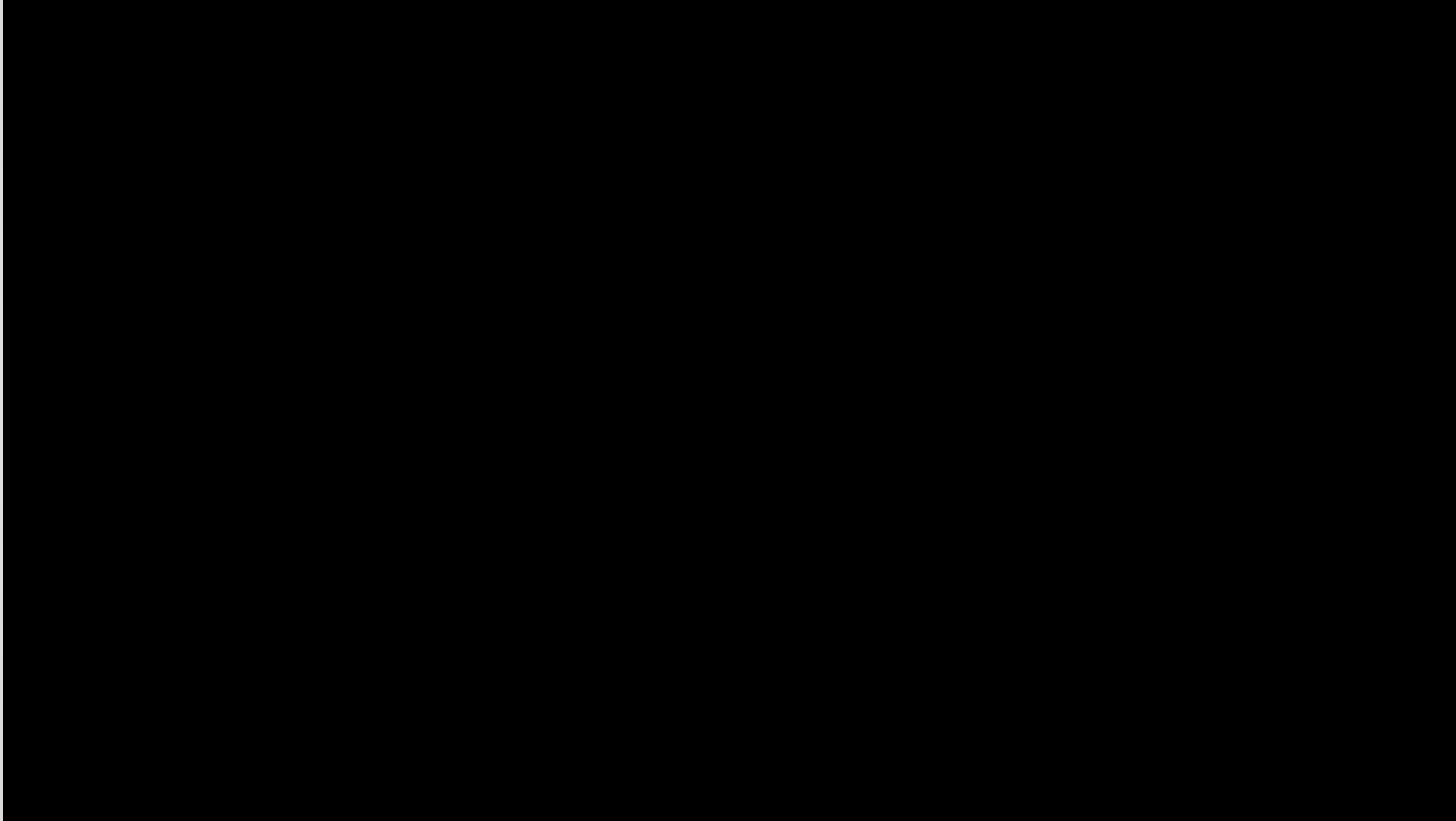


**METROPOLITANA DE PEREIRA
SECCIONAL DE INVESTIGACIÓN CRIMINAL**

CONTEXTO DEL CIBERCRIMEN EN PEREIRA

Subintendente **PETER VARGAS**
Investigador Cibercrimen
Ingeniero de Sistemas, CHFI,
Desarrollador Backend Python







ACTUALIZACIÓN CONSTANTE EN CIBERSEGURIDAD



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

@CaiVirtual



CAPACIDADES – ALCANCE INTERNACIONAL

Centro Regional para el Cibercrimen en las AMERICAS - Ameripol

Grupo de Trabajo Americano de delitos Tecnológicos de INTERPOL

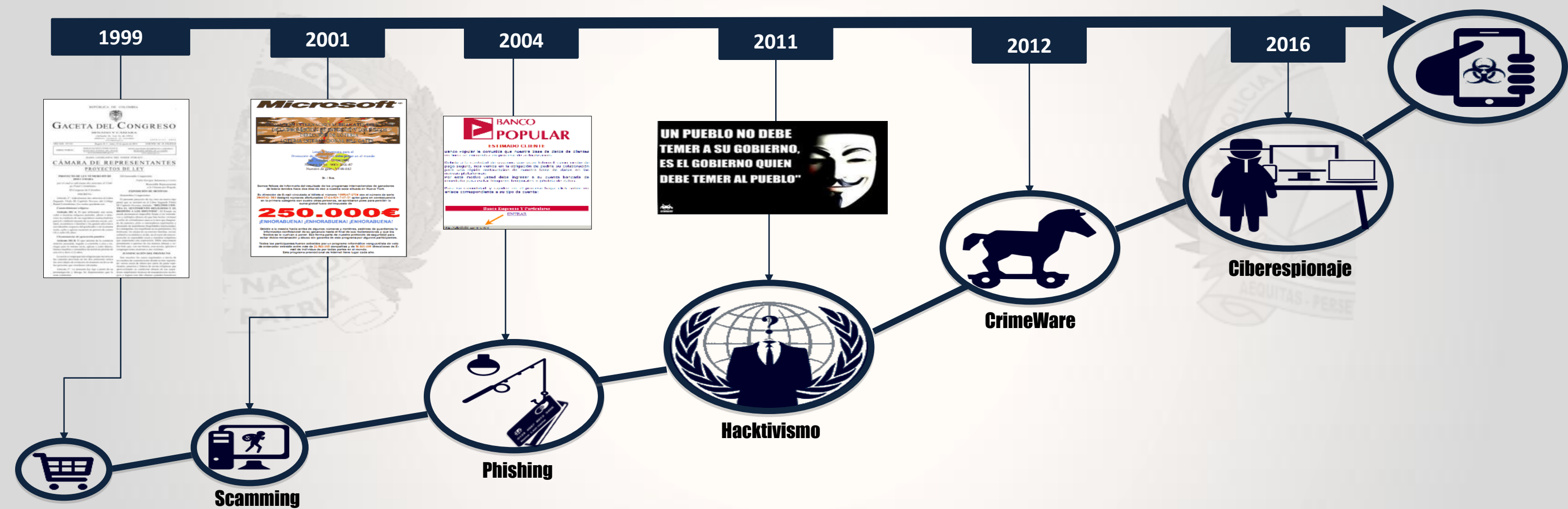
Ley 1582 de 2012 - Acuerdo de cooperación entre Colombia y la oficina Europea de Policía EUROPOL

Agencia Internacional de Cooperación Coreana





AMENAZAS – EVOLUCIÓN DEL DELITO





PHISHING



Apple Inc. [US] <https://www.icloud.com>

← → ↻ 🏠 www.itracking.me/icloud/location-id/L6hTrWcBimzFVj8ALj6mfBsbifRoD4miY36v/Nz6Fhj0KSj6mfBsbifRoD4miY36vj90Fh6wXzPkA017qW/ ☆ ☰

Aplicaciones Base de Datos - Pub... FOSYGA - Fondo de ... SUPERINTENDENCI... www.anm.gov.co/si... CMC - Catastro ... Policía Nacional de ... simit procuradoria Pipl - People Search »

ESTE ES EL LINK DE LA FALSA PAGINA DE ICLOUD



Iniciar sesión en iCloud

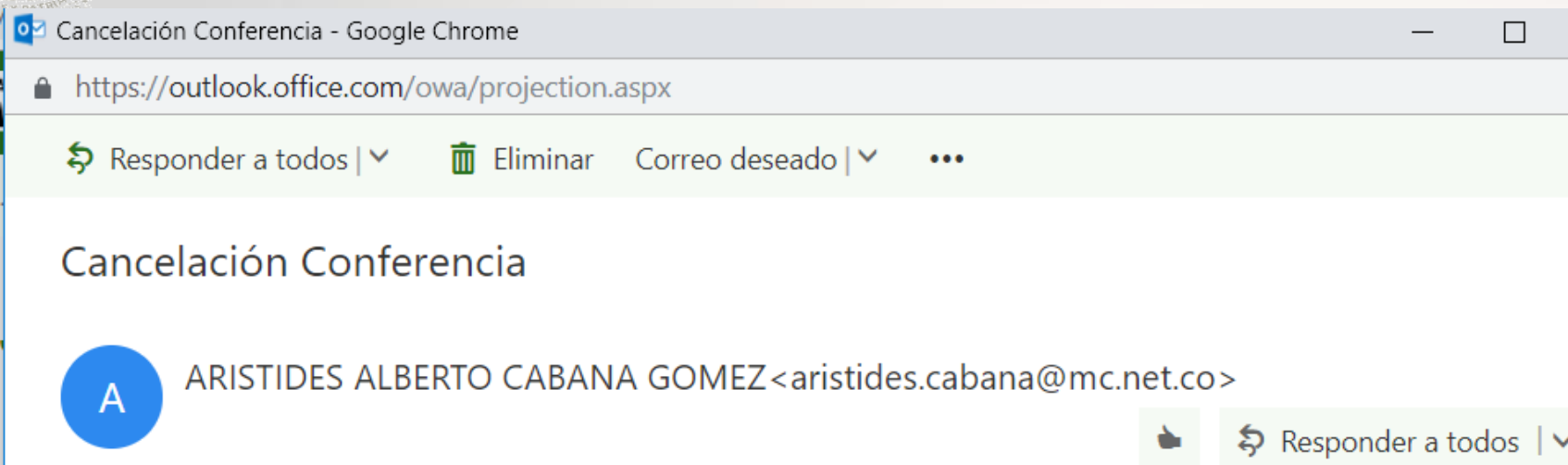
ID de Apple

Contraseña 

☐ Permanecer conectado



¿POR QUÉ ESTOY AQUÍ?



¿Por qué estoy aquí?

Buenos días Peter,

La presente tiene como fin en primera medida desearle éxitos en sus funciones y a la vez informarle que la conferencia programada para el día de hoy fue cancelada.

Atentamente;

ARISTIDES ALBERTO CABANA GOMEZ
Administrador de Red



EMAIL SPOOFING



EMKES'S MAILER

Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

✓ E-mail sent successfully

From Name: ARISTIDES ALBERTO CABANA GOMEZ

From E-mail: aristides.cabana@mc.net.co

To: peter.vargas4942@correo.policia.gov.co

Subject: Cancelación Conferencia

Attachment: No se eligió archivo

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text: Buenos días Peter,

La presente tiene como fin en primera medida desearle éxitos en sus funciones y a la vez informarle que la conferencia programada para el día de hoy fue cancelada.

Atentamente;

ARISTIDES ALBERTO CABANA GOMEZ
Administrador de Red

From Name: ARISTIDES ALBERTO CABANA GOMEZ

From E-mail: aristides.cabana@mc.net.co

To: peter.vargas4942@correo.policia.gov.co

Subject: Cancelación Conferencia

Attachment: No se eligió archivo

Content-Type: ☒ text/plain ☐ text/html ☐ Editor

Text: Buenos días Peter,

La presente tiene como fin en primera medida desearle éxitos en sus funciones y a la vez informarle que la conferencia programada para el día de hoy fue cancelada.

Atentamente;

ARISTIDES ALBERTO CABANA GOMEZ
Administrador de Red



MALWARE



Hola como estas espero te encuentres bien, el motivo de mi mensaje es para alertarte de lo que están preparando a tus espaldas gente que dice ser tu amigo solo por envidia quieren atentar contra tu vida, recién ayer estuve en una reunión el cual 2 personas mencionaron tu nombre y tu apellido, yo me sorprendí ya que pues un conocido mio me había hablado de ti y me hablo muy bien en resumen en mi consciencia no quiero cargar con un muerto, en el momento que ellos hablaban yo grabe la conversación con mi celular acá te la dejo para que la escuches :

<http://co.blackberry.com/notasdevozdate07052014>

----- Forwarded Message -----
From: carter a dian <administracioncartera@dian.com.co>
To: [REDACTED]
Sent: Saturday, August 15, 2015 2:33 PM
Subject: Cobro juridico - dian

DIAN

La presente es con el fin de informarle que su cuenta parara a cobro jurídico.

el siguiente enlace consta de lo correspondiente para ponerse al día con sus obligaciones

<https://drive.google.com/uc?authuser=0&id=0B2f4sRRXWgYNUVCR2h0Y203Mik&export=download>

Ultima actualización 03 de octubre de 2013 - [Políticas de privacidad y terminos de uso](#) | [Mapa del sitio](#) | Hora Legal Colomb
Sede principal: Bogotá, Nivel Central, carrera 8 #6 - 64 edificio San Agustín; PBX (57+1) 6069999; fax (57+1) 3347841

LooksLike.Win32.Malware/vb (v)
W32/Agent.QZ!tr
LooksLike.Win32.Malware/vb (v)

cobro juridico.exe cobro juridico.v

#Malware

To: a
Subject: Denuncia Penal - (-407656069)
From: aalcom
Date: Tue, 11 Aug 2015 21:37:24 -0300

FISCALIA GENERAL DE LA NACION

Radicado No. 2234122418845
Oficio No. 182 10-08-2015
Página 1 de 1
DFCM-GN
CITACION UNICA
BOGOTÁ D.C.

La FISCALIA GENERAL DE LA NACION y La doctora Martha Oliva Pineda Correa, en su condición de Fiscal ES Seccional Delegada ante los Jueces Penales del Circuito de la ciudad de Bogotá, Por medio del presente documento le informamos que la resolución de acusación en su contra ha sido determinada y en consecuencia solicitamos su asistencia en este despacho, sin falta, el día JUEVES, 22 DE SEPTIEMBRE DE 2015, A LAS 3:00PM, con el fin de rendir indagatoria por los cargos de hurto agravado en primera persona en el caso contra el señor PEDRO DEL CARMEN BEHAVIDES. SU ASISTENCIA ES OBLIGATORIA (recuerde llevar su documento de identidad).

Para ver mas información acerca su proceso y fecha de la citación visualice el siguiente archivo en línea:
<http://fiscalia.gov.co/procesos/bogota/2234122418845>

REP:
DENUNCIA PENAL
Hurto-HURTO AGRAVADO(Ley 599 del año 2000 artículos 239 a 243)
Ref: Citación diligencia de Descargos
11/08/2015 09:37:24

#Troyano

TR/Spy Banker Gen
Trojan Win32.Bankload.WEO
a variant of Win32/TrojanDownloader.Bankload.WEO
W32/Bankload.UK2!tr.dll
Trojan-Downloader (004c80361)
PE: Trojan.Win32.Generic.16F3122E!416583086

Visualiza_documento_penal.pdf Visualiza_documento_penal.exe

¿Qué sucede si instalo este "archivo"?

El Laboratorio de Informática Forense del Centro Cibernético Policial, analizó detalladamente este archivo, con el fin de identificar sus objetivos.

"¿Por qué el correo me lo envían desde cuentas oficiales?", no lo envían desde cuentas oficiales, utilizan la técnica llamada "Email Spoofing" o "suplantación de correo electrónico".

¿Qué hace este software malicioso?"

En el momento de ser ejecutado se duplican subprocesos legítimos del sistema operativo, para dificultar la detección por parte de los antivirus.

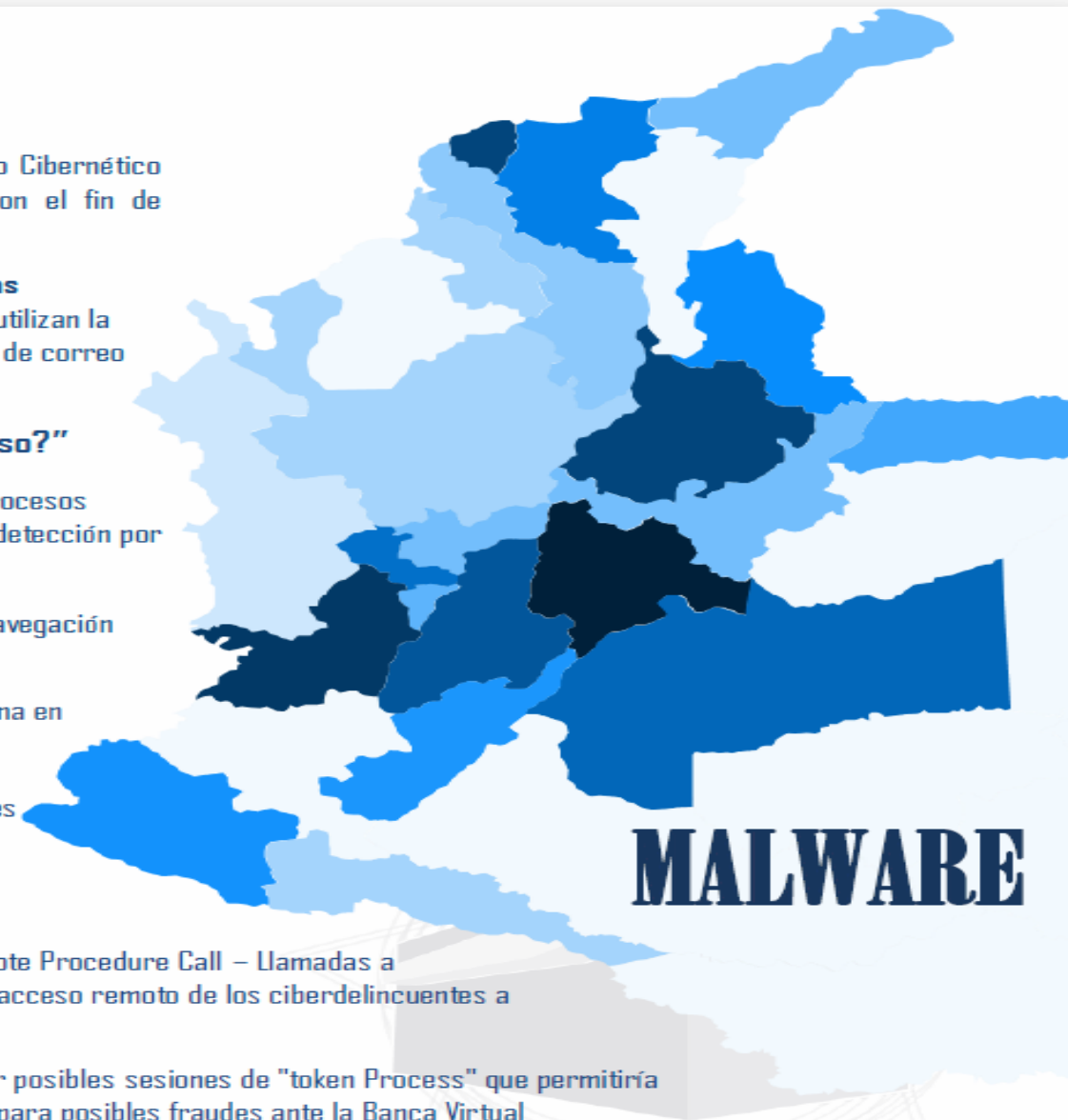
Captura las entradas por teclado y registros de navegación referentes a la banca virtual.

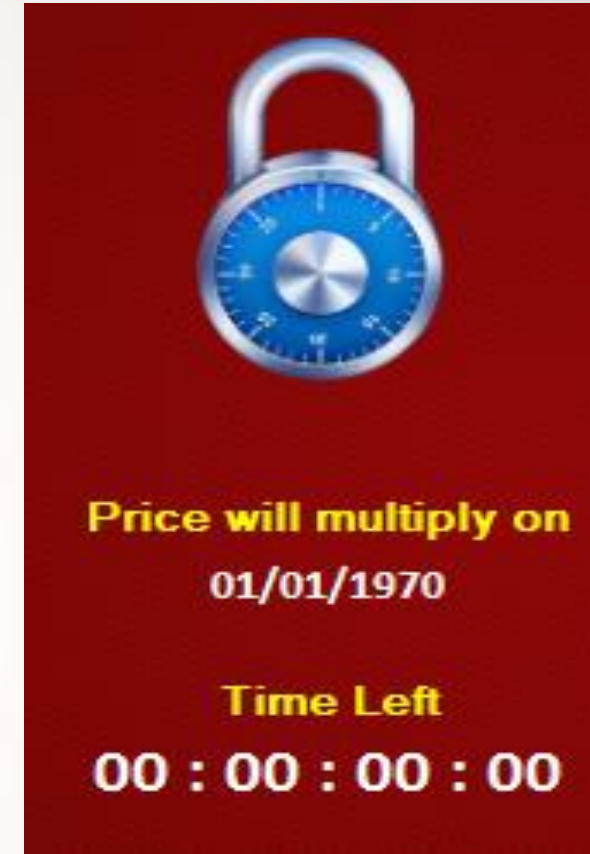
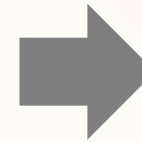
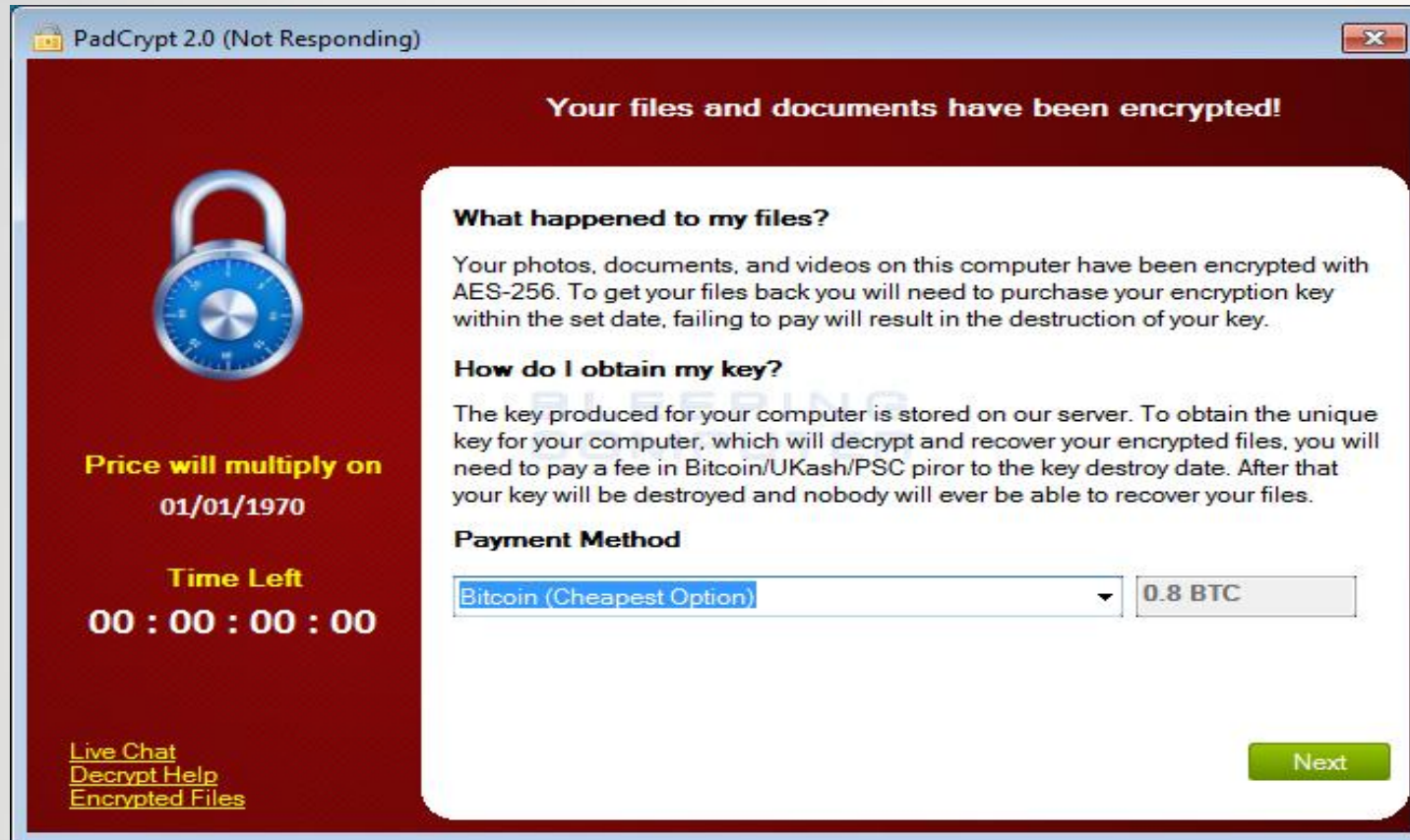
Crea un archivo llamado "server.exe" y lo almacena en la carpeta de las librerías del sistema operativo.

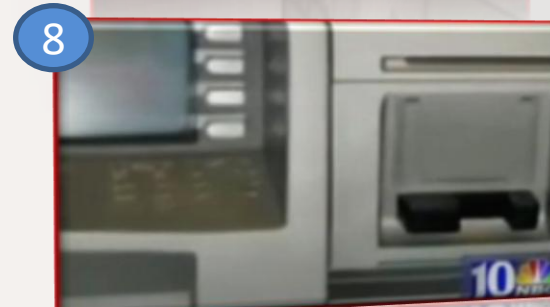
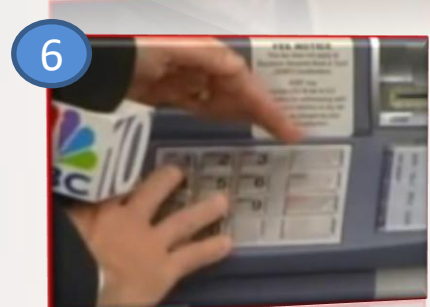
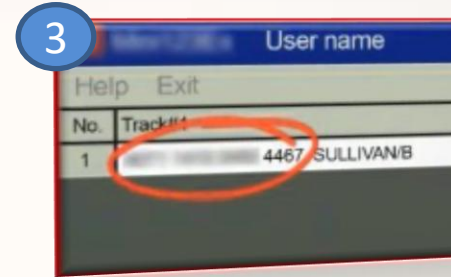
El archivo "server.exe" tiene varias funcionalidades una de ellas es el envío de la información recolectada a un servidor que está previamente configurado por el ciberdelincuente.

También realiza la apertura de puertos RPC (Remote Procedure Call – Llamadas a Procedimientos Remotos), los cuales permiten el acceso remoto de los ciberdelinquentes a nuestros equipos de cómputo.

Puede ser configurado para supervisar y capturar posibles sesiones de "token Process" que permitiría el acceso a información financiera o confidencial para posibles fraudes ante la Banca Virtual









METADATOS





OBTENIENDO EL RASTRO INFORMÁTICO

Basic Image Information

Target file: IMG_20181025_181210.jpg

Camera:	Huawei ALE-L23
Lens:	3.7 mm
Exposure:	Auto exposure, Program AE, $\frac{1}{14}$ sec, f/2, ISO 1550
Flash:	none
User Comment:	Hisilicon Balong
Date:	October 25, 2018 6:12:14PM (timezone not specified) (3 hours, 9 minutes, 49 seconds ago, assuming image timezone of 5 hours behind GMT)
Location:	Latitude/longitude: 4° 48' 20.6" North, 75° 43' 2.5" West (4.805735, -75.717351) Map via embedded coordinates at: Google , Yahoo , WikiMapia , OpenStreetMap , Bing (also see the Google Maps pane below) Altitude: 1,363 meters (4,472 feet) Timezone guess from earthtools.org: 5 hours behind GMT
File:	4,160 × 2,336 JPEG (9.7 megapixels) 2,361,650 bytes (2.3 megabytes)



<http://exif.regex.info/exif.cgi>



GRABIFY - <https://grabify.link>



GRABIFY

Create or Track URLs

- Facebook - Like our Facebook page for updates and changes! <https://www.facebook.com/Grabify>
- New Backend - We have recently remade the whole backend of Grabify. If you notice any bugs, please report them.

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

Create URL

Tracking Code

LINK INFORMATION:

Select Domain Name: [Click here](#)

(All custom links will stay active)

Original URL	https://caivirtual.policia.gov.co
New URL	https://grabify.link/NCZQVD Copy
Other Links	View Other link Shorteners
Tracking Code	4PEANV
Access Link	https://grabify.link/4PEANV

<https://grabify.link>



RESULTS: 1

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Hide Bots ☐

Date/Time	IP Address	Country ?	User Agent	Referring URL	Host Name	ISP
2018-10-26 15:30:42	190.9.195.133	Colombia, Medellin	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134	no referrer	Cable-Costavision190-9-195-133.une.net.co	EPM Telecomunicaciones S.A. E.S.P.

<https://grabify.link>



[@danielzarama](#) El criterio es "¿es famoso?-Si, ¿es "artista", político o periodista?-Si" entonces es un objetivo para nosotros.



DanielSamperO Sophie Germain

[@guitarradavid](#) En Colombia si, en otra nación creo que el FBI ya estaría tocando la puerta a menos que sea un Hacker ruso.

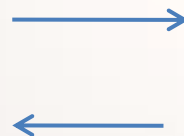
12 ago

Agosto 12



Víctima

Agosto 13



Agosto 14



Indiciado

Agosto 15





¿Por qué es necesaria una estación de informática forense en software libre para la Policía Nacional?

Prueba Piloto – Metropolitana de Pereira

- Colombia pionero en la implementación en software libre en la informática forense.
- Austeridad en el gasto.
- Apoyo Técnico – Científico a la Administración Justicia.

- Despliegue nacional de estaciones de informática forense.
- Aumento de las capacidades de atención de incidentes informáticos.
- Innovación en la atención e investigación del Cibercrimen.

**Innovación y
Optimización
de Indagación
Penal**

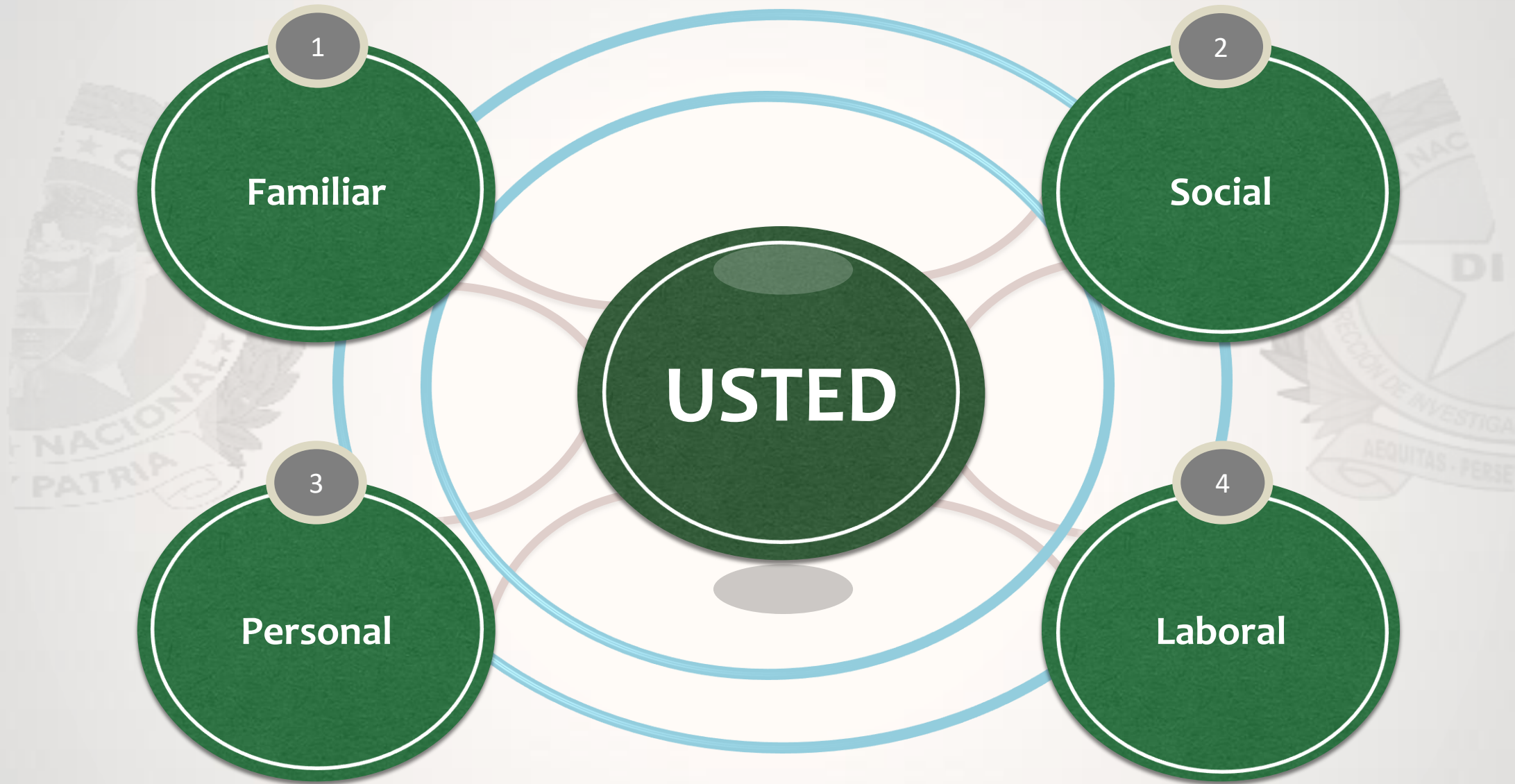
**80%
Reducción de
Costos**

**Nuevas
técnicas de
indagación**

**Análisis
Profundo de
Metadatos**

**Cloud
Computing**

**Monedas
Electrónicas**



**METROPOLITANA DE PEREIRA
SECCIONAL DE INVESTIGACIÓN CRIMINAL**

GRACIAS

Subintendente **PETER VARGAS**
Investigador de Cibercrimen
Ingeniero de Sistemas, CHFI,
Desarrollador Backend Python
(+57) 314 4785159

