denuncia de la mano con la modalidad que más se identifica en su materialización.

Pornografía Infantil:

Durante el año 2017, el CAI Virtual atendió 280 incidentes asociados a la modalidad de GROOMING (la suplantación de un NNA - Niño, Niña y/ Adolescente en la red).

MAPA DE CALOR DEL CIBERDELITO

En Colombia, la panorámica del delito informático se ve reflejada en el siguiente mapa de calor, donde en las principales ciudades se encuentra más del **75%** de suscriptores de internet fijo y el mayor índice de habitantes por ciudad.



CENTRO CIBERNÉTICO POLICIAL

ASISTENCIA INTERNACIONAL

En materia de cooperación internacional, la Policía Nacional participó activamente el acompañamiento asesoría, transferencia de conocimiento y experiencias a través de mecanismos bilaterales entre los cuales se destacan:

Panamá	Uruguay
Honduras	España
El Salvador	Argentina
Guatemala	Jamaica
Rep. Dominicana	Portugal

Respecto a operaciones nacionales / internacionales como los días de acción conjunta - "*Joint Action Day*", la Policía Nacional participó en **10** iniciativas para combatir los fraudes por medios de pago en los principales aeropuertos de Europa y América.

Durante el año 2,017 se compartieron **171** boletines **SIENA** con el **EC3 de EUROPOL,** lo cual convierte a Colombia en un importante aliado para el intercambio de información con EUROPA en lo que respecta a investigación criminal.

Con los "*Joint Action Day*" se logró impactar en **834** reportes de fraude asociados a 691 personas, en **230** aeropuertos de **60** países. Esta actividad contó con la articulación de los países miembros de Europol y Ameripol, liderados por la Policía de Colombia en América Latina y el caribe.

Reuniones de planeación estratégica operativa como el JCAT de Europol, permitieron combatir los fraudes por medios de pago y amenazas de Cibercrimen en sus modalidades a través de la realización de **3** convenciones en las que participaron **14** países.

"Dentro de las operaciones internacionales se destacan TANTALIO contra la pornografía infantil con 6 capturas, SIN FRONTERAS con 3 capturas, E-COMMERCE con 2 capturas y CYBER SURGE con 1 captura".

CENTRO CIBERNÉTICO POLICIAL

CAMPAÑAS PREVENTIVAS

Con el fin de prevenir actividades ilícitas asociadas al comercio electrónico, el Centro Cibernético Policial realizó en compañía con INCOCRÉDITO, ASOBANCARIA y la Cámara Colombiana de Comercio Electrónico **857** alertas de Ciberseguridad orientadas a generar conciencia y evitar riesgos a la hora de realizar compras en el ciberespacio, ofreciendo recomendaciones al momento de realizar transacciones por medios de pago no presencial.

Con esta actividad se busca mitigar los riesgos de realizar transacciones electrónicas de manera insegura, así como crear conciencia a la hora de utilizar los medios tecnológicos para la interacción con la banca y el comercio.

El pilar de esta estrategia fue el lanzamiento del programa "**Por una red más segura**" a través de la campaña publicitaria de gran impacto **"tu correo por un carro".**

"En el marco del lanzamiento del programa por una red más segura se impactaron 668,000 ciberusuarios, a través de los canales de @caivirtual"

En este sentido se apoyaron actividades para generar confianza de los ciberciudadanos en el comercio electrónico tales como:

12 Cyberlunes / Black friday

25 Mesas de seguimiento de modalidades de cibercrimen enfocadas en fraudes por medios de pago

820 Alertas focalizadas de ciberseguridad desde @caivirtual