



POLICÍA NACIONAL

ICANN 39 “Desafíos Cibernéticos en Colombia”.

Cartagena, 5 – 10 Diciembre 2010



1

Desafíos.

Los 10 +



Hurtos por Transferencias electrónicas (phishing, clonación, etc)



Ofertas de dinero fácil y rápido. Bolsas de empleo



Smishing Mensajes falsos vía SMS



Suplantación de identidad



Venta de bases de datos



Robo de datos, espionaje



Virus, Troyanos, malware



Hacking – saboteo



Delitos de contenido

(Cyberbullying – Grooming)



Organización Criminal



Codificadores / programadores.

Distribuidores.



Expertos en tecnología.



Los hackers.

Los estafadores.



Proveedores de sistemas hospedados.

Cajeros.



Mulas de dinero.



Contadores.



Líderes de la organización.

El Problema ?

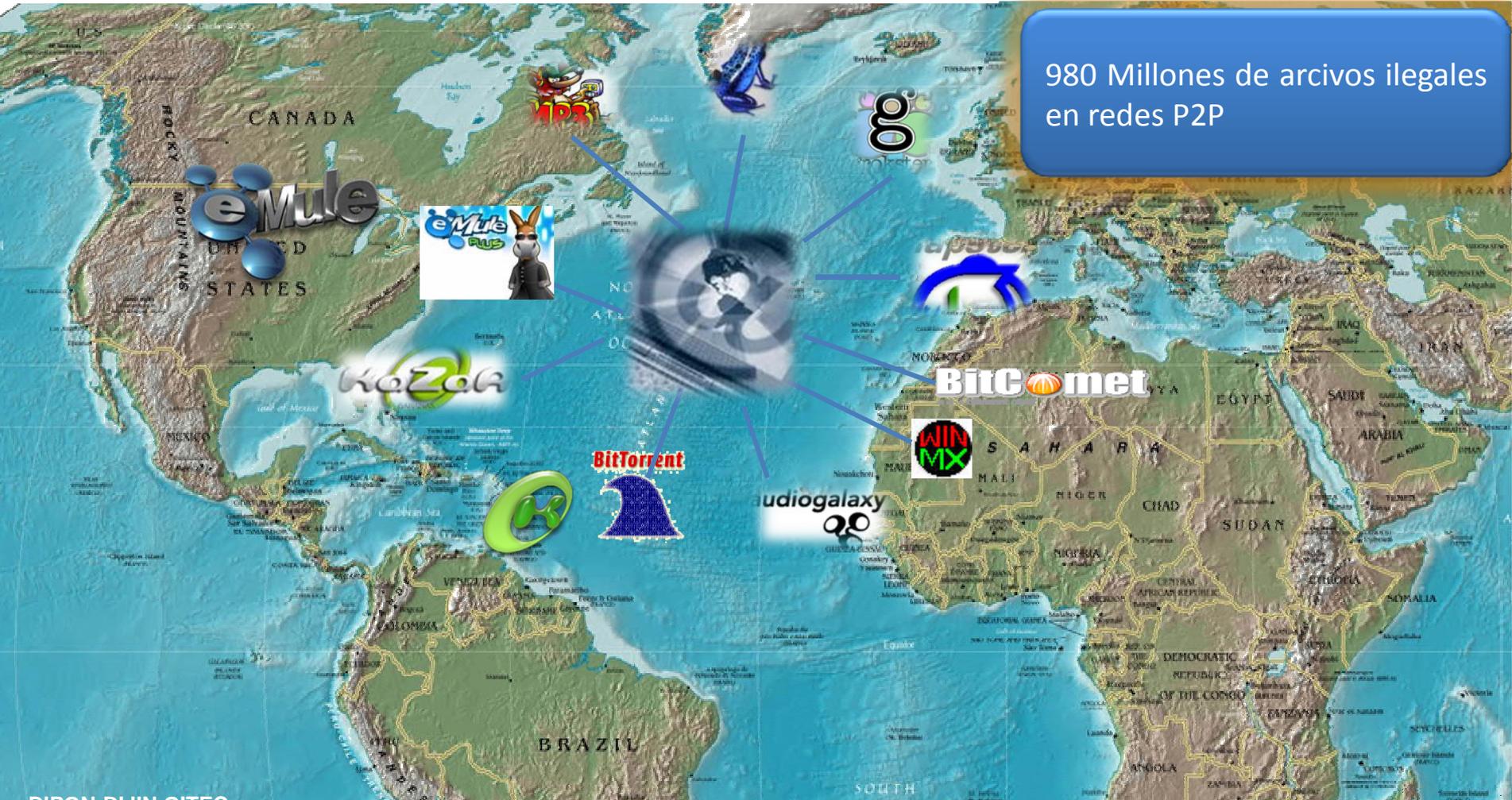


Uso de Internet como medio de información y búsqueda de contenidos ilegales

El Problema ?



980 Millones de archivos ilegales en redes P2P





2

Ataques DNS.



Voto 2010 – Colombia Elige

Fiscalía confirmó “cientos de ataques” que recibió Registraduría en elecciones

mayo 24 2010, 08:59

Search Web by Domain

Explore 1,208,002 web sites visited by users of the Netcraft Toolbar

7th December 2010

Search: [search tips](#)

site contains

example: site contains .netcraft.com

Results for registraduria.gov.co

Found 3 sites

Site	Site Report	First seen	Netblock	OS
1. www.registraduria.gov.co		december 1997	epm telecomunicaciones s.a. e.s.p.	freebsd
2. web.registraduria.gov.co		august 2010	epm telecomunicaciones s.a. e.s.p.	unknown
3. www3.registraduria.gov.co		december 2008	epm telecomunicaciones s.a. e.s.p.	freebsd

COPYRIGHT © NETCRAFT LTD 2010. ALL RIGHTS RESERVED.

Fiscal general dice que plataforma de la Registraduría fue atacada por hackers

[Todos los Hoteles Aquí](#)

Boutique, Apart, Hosteria, Posada, All Inclusive, Hostel, Spa y más
Despegar.com.co/Bogota



Abril 10, 2010 10:46 am

Anuncios Google



El Fiscal General de la Nación encargado, Guillermo Mendoza Diago dijo que las indagaciones sobre las demoras en los escrutinios de las pasadas elecciones parlamentarias, indican que hackers (piratas electrónicos) atacaron la plataforma tecnológica de la Registraduría Nacional.

El funcionario advirtió que las pesquisas arrojan entre las hipótesis que desde el interior del organo comicial hubo ayuda para el ataque informático.

Esta formulació se da con base en las investigaciones adelantadas por la firma Adalid Abogados que indican que individuos ajenos al grupo dce personas que tenían acceso ala plataforma de datos ingresaron a bases de datos que no eran públicas y en las que no había resultados, aunque sí información electoral.

El fiscal también explicó que al parecer, los hackers no solo buscaban que la página de la Registraduría se cayera, para sabotear el proceso informativo sino que amenazaron las bases de datos con los resultados electorales.

Es decir, intentaron un fraude electrónico que no se concretó “Tenían información pero no las ruta exactas y no pudieron meterse en las bases de datos”, dijo Andrés Guzmán, de Adalid.



Netcraft Services

→ [Netcraft News](#)

Phishing & Security

- [Anti-Phishing Toolbar](#)
- [Phishing Site Feed](#)
- [Hosting Phishing Alerts](#)
- [Bank Fraud Detection](#)
- [Phishing Site Countermeasures](#)
- [Audited by Netcraft](#)
- [Open Redirect Detection](#)
- [Web Application Security Testing](#)
- [Web Application Security Course](#)

Internet Data Mining

- [Million Busiest Websites](#)
- [Hosting Provider Switching Analysis](#)

Search Web by Domain

Explore 1,208,002 web sites visited by users of the [Netcraft Toolbar](#)

7th December 2010

Search:

[search tips](#)

site contains

delitosinformaticos.gov.co

lookup!

example: site contains .netcraft.com

Results for delitosinformaticos.gov.co

Found 1 site

	Site	Site Report	First seen	Netblock	OS
1.	delitosinformaticos.gov.co		january 2008	etb - colombia	unknown

COPYRIGHT © NETCRAFT LTD 2010. ALL RIGHTS RESERVED.

Ataques a Infraestructura Critica del Estado



Results for presidencia.gov.co

Found 3 sites

Site	Site Report	First seen	Netblock	OS
1. www.presidencia.gov.co		september 1996	colombia telecomunicaciones s.a. esp	linux
2. web.presidencia.gov.co		october 2007	colombia telecomunicaciones s.a. esp	windows server 2003
3. wsp.presidencia.gov.co		october 2010	colombia telecomunicaciones s.a. esp	windows server 2003

COPYRIGHT © NETCRAFT LTD 2010. ALL RIGHTS RESERVED.

Results for policia.gov.co

Found 2 sites

Site	Site Report	First seen	Netblock	OS
1. www.policia.gov.co		february 1997	policia nacional bogota	linux
2. webrp.policia.gov.co		january 2010	policia nacional bogota	windows server 2008

COPYRIGHT © NETCRAFT LTD 2010. ALL RIGHTS RESERVED.



3

Phishing - Spoofing.

De: Invitados ICANN Cartagena 2010 <cartagena2010ejemplo@icann.org>

Asunto: **Bienvenida Datos de reserva**

Fecha: 7 de diciembre de 2010 18:28:28 GMT-05:00

Para: Jeffer Ruiz RUIZ LEAL

Responder a: cartagena2010ejemplo@icann.org

▶ 1 archivo adjunto, 7,1 KB Guardar Pase de diapositivas



Entrada — Cuenta POP (276 mensajes)

Eliminar No deseado Responder Resp. a todos Reenviar Chat Cabeceras largas Nuevo Recibir Conectar

Buscar

De	Asunto	Fecha recepción	
Asobancaria - Eventos	Asobancaria Eventos, Foro de Vivienda 2010.	9 de noviembre de 2010	16:25
ALEX SANCHEZ	FW: ATENTA SOLICITUD URGENTE	22 de octubre de 2010	13:43
Semana Económica	Balance de la banca en 2010 - Semana Económica 781	Ayer	7:50
Invitados ICANN Cartagena 2010	Bienvenida Datos de reserva	Hoy	18:28

De: Invitados ICANN Cartagena 2010 <cartagena2010ejemplo@icann.org>
Asunto: **Bienvenida Datos de reserva**
Fecha: 7 de diciembre de 2010 18:28:28 GMT-05:00
Para: Jeffer Ruiz RUIZ LEAL
Responder a: cartagena2010ejemplo@icann.org
▶ 1 archivo adjunto, 7,1 KB Guardar Pase de diapositivas

Buenas tardes señoras y señores, este es un e-mail de prueba, por favor entregue sus datos personales, podemos comenzar con los de reserva de Hotel ingreso al Centro de Convenciones y Exposiciones ENTRÉGUELOS AQUÍ: <http://www.icanncartagena2010.com>



Gracias.....

- Entrada
- hotmail
- Cuenta POP
- Borradores
- Enviado
- hotmail
- Cuenta POP

De	Asunto	Fecha recepción	
Asobancaria - Eventos	Asobancaria Eventos, Foro de Vivienda 2010.	9 de noviembre de 2010	16:25
ALEX SANCHEZ	FW: ATENTA SOLICITUD URGENTE	22 de octubre de 2010	13:43
Semana Económica	Balance de la banca en 2010 - Semana Económica 781	Ayer	7:50
Invitados ICANN Cartagena 2010	Bienvenida Datos de reserva	Hoy	18:28

De: Invitados ICANN Cartagena 2010 <cartagena2010ejemplo@icann.org>
 Asunto: **Bienvenida Datos de reserva**
 Fecha: 7 de diciembre de 2010 18:28:28 GMT-05:00
 Para: Jeffer Ruiz RUIZ LEAL
 Responder a: cartagena2010ejemplo@icann.org
 X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtQ0w9MA==
 X-Message-Status: n
 X-Sid-Pra: Invitados ICANN Cartagena 2010 <cartagena2010ejemplo@icann.org>
 X-Auth-Result: NONE
 X-Message-Info: JGTYoYF78jG9aBrNNNgFe7AicK+aoEDDWShB0nDNcwn45o8QOC5gfkTCN6YJNq9te94dHWwGa34mSO6oCghm/LKmAl0vnnLeDGyYz3WoX4=
 Received: from emkei.cz ([87.236.195.67]) by BAY0-PAMC1-F5.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675); Tue, 7 Dec 2010 15:28:28 -0800
 Received: by emkei.cz (Postfix, from userid 33) id A619ABD0F9D; Wed, 8 Dec 2010 00:28:28 +0100 (CET)
 X-Priority: 3 (Normal)
 Importance: Normal
 Errors-To: cartagena2010ejemplo@icann.org
 Mime-Version: 1.0
 Content-Type: multipart/mixed; boundary=BOUND_4CFEC31C9EC6E7.20715151
 Message-Id: <20101207232828.A619ABD0F9D@emkei.cz>
 Return-Path: www-data@emkei.cz
 X-Originalarrivaltime: 07 Dec 2010 23:28:28.0929 (UTC) FILETIME=[74203710:01CB9666]
 1 archivo adjunto, 7,1 KB

Buenas tardes señoras y señores, este es un e-mail de prueba, por favor entregue sus datos personales, podemos comenzar con los de reserva de Hotel ingreso al Centro de Convenciones y Exposiciones ENTRÉGUELOS AQUÍ: <http://www.icanncartagena2010.com>



Gracias.....

Invitados ICANN Cartagena 2010 [Agregar a contactos](#)

Para jeffer.ruiz@correo.policia.gov.co

De: **Invitados ICANN Cartagena 2010** (cartagena2010ejemplo@icann.org)

Enviado: martes, 07 de diciembre de 2010 11:28:30 p.m.

Para: jeffer.ruiz@correo.policia.gov.co

1 archivo adjunto | [Descargar todos los archivos adjuntos](#) (7,1 KB)
cartagena...jpg (7,1 KB)



Buscar correo electrónico



Organizar por >

Mostrar: **Todos** | No leídos | De contactos | Actualizaciones sociales | De grupos | Todo lo demás <<

Bienvenida Datos de reserva

[Vista completa](#)

Invitados ICANN Cartagena 2010 [Agregar a contactos](#)

Para jeffer.ruiz@correo.policia.gov.co

11:28 p.m.

[Responder](#)

De: **Invitados ICANN Cartagena 2010** (cartagena2010ejemplo@icann.org)

Enviado: martes, 07 de diciembre de 2010 11:28:30 p.m.

Para: jeffer.ruiz@correo.policia.gov.co

1 archivo adjunto | [Descargar todos los archivos adjuntos](#) (7,1 KB)
cartagena...jpg (7,1 KB)

Los datos adjuntos, las imágenes y los vínculos de este mensaje se han bloqueado por motivos de seguridad.

[Mostrar el contenido](#) | [Mostrar siempre contenido de cartagena2010ejemplo@icann.org](#)

Buenas tardes señoras y señores, este es un e-mail de prueba, por favor entregue sus datos personales, podemos comenzar con los de reserva de Hotel ingreso al Centro de Convenciones y Exposiciones **ENTRÉGUELOS AQUÍ:** <http://www.icanncartagena2010.com>

Gracias.....

Entrada

Invitados ICANN Cart 11:28 p.m.
Bienvenida Datos de reser

Semana Económica 06/12/2010
Balance de la banca en 20

Resumen quincenal c 03/12/2010
Resumen quincenal de de:

Corte Constitucional 03/12/2010
COMUNICADOS DE PRENS

DIJIN.ADEPE-GRIDI 03/12/2010
(Sin asunto)

YAIR ALEXIS VANEG 03/12/2010
Estadística

juan carlos castro sal 02/12/2010
RE: Saludo

Jorge Hernandez 02/12/2010
RE: Saludo

Jorge Hernandez 02/12/2010
RE: Saludo



POLICÍA NACIONAL

Información...

Ingeniería Social



Mi nombre es Jenna. Tengo 7 años de edad, cabello rubio y ojos aterradores. No tengo nariz ni orejas, estoy muerta. Si tu no mandas este mail a 15 personas en los proximos 5 minutos me aparecere esta noche junto a tu cama con un cuchillo y te matare... esto no es una broma algo bueno te sucederá a ti esta noche a las 9:22. Te lo vuelvo a decir esto no es una broma Alguien especial te llamara por telefono o hablara contigo y te dira cuanto te quiere.

NO LA ROMPAS!!!!!! PASALA





POLICÍA NACIONAL

Información...



4

Fortalezas.

Ley 1273 de 2009



Comunicación y difusión de la entrada en vigencia de la Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado **“de la protección de la información y de los datos”**- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1273 de 2009



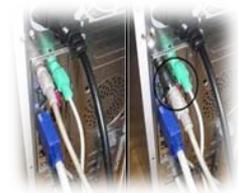
Art 269 A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.



Art 269 B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.



Art 269 C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.



Ley 1273 de 2009



Art 269 D. DAÑO INFORMÁTICO.



Art 269 E. USO DE SOFTWARE MALICIOSO.

Art 269 F. VIOLACIÓN DE DATOS PERSONALES.



Art 269 G. SUPLANTACIÓN DE SITIO WEB PARA CAPTURAR DATOS PERSONALES.



Ley 1273 de 2009



Art 269 H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.



Art 269 I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.



Art 269 J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.



Ley 1273 de 2009



LEY N.º. 1273

"POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO - DENOMINADO "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS"- Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES".

REPÚBLICA DE COLOMBIA - GOBIERNO NACIONAL

PUBLÍQUESE Y CÚMPLASE

5 ENE 2009

Dada en Bogotá, D.C., a los

W

Ley 906 Código de Procedimiento Penal



Art. 236 RECUPERACIÓN DE INFORMACIÓN DEJADA AL NAVEGAR POR INTERNET U OTROS MEDIOS TECNOLÓGICOS QUE PRODUZCAN EFECTOS EQUIVALENTES.



Cómo Investigar



ARTÍCULO 275. ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA.

g) El mensaje de datos, como el intercambio electrónico de datos, Internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen





GRUPO DE INVESTIGACIONES TECNOLÓGICAS



CAI Virtual



Inicio
Descargas
Enlaces de Interés
Contacto

cai virtual
caivirtual

Con el avance de las tecnologías muchas amenazas y riesgos han hecho transición al espacio virtual.

"Spyware" son programas espía que se instalan en un ordenador sin el conocimiento del usuario, para recopilar información personal.



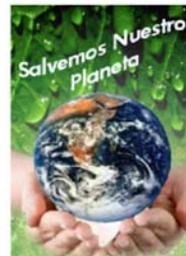
Asegúrese de que el sitio Web utiliza cifrado



Si no se puede confiar en un sitio Web por su barra de direcciones, ¿cómo se sabe que será seguro? Existen varias formas: En primer lugar, antes de ingresar cualquier tipo de información personal, compruebe si el sitio Web utiliza cifrado para transmitir la información personal. En Internet Explorer puede comprobarlo con el icono de color amarillo situado en la barra de estado, tal como se muestra en la figura.

[Read more](#)

Tips para hacer un uso ecológico del ordenador



Los grandes fabricantes de componentes informáticos destinan anualmente parte de sus inversiones a investigar métodos para ganar en eficiencia energética. Las pantallas, procesadores y discos duros cada vez aprovechan mejor la energía y gastan menos.

De todos modos, aunque los componentes mejoren, el punto clave en el ahorro energético seguirá siendo el usuario.

Podemos comprar un magnífico ordenador que haya pasado todos los controles de eficiencia energética, tenga mil certificados de calidad y otras tantas pegatinas que empiecen por eco, que si no hacemos un uso con mentalidad de ahorro, tanta tecnología no servirá para nada.

[Read more](#)

Cai Virtual



Ingresar

Por favor ingresa tu usuario y password
para poder acceder

Usuario:

Contraseña:

[\[Regístrate\]](#)



5

Retos.

Visión al Futuro



COBERTURA

44 SECCIONALES DE INVESTIGACIÓN CRIMINAL , 08 LABORATORIOS REGIONALES DE INFORMÁTICA FORENSE, 135 INVESTIGADORES EXPERTOS EN CIBERCRIMEN.



ÁMBITO INTERN.

GLDT GRUPO DE TRABAJO LATINOAMERICANO DE DELITOS TECNOLÓGICOS.
FIEC FORO IBEROAMERICANO DE CIBERPOLICÍAS.



CAI VIRTUAL

ATENCIÓN A REQUERIMIENTOS CIUDADANOS ON-LINE , SERVICIO DE CHAT Y WEB PARA RESPONDER A INCIDENTES DE CIBERDELITOS.



COL CERT

CENTRO DE RESPUESTA A INCIDENTES CIBERNÉTICOS EN COLOMBIA – INICIATIVA QUE VINCULA MINDEFENS.



CETS

CHILD EXPLOITATION TRACKING SYSTEM SISTEMA DE MONITOREO DE PORNOGRAFÍA INFANTIL EN INTERNET.



Procesamiento de la evidencia digital



- Procedimientos Estandarizados en el Laboratorio de Informática Forense.
- Network Forensics.
- Cloud Computing.



Hallazgo

Identificación

Imagen Forense

Búsquedas Avanzadas

Extracción Información

Análisis

Proyección informes

Investigaciones Tecnologicas Policia Nacional



SI JEFFER RICARDO RUIZ LEAL

**AV el Dorado No 75-25 Modelia
Bogotá D.C.**

www.delitosinformaticos.gov.co

caivirtual@correo.policia.gov.co

4266301 - 4266256



POLICÍA NACIONAL

GRACIAS