PRIVACY INTERNATIONAL

Shadow State: Surveillance, Law and Order in Colombia

Special Report



Shadow State: Surveillance, Law and Order in Colombia

XXXXXXXXXXXX
August 2015

PRIVACY INTERNATIONAL

www.privacyinternational.org



Bogotá skyline from Monseratte mountain.
Credit - Privacy International 2014

Table of Contents

List of Acronyms	6
Executive Summary	7
Recommendations	10
Introduction	13
Surveillance and Insecurity	17
Esperanza	21
PUMA and Mass Interception	27
Beyond the Law	32
Shadow System: DIPOL and The Integrated Recording System	37
Tactical Tools	42
DIPOL and the Silicon Valley Surveillance Company	44
DAS Network probes and Tactical Interception	47
Legal and Technical Controls	51
A New Phase of Chuzadas	53
Conclusion	56
Annex	57

List of Acronyms

3G	Third generation mobile telecommunications technology
4G	Fourth generation mobile telecommunications technology
ASFADDES	Association of Relatives of Detainees, Disappeared Persons
CCAJAR	The José Alvear Restrepo Lawyers' Collective
CALEA	US Communications Assistance for Law Enforcement Act
Chuzadas	Term popularly denoting illegal interceptions and surveillance
CIA	US Central Intelligence Agency
CIJP	Inter-Church Justice and Peace Commission
CSPP	Committee for Solidarity with Political Prisoners
CTI	Fiscalía Technical Investigations Unit
DAS	Administrative Department of Security
DEA	US Drugs Enforcement Agency
DIASE	Anti-kidnapping and Anti-extortion Directorate
DIJIN	Directorate of Criminal Investigation and Interpol
DIPOL	Directorate of Police Intelligence
DNI	National Intelligence Directorate
E1	Telecommunications link designed to carry voice and data communications
ELN	National Liberation Army
EMS	Electromagnetic spectrum
Esperanza	Interception platform managed by Fiscalía
ETSI	European Telecommunications Standards Institute
FARC	Revolutionary Armed Forces of Colombia
Fiscalía	Office of the Attorney General of Colombia
GAULA	Unified Action Groups for Personal Liberty
ICCPR	International Covenant on Civil and Political Rights
IMSI	International Mobile Subscriber Identity
INTERPOL	International Criminal Police Organization
IP	Internet protocol
IRS	'Integrated Digital Recording System', communications surveillance system managed by DIPOL
ISP	Internet service provider
NGO	Non-governmental organisation
PGP	Pretty Good Privacy, data encryption program
PUMA	Single Monitoring and Analysis Platform, communications surveillance system managed by DIJIN
RCS	Remote Control System, surveillance solution by Hacking Team
SIJIN	Regional Police Criminal Investigation Section
SMS	Short message service
VoIP	Voice over Internet Protocol

Executive Summary

Government ambition to conduct surveillance of citizens' communications often extends further than the law. Unconstrained surveillance powers threaten the right to privacy and other fundamental rights. It makes democratic governance impossible. Citizens fear to speak, think and organize freely when faced with disproportionate, unjust or politically-motivated spying on their communications.

The Colombian government has reformed its surveillance laws, interrogated its technical capabilities, and even disbanded one of its security agencies in light of revelations about the abuse of surveillance systems. This investigation by Privacy International based on confidential documents and testimonies shows that recent reforms have been undermined by surreptitious deployment of mass, automated communications surveillance systems by several government agencies outside the realm of what is proscribed by Colombia's flawed intelligence laws.

Colombia's challenging history is well known. More than 220,000 lives have been lost since 1958 in a brutal conflict that has left millions of people internally displaced and over 25,000 disappeared, according to some estimates.

Communications surveillance has been integral to the conflict. Phone tapping helped to locate leaders of the rebel FARC group. In 2002 it was revealed that around 2,000 phone lines had been tapped, including those of groups representing families of the disappeared. In 2007, eleven police generals were dismissed after it was disclosed the agency was tapping opposition politicians, journalists, lawyers, and activists. In 2009, it was revealed that the Administrative Department of Security (Departamento Administrativo de Seguridad, 'DAS') had surveilled and harassed over 600 public figures. In 2014, the newspaper Semana revealed that the Colombian army unit codenamed Andromeda had been spying for more than a year on the government's negotiating team in the ongoing peace talks with the FARC. The scandals have shocked and galvanized Colombia's civil society and ordinary citizens. But it has reinforced their assumption that that they are always monitored.

The key agencies in Colombia that monitor communications all compete for resources and capabilities. This has resulted in overlapping, unchecked systems of surveillance that are vulnerable to abuse.

The nation's most visible communications interception system is Esperanza (Sistema Esperanza); it is heavily supported by the US Drugs Enforcement Agency (DEA). The Office of the Attorney General (Fiscalía General de la Nación, 'Fiscalía') manages and administers the platform, which can obtain mobile and fixed-line call data and content. Esperanza, to which various law enforcement agencies have access, is connected to the nation's telecommunications operators. It is used to obtain evidence for judicial prosecution on a case-by-case basis. It requires that a Fiscalía

agent physically request an individual phone line or record be intercepted. Other safeguards built in to the Esperanza system include an electronic warrant submission system and supervisory judges (jueces de control de garantías). However, as this investigation shows, Esperanza suffered from various security vulnerabilities and its restriction to accessing data only for pre-defined individual targets on the basis of a warrant was a point of friction for other law enforcement agencies.

Beyond Esperanza, however, numerous other communications interception systems exist in Colombia, either unlawfully or with dubious legal justification. The Police Directorate of Criminal Investigation and Interpol (Dirección de Investigación Criminal e INTERPOL, 'DIJIN') has built the Single Monitoring and Analysis Platform (Plataforma Única de Monitoreo y Análisis, 'PUMA'), a phone and internet monitoring system linked directly to the service providers' network infrastructure by a probe that copies vast amounts of data and sends it directly to DIJIN's monitoring facility. PUMA is capable of intercepting and storing potentially all communications that pass through its probes. Communications service providers know of its existence and cooperated in its installation but are excluded from its day-to-day operation.

PUMA was acquired in 2007. In 2013, the Police put forward proposals to extend the system, claiming that an expanded PUMA would be capable of capturing three times more phone calls and data. The expanded PUMA was to include a monitoring module for internet service providers (ISP) and up to 700 workstations throughout the country. Yet disagreement between the Fiscalía and the Police over its management stalled the expansion, and the project was put on hold. Nonetheless, new contracts are still being settled.

While Esperanza and PUMA were being deployed by the Fiscalía and DIJIN respectively, the Police Intelligence Directorate (Dirección de Inteligencia Policial, 'DIPOL') acquired and deployed its own mass, automated communications surveillance system, the Integrated Recording System ('IRS'). Established in 2005, the IRS monitors massive communications traffic across E1 lines and 3G mobile phone traffic. Like PUMA, it is set up with service providers' knowledge and monitoring is done without their knowledge. Our analysis of the technologies is that the system is capable of collecting 100 million call data records per day and intercepting 20 million SMS per day. This vast data store is then processed and combined with other types of data including images, video, and biometric details.

This type of mass, automated surveillance is not explicitly authorised under Colombian law. Whereas the interception of communications may be authorised by the Attorney General's office for the purpose of seeking evidence in judicial proceedings, as enshrined in the Constitution and the Criminal Procedure Code, such powers are ill-fitting to authorise the type of bulk passive phone and internet monitoring and analysis made possible by PUMA and the IRS.

The technologies undergirding both systems automatically collect and store communications data passively via a set of probes linked to a monitoring centre. The result is that both DIPOL and DIJIN are conducting mass interception of

communications without explicit lawful authority, and, in the case of DIPOL, without any legal authority to intercept communications at all.

This report also establishes that Colombian government agencies deploy tactical surveillance. DIPOL currently has the capacity to deploy fake mobile phone base stations that can monitor phone usage and intercept communications without involvement from service providers nor necessarily with the knowledge of judicial authorities; DAS previously possessed such technology, too. The Colombian police is known to have contracted with hacking and malware companies to enable access to computers and mobile phones.

This report concludes that agencies are building their own surveillance systems, in the shadows, without sufficient scrutiny and without lawful basis.

Recommendations

To the National Police of Colombia (Policía Nacional de Colombia):

- Declassify and publish all procurement documents for technologies for which information about technical capabilities is in the public domain.
- Declassify and publish all procurement documents related to the expansion of the Single Monitoring and Analysis Platform ('Plataforma Única de Monitoreo y Análisis', PUMA).
- Declassify and publish all procurement documents related to the Police Integrated Recording System ('Sistema Integral de Grabación Digital con Destino a la Policía Nacional').
- Publicly confirm the existence and specify the nature of any contracts for malware and hacking companies – including the Italian company Hacking Team – that are currently active or have been active in the past ten years.

To the Office of the Attorney General (Fiscalía General de la Nación):

- Consider the implications of the evidence presented here of DAS' procurement and maintenance of an interception probe provided by Verint and technologically independent tactical surveillance technologies including IMSI catchers for allegations of unlawful behaviour by the DAS prior to its dissolution.

To the Senate Legal Commission for the Monitoring of Intelligence and Counter-Intelligence Activities (Comisión legal de seguimiento a las actividades de inteligencia y contrainteligencia del Senado):

- Convene a hearing to ascertain the nature, manner and number of monitoring activities carried out by Colombia's national intelligence and police agencies under the authorisation of Article 17 of the Intelligence Law of 2003 and recommend appropriate amendments accordingly.
- Convene an inquiry to ascertain whether the safeguards in place in Law 1621 of 2013 are sufficient to avoid abusive practices and to maintain public trust.
- Convene an inquiry to ascertain the extent to which the technology detailed in this report is currently in use, focusing particularly on the institutions with access to such technologies.
- Call for a review of existing contracts, procurement documents, and policies for use by congressional committees to enable them to understand and audit existing surveillance capabilities.

- Convene an inquiry to ascertain whether the five year minimum data retention obligation of telecommunications service providers established by Decree 1704 of 2012 and Law 12621 of 2013, is proportionate.
- Release any transparency reports that have been provided to the committee by the Directorate of National Intelligence (Dirección Nacional de Inteligencia, 'DNI') in relation to its activities.
- Publish any findings related to the above inquiries.

To the Office of the Inspector General (Procuraduría General de la Nación):

- Investigate whether the DIJIN and DIPOL officials responsible for procurement have acted within their lawful mandate, including by procuring, purchasing and deploying surveillance technologies.
- Publish any findings related to the above inquiries.

To the Deputy Superintendent for the Protection of Personal Data (Superintendente Delegado para la Protección de Datos Personales):

- Ascertain what, if any, implications the revelations of mass surveillance in Colombia have on compliance with data protection legislation.
- Publish any findings related to the above inquiry.

To the Ombudsman's Office of Colombia (Defensoría del Pueblo):

- Ascertain whether the deployment of PUMA by the Fiscalía and Police is compliant with Colombia's domestic and international human rights obligations.
- Publish any findings related to the above inquiry.



National Capitol building where the Congress of Colombia is housed, Bolivar Square, Bogotá. Credit - Privacy International (2014).

Introduction

Over the past decade the Colombian state has been building a mass surveillance architecture without clear lawful authority or adequate safeguards against abuse, and without sufficient opportunity for public scrutiny. In a country that has seen communications surveillance routinely used to harass critics of government policies, keep tabs on public servants, and compromise efforts to peacefully resolve ongoing armed conflict, the expansion of Colombia's shadow surveillance state is of serious concern.

This Privacy International report is the first of two exposing Colombia's surveillance architecture. It highlights the legal deficiencies and political conditions that have led to the expansion of mass surveillance capabilities, as well as ramifications for Colombia of mass surveillance, drawing from public records, previously confidential documents, and the testimony of persons directly involved in these interception systems.

The surveillance capabilities of the Colombian state have increased in parallel with ongoing military operations against the country's largest guerrilla groups.[1] Yet evidence of the illegal interception of private communications pervade accounts of extrajudicial disappearances and killings, however, and the country has witnessed a series of scandals about the abuse of interception capabilities by various state agencies.

Since the late 1990s, the lawful interception of communications on Colombian networks has been effected through Esperanza, an interception system managed by the Office of the Attorney General of Colombia (Fiscalía General de la Nación, 'Fiscalía'), and accessed by the Police and the now-disbanded Administrative Department of Security (Departamento Administrativo de Seguridad, 'DAS').

Esperanza functions as a targeted interception system that relies on active requests by human users, the Fiscalía administrators, to 'task' Colombia's service providers to

1 This report focuses on the communications interception and monitoring capacities of Colombian law enforcement and intelligence services and not of the armed forces. In Colombia, the Police and Army are two branches of the 'public force' that come under the control of the Ministry of Defence. The armed forces of Colombia carry out significant interception and monitoring activities in the course of operations against armed groups. Privacy International holds information on these capacities that it chooses not to disclose at this time for security reasons.

send specifically requested audio and data records for mobile phone and fixed-line calls. This is explicitly sanctioned by the Colombian Constitution and Criminal Procedure Code.

In recent years there has been an attempt to expand Colombia's communications interception capacity beyond Esperanza to include large-scale, automated interception of phone and email traffic on the backbone of Colombia's telecommunications infrastructure. This is mass surveillance. Potentially all communications are swept up, filtered, monitored and analysed before being stored for further interrogation or deletion. Unlike traditional forms of targeted interception like Esperanza, when the telecommunications company or service provider facilitates the interception of a particular phone number or wire, automated interception allows for whole cables to be intercepted en masse by placing a probe directly on the cable.

Colombia has acquired mass surveillance capabilities both in public and in the shadows. The most public embodiment of the government's attempts to expand its surveillance capabilities is PUMA, the Single Monitoring and Analysis Platform (Plataforma Única de Monitoreo y Análisis). Launched in 2007 as a system administered and paid for by the Police Directorate of Criminal Investigation and Interpol (Dirección de Investigación Criminal e INTERPOL, 'DIJIN'), PUMA is designed to intercept, store and analyse massive amounts of phone traffic. A 2014 upgrade to the system saw the inclusion of mass internet traffic surveillance capacities. Concerned that the growing police system might unnecessarily violate fundamental rights, the head of the Fiscalía called for a halt to the project pending an interagency review in August 2014.[2]

The Police has characterized PUMA as a simple modernisation and expansion of the current lawful interception capabilities of Esperanza. In fact, PUMA conducts a completely different and far more invasive form of surveillance. This is not only of concern from the perspective of public transparency and accountability; it also raises serious questions about the lawful basis of such a system. Interception is lawful in Colombia only when it is conducted pursuant to a court order, following the formalities established by law. Exceptionally, the Fiscalía may act to intercept communications without a warrant but it requires ex post judicial authority to use the data. The Criminal Procedure Code provides for the Attorney General's Office to intercept communications for the sole purpose of obtaining evidence in judicial proceedings. Mass or automated interception of communications for the purpose of intelligence gathering is neither contemplated nor explicitly authorised by Colombian law, yet DIJIN purports that the acquisition of PUMA – which enables mass, automated interception of communications – is lawful.

Privacy International can also reveal that the Colombian Police have also been engaged in building a shadow interception architecture without clear lawful authority

2 "Fiscalía le dice 'no' a sistema de interceptación 'Puma' de la Policía", El Tiempo, 20 August 2014, http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

or public scrutiny, and that the DAS, before it was disbanded, had the technical capacity to conduct communications interceptions independently of Esperanza. The Police Intelligence Directorate (Dirección de Inteligencia Policial, 'DIPOL') intercepts vast volumes of communications signals that travel across Colombia's telecommunications backbone via network probes connected to a monitoring centre platform, called the Integrated Recording System ('IRS'). This monitoring centre receives, processes and retains data collected by a variety of surveillance systems, including internet monitoring, location monitoring, phone monitoring, and audio surveillance. Once collected, this data is analysed by powerful computers that display connections between people, their conversations and events, and build profiles of individuals and their contacts.

A number of other state agencies beyond the police are also acquiring these intrusive capabilities. DAS, which in 2011 was disbanded after a media investigation revealed its agents had committed illegal interceptions, had maintained its own network interception capabilities. Sometime before 2010, DAS acquired a network probe that appears to have operated separately from the Esperanza system. DIPOL, DIJIN and other agencies including DAS until its dissolution also used mobile interception devices (generically called "IMSI catchers") that allow for localised indiscriminate interception of all mobile phone calls and text messages in a specific location. Furthermore, in 2012, DIPOL also negotiated a potential purchase of powerful open source intelligence technology from Palantir, an American data analytics company. This would have allowed DIPOL to build on their existing databases to analyse and process vast amounts of data and communications. In addition, the police acquired intrusion software from Italian company Hacking Team which would enable the police to undertake targeted remote exploitation – hacking and subsequent control – of individuals' devices.

The State agencies acquiring these capabilities do so not only outside of public scrutiny, but also without clear legal sanction. None of the above listed agencies are authorized to conduct interception without first obtaining judicial authorisation and following formalities established by law. The Criminal Procedure Code provide that the interception of communications can only be effected upon the order of the prosecutor, in the presence of a judicial investigation, and in order to seek evidence. The 2013 Intelligence Law grants wide powers for monitoring the electromagnetic spectrum, but such powers do not authorise the use of mass, automated interception of communications such as that effected by PUMA and the IRS.

More generally, the proliferation of interception under the justification of intelligence-gathering is extremely worrying. Surveillance is a tool for political control. Public officials routinely tell Colombians that the interception of their communications is subject to rigorous safeguards[3]. Safeguards built in to the Esperanza system include

3 In February 2011, the Colombian Defence Minister Juan Carlos Pinzón Bueno stated: "Colombians can be sure that the use of these tools [communications surveillance technologies] by the State is fully in accordance with the law and always aimed [to assure] the safety of all Colombians", 5 February 2011, http://www.policia.gov.co/portal/pls/portal/JOHN.NOTICIAS_NUEVAS_DETALLADAS.SHOW?p_arg_names=identificador&p_arg_values=356593

an electronic warrant submission system and supervisory judges (jueces de control de garantías), both of which are designed to provide a check on unlawful interception.

However, even the most tightly regulated of lawful interception systems in Colombia, Esperanza, has been subject to abuse by government agencies. As set out above, the Fiscalía is currently investigating the DAS following allegations that its officials misused Esperanza by presenting fraudulent interception requests to obtain unlawful access to individuals' communications. DAS officials are alleged to have subsequently tracked, harassed, and intimidated Colombian journalists, activists and politicians. However, these allegations of abuse did not stop the DAS from purchasing and installing more surveillance equipment.

This investigation finds that the national police, intelligence and security services were and are capable of carrying out interception on a massive scale outside of the existing Colombian legal framework. Rivalries between different law enforcement and intelligence agencies, each operating with different budgets and legal mandates, create a situation in which Colombians' communications traffic is being passively collected by different uncoordinated and often competing surveillance systems. An overly broad, technically unsound legal framework enables interception of communications to occur without adequate safeguards.

Surveillance and Insecurity

Colombian law enforcement and intelligence agencies' surveillance capabilities have grown as military operations against the country's largest guerrilla group, FARC (the Revolutionary Armed Forces of Colombia), and its smaller cousin, ELN (the National Liberation Army) have expanded.[4] The Colombian armed conflict is the longest-running of its kind in the Western Hemisphere and has, over more than fifty years, involved a number of actors. Paramilitary groups, sometimes working in tandem with parts of the state, officially demobilised in the mid-2000s. Several other leftist guerrilla groups also demobilised at various stages of the conflict. Since 1958, the conflict has claimed the lives of nearly 220,000 people[5], most of them civilians. In the period 1985-2012, 5.7 million people were internally displaced[6] and 25,000 people were disappeared.[7]

Hardliner Álvaro Uribe was elected president in 2002 following failed peace talks that had allowed FARC to expand its territorial influence. During his two terms in office he pursued a "Democratic Security Policy" with the aim of regaining control of territory and eliminating the drug trade. The policy expanded the military's presence into areas where it had not previously been active and increased spending on defence, employing and training additional soldiers and police, and improving intelligence capabilities. Much of this work was financed through Plan Colombia, a US programme that between 2000 and 2011 gave Colombia more than US$ 8 billion in assistance, much of which went to the military.[8]

In 2007, with FARC weakened militarily as a result of a sustained military campaign, the Uribe administration launched a follow-up plan to the Democratic Security Policy that aimed to consolidate military gains by establishing civilian governance and providing social services in remote areas[9]. Uribe's successor, Juan Manuel Santos has largely pursued the same approach of consolidation. In 2012, Santos initiated

4 The US State Department has listed both groups on its Foreign Terrorist Organizations list. 2015, http://www.state.gov/j/ct/rls/other/des/123085.htm

5 "Report says 220,000 died in Colombia conflict", Al Jazeera, 25 July 2013, http://www.aljazeera.com/news/americas/2013/07/201372521122146399.html

6 "2015 UNHCR country operations profile – Colombia", UNHCR, 2015, http://www.unhcr.org/pages/49e492ad6.html

7 "NGO's remember 25,000 forcibly disappeared in Colombia, call on govt to do more", Colombia Reports, 22 May 2014, http://colombiareports.co/ngos-organize-commemoration-week-25000-forcibly-disappeared-colombia/

8 "The Colombia Strategic Development Initiative", US Department of State, 14 April 2012, http://www.state.gov/p/wha/rls/fs/2012/187926.htm

9 "Política de Consolidación de la Seguridad Democrática", Colombia National Ministry of Defence, 2007, http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Home/Politica_de_Consolidacion_de_la_Seguridad_Democratica.pdf

peace talks with FARC and negotiators have already reached agreements in several areas. Communications interception scandals (chuzadas) have been a feature of Colombian security politics since the 1990s. Authorities have been tapping phone lines since at least 1971[10] and surveillance has played an important role in military operations against the FARC in recent years. In 2011, intercepted phone calls were reportedly crucial to locating FARC's supreme leader, Alfonso Cano, subsequently killed in a military attack.[11] The military reportedly used the Esperanza interception system to locate the FARC's military leader, Mono Jojoy, also subsequently killed.[12]

However, stories of the illegal interception of private communications pervade accounts of extrajudicial disappearances and killings. Different agencies have been involved in these illegal interceptions. In one famous case, more than 2,000 phone lines were illegally tapped by the joint military-police Unified Action Groups for Personal Liberty (Grupos de Acción Unificada por la Libertad Personal, 'GAULA'), according to the Fiscalía in 2002.[13] Targeted were a group representing families of the disappeared, ASFADDES, who had seen at least two of its own members disappeared that year. In 2007, eleven police generals from DIPOL were dismissed following revelations that the agency had tapped influential opposition politicians', journalists', lawyers' and activists' phones.[14] In 2014, the Colombian weekly magazine Semana alleged that a Colombia army unit codenamed Andromeda was spying for more than a year on the government's negotiating team in ongoing peace talks with the country's FARC guerrillas.[15]

Yet the most notorious of the interception scandals involves the DAS and was revealed by Semana in February 2009. Special strategic intelligence groups of the DAS conducted targeted surveillance of an estimated 600[16] public figures including parliamentarians, journalists, human rights activists and lawyers, and judges among others. According to files retrieved during an investigation by the Fiscalía[17], the DAS

10 According to testimony from the former DAS director Carlos Arzayus before the Supreme Court in May 2010. "Un ex director del DAS confirma seguimientos desde 1971 y revela nuevos nombres de personas espiadas", El Diario Exterior, 4 May 2010, http://www.eldiarioexterior.com/articulo.asp?idarticulo=26464&accion=ext

11 "Top Farc rebel leader Alfonso Cano killed in Colombia", BBC News, 5 November 2011, http://www.bbc.com/news/world-15604456

12 "Chuzadas: así fue la historia", Semana, 8 February 2014, http://www.semana.com/nacion/articulo/chuzadas-asi-fue-la-historia/376548-3

13 "Informe sobre Derechos Humanos: Colombia", US Department of State, 4 March 2002, http://www.acnur.org/t3/uploads/media/COI_53.pdf

14 "El DAS-gate y las 'chuzadas', vuelve y juega", El Espectador, 21 February 2009, http://www.elespectador.com/impreso/judicial/articuloimpreso120201-el-das-gate-y-chuzadas-vuelve-y-juega

15 Alguien espió a los negociadores de La Habana?" Semana, 3 February 2014, http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/37607

16 "Más de 600 personas habrían sido 'chuzadas' ilegalmente por el DAS, según investigadores", Caracol Radio, 17 April 2009, http://www.caracol.com.co/noticias/judiciales/mas-de-600-personas-habrian-sido-chuzadas-ilegalmente-por-el-das-segun-investigadores/20090417/nota/796294.aspx

17 "Un 'manual' para seguir y acosar a personas calificadas como opositores tenía el DAS", El Tiempo, 13 June 2009, http://www.eltiempo.com/archivo/documento/CMS-5436047

intercepted phone calls, email traffic and international and national contacts lists, using this information to compile psychological profiles of targets and conduct physical surveillance of subjects and their families, including children.

Communications surveillance was central to the DAS abuses. The phone lines of journalist Hollman Morris were under near-constant surveillance. Morris was later forced into exile on several occasions. Claudia Duque, a lawyer and journalist formerly working with the CCAJAR lawyers collective survived kidnapping attempts and received graphically violent phone threats; DAS files about her contained extensive evidence of communications and physical surveillance.[18] Such was the scale of the illegal interception that seven Supreme Court justices were recused from the 2011 trial of the former DAS head because evidence suggested that even they had been illegally spied on.[19]

Although the DAS had weathered previous abuse scandals by publicly purging its ranks, the Semana revelations were the last straw. In his first speech after the scandal broke, then-President Álvaro Uribe announced that intelligence agency DAS was no longer allowed to intercept any phone conversation without Police authorization.[20]

The scandal-ridden DAS was disbanded in October 2011. Several former DAS heads were convicted for illegal interception and associated crimes. Fernando Tabares, former DAS director, was convicted for illegal wiretapping of government opponents in 2010.[21] Maria del Pilar Hurtado, who headed DAS in 2008 is the highest-ranking official to have been convicted for illegal surveillance.[22] In 2011 a new agency, the National Intelligence Directorate (Dirección Nacional de Inteligencia, 'DNI'), was established to head the intelligence and counterintelligence sector within the overall structure of the state. [23]

18 "Former security operatives charged in journalist's torture in Colombia", IFEX, 18 March 2013, https://www.ifex.org/colombia/2013/03/18/security_charged/ and "Colombian official convicted of 'psychological torture' of journalist", Committee to Protect Journalists, 22 December 2014, https://cpj.org/2014/12/colombian-official-convicted-of-psychological-tort.php

19 "7 judges withdrawn from wiretap trial", Colombia Reports, 12 August 2011, http://colombiareports.com/7-supreme-court-judges-victimized-in-wiretap-scandal-withdrawn-from-trial/

20 Nevertheless, DAS investigations relying on phone call interceptions would continue with the DAS monitoring rooms remaining operative. "Uribe forbids DAS to independently wiretap suspects", Colombia Reports, 26 February 2009, http://colombiareports.co/uribe-forbids-das-to-independently-wiretap-suspects/

21 "Ex-DAS head convicted of illegal wiretapping", Colombia Reports, 12 August 2011, http://colombiareports.co/former-das-director-convicted-wiretapping-scandal/

22 "Chuzadas' del DAS: crimen y castigo", Semana, 28 February 2015, http://www.semana.com/nacion/articulo/chuzadas-del-das-crimen-castigo/419365-3

23 "Preguntas frecuentes", Dirección Nacional de Inteligencia, 2011, http://webcache.googleusercontent.com/search?q=cache:as90hKvsQOMJ:www.dni.gov.co/index.php%3Fidcategoria%3D624%26download%3DY+&cd=1&hl=en&ct=clnk&gl=uk

DAS is alleged to have committed the illegal interceptions by abusing the Esperanza System.[24] During the Fiscalía's investigation, DAS officials denied knowledge of having independent interception capabilities;[25] this report will demonstrate the DAS did possess those capabilities, at least in the latter half of the 2000s. Instead, the inquiry focused on whether or not the DAS had access to Esperanza during the period in which the abuses occurred.[26] This report shows that the DAS was independently able, in a technical sense, to intercept phone and email communications without relying on the Esperanza system.

24 "Procuraduría profiere decisión disciplinaria en caso de interceptaciones ilegales", Procuraduría General de la Nación, 4 October 2010, http://www.procuraduria.gov.co/html/noticias_2010/noticias_708.htm

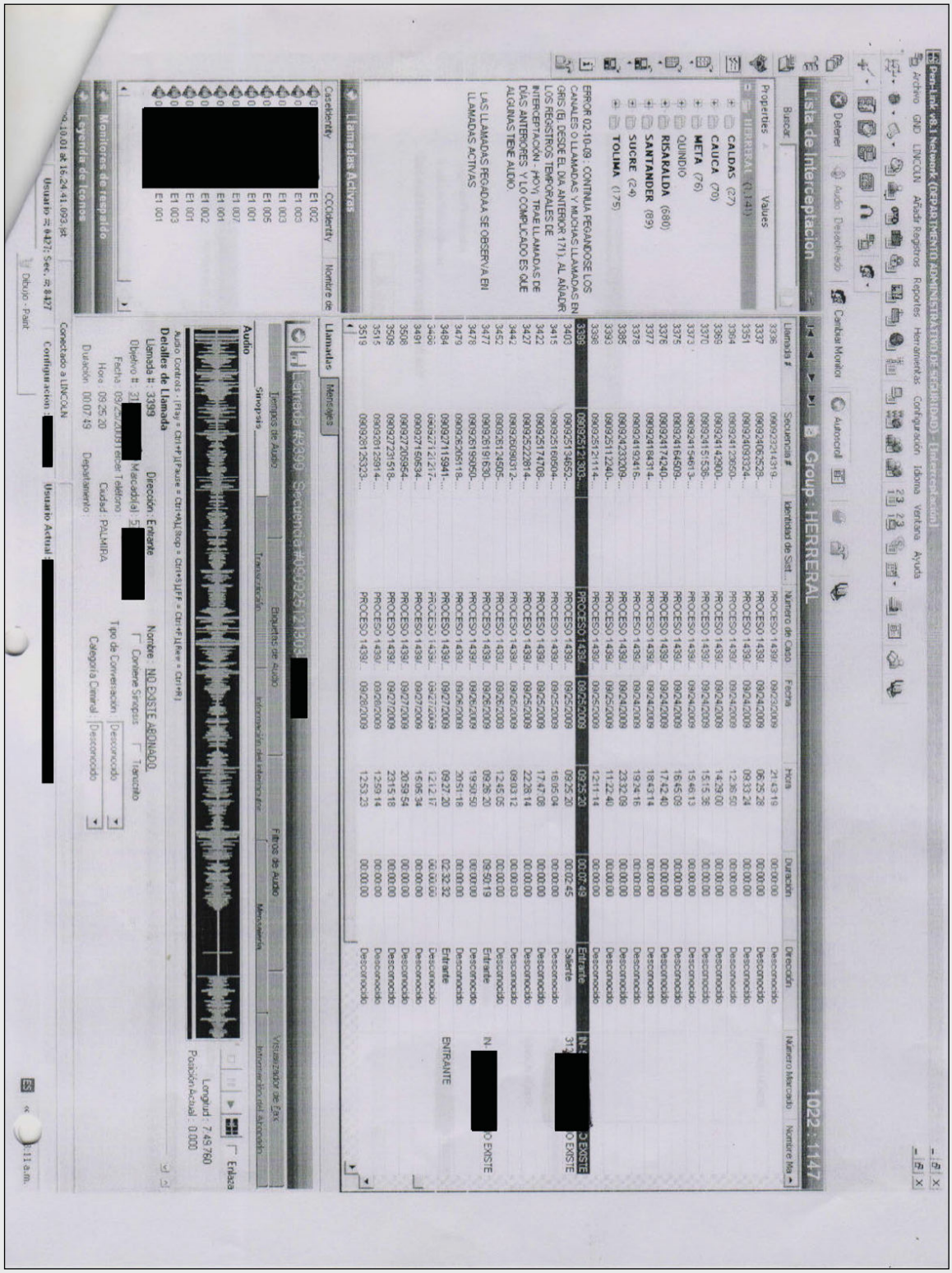
25 "Texto de la sentencia en el caso de las escuchas ilegales del DAS", Criminal Court Third Circuit, Bogotá, 30 November 2012, http://www.derechos.org/nizkor/colombia/doc/das299.html#373

26 "Texto de la sentencia en el caso de las escuchas ilegales del DAS", Criminal Court Third Circuit, Bogotá, 30 November 2012, http://www.derechos.org/nizkor/colombia/doc/das299.html#373

Esperanza

Fiscalía officials met with US Drugs Enforcement Agency (DEA) officials in the early 2000s to develop the system, originally established in 2004 as 'Project Esperanza' and formalized in 2005 by Interadministrative Agreement 038 of 2005 as a joint interception system of the Fiscalía, Police and DAS.

Interception through Esperanza involves capturing individuals' communications on a targeted basis, with the knowledge and cooperation of the telecommunications service provider, and is explicitly authorised under Colombian law. Esperanza allows the Fiscalía to connect to telecommunications providers' servers, to receive and package real-time call information to transmit into a central monitoring room. The signal is then dispatched to other monitoring rooms controlled by the Fiscalía's Technical Investigations Unit (Cuerpo Técnico de Investigación, 'CTI'), the Police and DAS, when it was functional.



WHAT THE DAS SAW

Analysts would query the systems interface, software provided by US company Pen-Link and see real-time call information for a target's phone.

Esperanza relies on a bespoke platform assembled by Colombian company STAR Inteligencia & Tecnología. STAR is also the exclusive provider of a number of British and American firms' products, which also feature in the Esperanza system. The companies are discussed in more depth in the second report by Privacy International, Demand/Supply: Exposing the Surveillance Industry in Colombia.



Credit: Star I & T, 2015 http://star-it.co

Octopus is one of STAR's signature interception suites, a cross connect switch that receives signals from different protocols, including GSM (mobile phones), IP (internet) and lawful interception protocols ETSI and CALEA and sends it onward to its destination – a law enforcement monitoring centre.

Interceptions are effected through Esperanza in the following way: an analyst must first submit a document requesting the interception of a particular line to a Fiscalía agent. That document must set out the justification for the interception. The Fiscalía agent should authorise it and request the routing of the call through the Esperanza system to the Fiscalía's main monitoring centre in its basement, the 'Bunker', which would subsequently route it to any of the other monitoring rooms. Esperanza was connected to at least 20 rooms in 2012 identified by colours. At least six of these rooms received financial and technical support from the DEA, and DEA analysts share workspace with their Colombian colleagues.[27] The US embassy is metres away.

27 "Acta nº 448-2009 de Consejo Superior, 3 de Septiembre de 2009", Superior Council of the Judiciary, 3 September 2009, http://vlex.co.cr/vid/-456419551

A Rainbow of Rooms

Esperanza's known interception rooms are named for colours, with five main rooms at the headquarters, 15 at the Fiscalía's regional 'sectional directorates' and a further 8 rooms for specialised analysis.





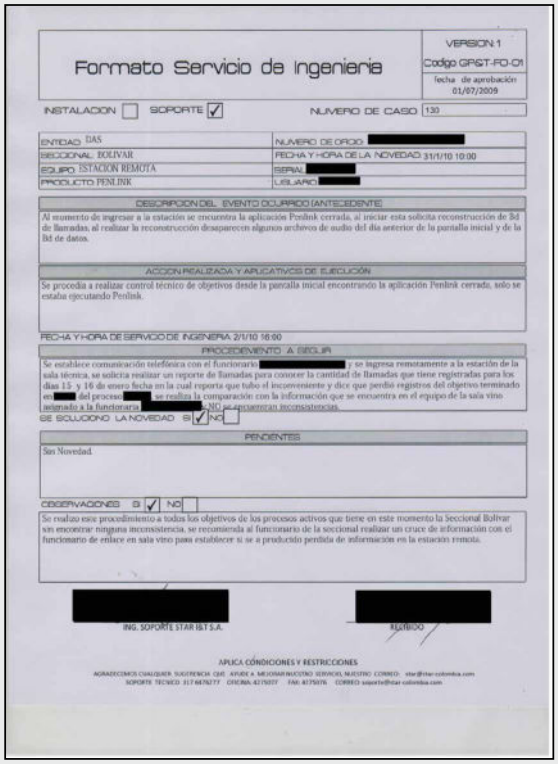
THE SAPPHIRE ROOM

The Sala Zafiro is one of the Bogotá monitoring and analysis rooms of the Fiscalía's Technical Investigations Corps (CTI) at Calle 18A, No.69 B.

Credit: PI September 2014

Esperanza has not always worked as planned. By mid-2009, connections between the rooms were routinely breaking down. Police and DAS officials submitted panicked messages requesting help. A summary of the over 20 different complaints from the FAS about problems accessing the intercpted data is included as an annex.

STAR engineers made dozens of visits to DAS monitoring rooms in 2009 and 2010 to fix problems and make improvements to the platforms on which data intercepted in the Esperanza system was analysed. Despite Esperanza's numerous known technical faults and the revelations about the DAS' illegal surveillance of journalists, activists and public officials that had been publicly known since 2008, Esperanza's capacities have been continually expanded.



Formato Servicio de Ingeniería

VERSION 1
Código GP&T-FO-01
fecha de aprobación 01/07/2009

INSTALACION ☐ SOPORTE ☑ NUMERO DE CASO 130

ENTIDAD DAS	NUMERO DE ORDO [redacted]
SECCIONAL BOLIVAR	FECHA Y HORA DE LA NOVEDAD 31/1/10 10:00
EQUIPO ESTACION REMOTA	SERIAL [redacted]
PRODUCTO PENLINK	USUARIO [redacted]

DESCRIPCION DEL EVENTO OCURRIDO (ANTECEDENTE)

Al momento de ingresar a la estación se encuentra la aplicación Penlink cerrada, al iniciar esta solicita reconstrucción de Bd de llamadas, al realizar la reconstrucción desaparecen algunos archivos de audio del día anterior de la pantalla inicial y de la Bd de datos.

ACCION REALIZADA Y APLICATIVOS DE EJECUCIÓN

Se procedia a realizar control técnico de objetivos desde la pantalla inicial encontrando la aplicación Penlink cerrada, solo se estaba ejecutando Penlink.

FECHA Y HORA DE SERVICIO DE INGENIERIA 2/1/10 16:00

PROCEDIMIENTO A EJECUTAR

Se establece comunicación telefónica con el funcionario [redacted] y se ingresa remotamente a la estación de la sala técnica, se solicita realizar un reporte de llamadas para conocer la cantidad de llamadas que tiene registradas para los días 15 y 16 de enero fecha en la cual reporta que tubo el inconveniente y dice que perdió registros del objetivo terminado en [redacted] del proceso [redacted] se realiza la comparación con la información que se encuentra en el equipo de la sala vino asignado a la funcionaria [redacted] NO se encuentran inconsistencias.

SE SOLUCIONO LA NOVEDAD SI ☑ NO ☐

PENDIENTES

Sin Novedad.

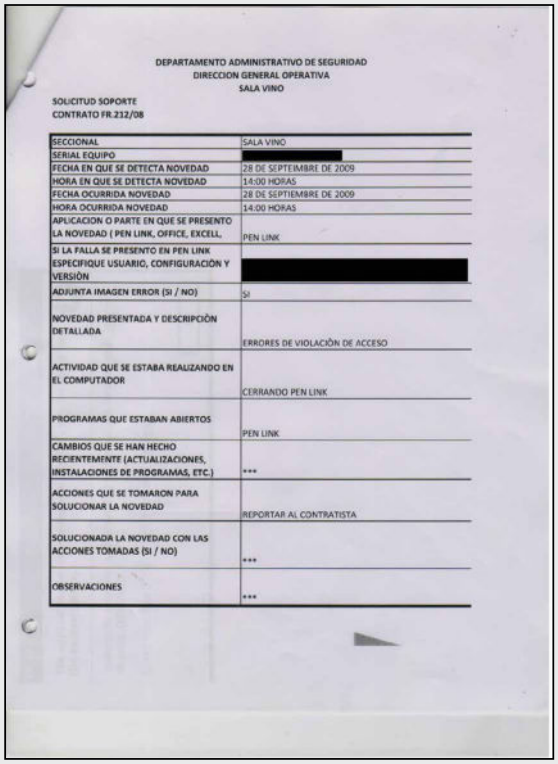
OBSERVACIONES SI ☑ NO ☐

Se realizo este procedimiento a todos los objetivos de los procesos activos que tiene en este momento la Seccional Bolivar sin encontrar ninguna inconsistencia, se recomienda al funcionario de la seccional realizar un cruce de información con el funcionario de enlace en sala vino para establecer si se a producido perdida de información en la estación remota.

[redacted] ING. SOPORTE STAR I&T S.A. [redacted] RECIBIDO

APLICA CONDICIONES Y RESTRICCIONES

AGRADECEMOS CUALQUIER SUGERENCIA QUE AYUDE A MEJORAR NUESTRO SERVICIO, NUESTRO CORREO: star@star-colombia.com
SOPORTE TECNICO 3174476377 OFICINA 4270377 FAX 4175076 CORREO soporte@star-colombia.com



DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD
DIRECCION GENERAL OPERATIVA
SALA VINO

SOLICITUD SOPORTE
CONTRATO FR.232/08

SECCIONAL	SALA VINO
SERIAL EQUIPO	[redacted]
FECHA EN QUE SE DETECTA NOVEDAD	28 DE SEPTEIMBRE DE 2009
HORA EN QUE SE DETECTA NOVEDAD	14:00 HORAS
FECHA OCURRIDA NOVEDAD	28 DE SEPTIEMBRE DE 2009
HORA OCURRIDA NOVEDAD	14:00 HORAS
APLICACION O PARTE EN QUE SE PRESENTO LA NOVEDAD (PEN LINK, OFFICE, EXCELL,	PEN LINK
SI LA FALLA SE PRESENTO EN PEN LINK ESPECIFIQUE USUARIO, CONFIGURACIÓN Y VERSIÓN	[redacted]
ADJUNTA IMAGEN ERROR (SI / NO)	SI
NOVEDAD PRESENTADA Y DESCRIPCIÓN DETALLADA	ERRORES DE VIOLACIÓN DE ACCESO
ACTIVIDAD QUE SE ESTABA REALIZANDO EN EL COMPUTADOR	CERRANDO PEN LINK
PROGRAMAS QUE ESTABAN ABIERTOS	PEN LINK
CAMBIOS QUE SE HAN HECHO RECIENTEMENTE (ACTUALIZACIONES, INSTALACIONES DE PROGRAMAS, ETC.)	***
ACCIONES QUE SE TOMARON PARA SOLUCIONAR LA NOVEDAD	REPORTAR AL CONTRATISTA
SOLUCIONADA LA NOVEDAD CON LAS ACCIONES TOMADAS (SI / NO)	***
OBSERVACIONES	***

TROUBLESHOOTING

Connections between Esperanza and three agencies' rooms routinely broke down.
For further error messages please see Annex: Error Messages

Today Esperanza still has its limits. The Police complained in 2010 that it was unable to intercept voicemail messages, Blackberry messages and communications over internet (IP-based communications).[28] These limitations are well known to law enforcement agencies. As far back as 2007, Esperanza's limitations provided justification for the initial acquisition of new technology with greater capacities, namely PUMA. In 2013, ongoing difficulties with Esperanza were used to justify PUMA's expansion: the police wanted an interception system based on a different technology provided by other companies.

28 "Acta de Comisión 06 del 24 de Agosto de 2010 Cámara", 24 August 2010, http://www.camara.gov.co/portal2011/gestor-documental/doc_download/153-acta-06-comision-primera

PUMA and Mass Interception

PUMA, the Single Monitoring and Analysis Platform (Plataforma Única de Monitoreo y Análisis) relies on technologies significantly more powerful and invasive than those of Esperanza. Esperanza is a 'switch' that requires a Fiscalía agent to remotely request and receive from the service provider information from a specific tapped line. Without this request, which is submitted electronically on the basis of an approval of a written request for interception, interception cannot be effected.

PUMA, by contrast, intercepts and stores potentially all communications transmitted on the high-volume cables that make up the backbone on which all Colombians rely to speak to and message each other. Its limitation is not the number of analysts available to 'task' service providers to send information, or quotas for interception per provider. PUMA's technology is only limited by the capacity of the storage of its monitoring centre servers and the capacity of the probes that are put on the backbone cables.

PUMA is linked directly to the service providers' network infrastructure by a probe that routes all data directly to the law enforcement monitoring facility without further facilitation from the service provider. PUMA is currently able to intercept, store and analyse massive amounts of phone traffic and is set to grow, and may also be made capable of intercepting internet traffic.

"There has been an exponential widening in the gap between criminals' technical capacity and ours," stated one DIJIN[29] official commenting on the acquisition of PUMA in 2014. PUMA was physically housed at the Police's Anti-Kidnapping and Anti-Extortion Directorate headquarters. Analysts of the Signals, Voice and Image Processing Group (Grupo de Procesamiento Señales, Voces e Imágenes) of DIJIN received the data at their main installation. In 2007, at its outset, PUMA had eight monitoring rooms spread across Colombia in its sectional divisions in Medellín, Bucaramanga, Cúcuta, Pereira, Villavicencio, Neiva, Cali and Barranquilla. From these rooms, analysts from the Sectional division of Criminal Investigation (SIJIN, under DIJIN) and the Unified Action Group for Personal Liberty (GAULA) would monitor intercepted calls.[30] Additionally, sometime between 2011 and 2013, a number of workstations for DIPOL agents were added.

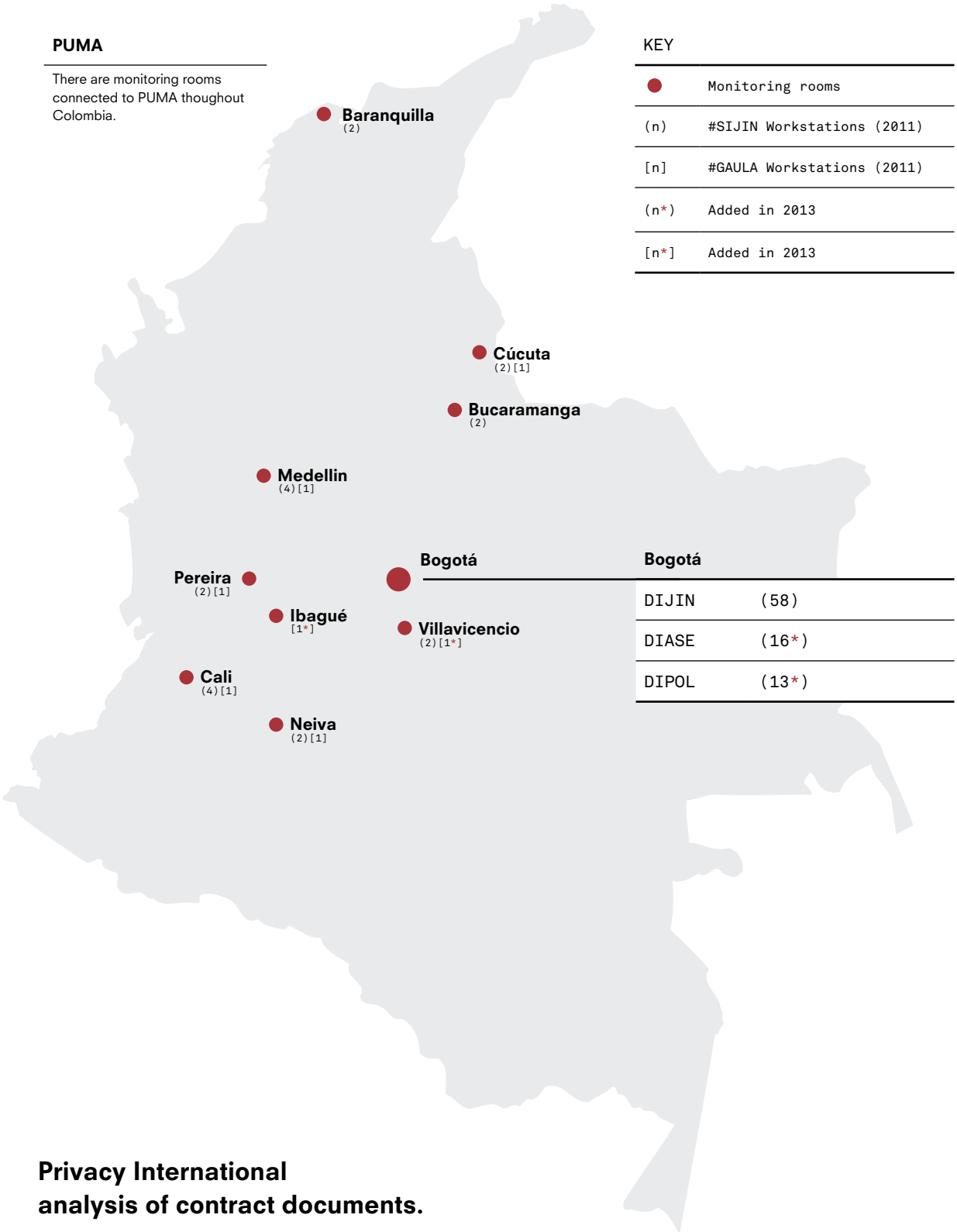
29 "Plan Estadístico de la Policía Nactional", 2008, http://www.policia.gov.co/portal/page/portal/HOME/Lineamientos/Tomo%205.1%20PLAN%20ESTADISTICO.pdf

30 "Resolución No 02049 del 15 Jun. 2007," Colombian National Police, 15 June 2007, http://www.policia.gov.co/portal/page/portal/INSTITUCION/normatividad/resoluciones/RESOLUCI%D3N%202049%20DIPOL%20%20150607.doc

Single Monitoring & Analysis Platform (PUMA)

PUMA

There are monitoring rooms connected to PUMA thoughout Colombia.



KEY	
●	Monitoring rooms
(n)	#SIJIN Workstations (2011)
[n]	#GAULA Workstations (2011)
(n*)	Added in 2013
[n*]	Added in 2013

Bogotá	
DIJIN	(58)
DIASE	(16*)
DIPOL	(13*)

Privacy International analysis of contract documents.

PUMA operated on patented technology from Israeli-American intelligence solutions company Verint Systems, primarily using the company's RELIANT monitoring centre platform.

After the Police concluded the initial contracts with Compañía Comercial Curacao de Colombia ('La Curacao'), the legal representative and only authorized distributor for Verint Systems in Colombia,[31] Verint engineers placed 16 'IP-PROBER'[32] probes on the trunk lines. Service providers knew of their existence and helped to install the connections but were not involved in their day-to-day operation, according to former Verint employees.

The probes intercept data and send it back to PUMA monitoring centres. La Curacao won subsequent contracts to install and maintain PUMA's hardware and software from 2008 to 2013.[33] La Curacao engineers were vetted by DIPOL[34] and maintained the monitoring centres' data centre, servers and data storage racks. They even updated administrator passwords on PUMA servers in 2011.[35]

In 2011, PUMA's monthly maintenance cost ran at 22 million pesos (around US$12,500).[36] It had grown to a total of 83 workstations, of which 58 were at the DIJIN headquarters in Bogotá. In 2013 the police announced a major plan to expand PUMA and make it the prime interception system of Colombia.

31 "Resolución No. 0589 del 18 Jun. 2013", Directorate of Administration and Finance, Colombia National Police, 18 June 2013.

32 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10124- 10", Directorate of Administration and Finance, Colombia National Police, 1 September 2010, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-351033

33 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10124- 10", Directorate of Administration and Finance, Colombia National Police,1 September 2010, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-351033

"Contrato de Compraventa Celebrado entre la Dirección de Investigación Criminal y la Firma Compañía Comercial Curacao de Colombia S.A.", Directorate of Administration and Finance, Colombia National Police, April 2008, https://www.contratos.gov.co/archivospuc1/C/116001000/07-2- 88996/C_PROCESO_07-2-88996_116001000_446982.pdf (archived)

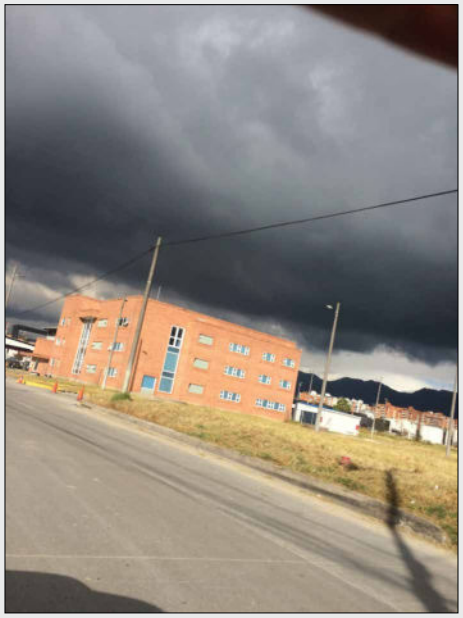
"Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Directorate of Administration and Finance, Colombia National Police, 31 August 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

34 "Contrato de Prestación de Servicios PN-DIRAF 06-7-10037- 13", Directorate of Administration and Finance, Colombia National Police, 23 June 2013, https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=13-12-1751484

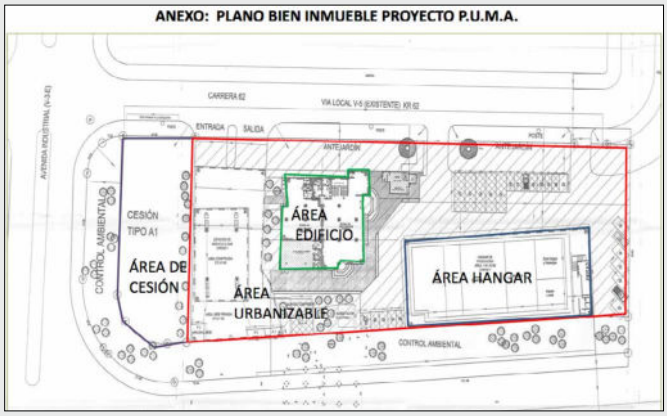
35 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Directorate of Administration and Finance, Colombia National Police, 31 August 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

36 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Directorate of Administration and Finance, Colombia National Police, 31 August 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

The Police allocated an unprecedented 50 billion pesos (US$ 28 million) to the project in January 2013.[37] Over half of this sum was earmarked for 'technical fortification' – the raw software and hardware needed to turn PUMA into a complete lawful interception system able to collect data and content of voice calls, VoIP, internet traffic, and social media over 12 of Colombia's telecommunications service providers – four voice and mobile data networks (Claro, Tigo, Avantel and Movistar) and eight internet service providers (Une, Telefonica, Emcali, Metrotel, ETB, Telebucaramanga, Telmex, EPM).



PUMA's headquarters formerly housed an industrial cleaning company. Left: On a Sunday in late September 2014, the hangar appeared open and it was relatively unguarded. Credit: Privacy International.
Below: Building plan of PUMA expansion



This time, however, the police broke with their usual interception supplier, Verint. Instead, they contracted with another Israeli company, NICE Systems, in consortium with the Colombian company Eagle Comercial SA.

Super-PUMA, as it became known, provided by NICE, was to provide the police with the ability to intercept 20,000 'objects', which may include targeted devices or lines, with the stated potential to scale up to 100,000 objects, although it is not clear on what timescale.

37 "Procedimiento: Formular y Evaluar Proyectos de Inversión, Proyecto: Fortalecimiento Plataforma Única de Monitoreo y Análisis Policía Nacional", National Police of Colombia, January 2013.

Super-PUMA also featured a monitoring module for ISP traffic and up to 700 workstations throughout the country.[38] Data would be intercepted by way of eight 'NiceTrack IP' probes that filter and extract huge quantities of data delivered simultaneously over highly loaded IP links. For the first time in the history of Colombia's known interception systems, the system would be able to intercept 4G data.

NICE-Eagle was also contracted to set up a mobile data centre that "concentrates all the infrastructure that supports the operational and administrative processes and has set a goal to cover voice and data communications." During this phase, NICE-Eagle was to oversee the migration of data from the Esperanza system to the new system. Finally, the updated PUMA was to include a system for the administration of judicial orders for voice and mobile data aimed at minimising the time and bureaucracy between warrant and retrieval.[39]

In 2014, during the second phase of PUMA's strengthening, NICE-Eagle was to focus on setting up the interception system for the eight internet service providers. The other focus of the second phase was to maintain the interception systems of the four telecoms providers and the data centre.

By the end of 2014, PUMA was supposed to have largely replaced the increasingly outdated Esperanza. However, its development has been stalled due to a disagreement between the Fiscalía and the Police, outlined in the conclusion of this report. PUMA is poised to become the most powerful and sophisticated – though not the first – mass communications monitoring system in Colombia.

38 "Asunto: Respuesta proposición N.04 de 2013", National Police of Colombia, 12 August 2013.

39 "Adquisición de Sistemas para el Fortalecimiento Tecnológico de la Plataforma Única de Monitoreo y Análisis (PUMA)", Administration and Finance Directorate, Ministry of Defence, 26 November 2013.

Beyond The Law

The Colombian legal framework provides a number of essential protections for the right to privacy, both in the text of the 1991 Constitution, and in the constitutional instrument (bloque de constitucionalidad) in accordance with Article 92 of the Colombian Constitution. This article incorporates Colombia's international human rights obligations into Colombian law and confers upon them the status of constitutional law, meaning they take precedence over statutory provisions.

Building on Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which Colombia is a signatory, which stipulates that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation," Article 15 of the 1991 Constitution provides that everyone has the right to personal and family privacy. It states:

> "Correspondence and other forms of private communication are inviolable. They may only be intercepted or recorded pursuant to a court order, following the formalities established by law."

The interception of communications is regulated by law, namely the Constitution and the Criminal Procedure Code. The Constitution empowers the Fiscalía to "[c]onduct searches, house visits, seizures and interceptions of communications" subject to judicial control (Article 250). The Criminal Procedure Code provides further details. It begins with a reiteration of the right to privacy, stating in Article 14:

> "Everyone has the right to respect for his/her privacy. No one shall be disturbed in his/her private life.
>
> No records, searches and seizures at home, residence or workplace can be made but by written warrant of the Attorney General or his/her delegate, in accordance with the forms and for the reasons previously defined in this code. In flagrante situations are considered excluded and others covered by the law.
>
> The same process is applicable when it is necessary to conduct a selective search in computerized, mechanized or any other form of database, which are not freely available, or when necessary to intercept communications.
>
> In these cases, within thirty-six (36) hours there shall be a respective

> hearing before the supervisory judge, in order to determine the formal and material legality of the action."

Article 235 of the Code stipulates the conditions under which the Attorney General's Office can order the interception of communications. The Article states:

> "The prosecutor may order, with the sole purpose of seeking probatory material and physical evidence, the interception, by tape-recording or similar, of telephone or radiotelephone communications or similar that use the electromagnetic spectrum, whose information have relevance for the purposes of the action. In this sense, the entities responsible for the technical operation of the respective interception are required to undertake it immediately after the notification of the warrant.
>
> In any case, the order shall be based in writing. Persons involved in these proceedings are obliged to keep the proper confidentiality. Under no circumstances the communications of the defending counsel shall be intercepted.
>
> The warrant will be in effect for a maximum of three (3) months, but may be extended for the same period, if in the opinion of the prosecutor the reasons that originated it persist."

The provision stipulates that the prosecutor may only lawfully order the interception of communications being transmitted via the electromagnetic spectrum ('EMS') (telephone, radio or fibre optic cable) for the sole purpose of seeking evidence. The order must be made in writing and is valid for three months.

In April 2013, a new Intelligence Law was adopted, stipulating that intelligence and counter-intelligence activities "include monitoring the electro-magnetic spectrum". Article 4 of the Law provides that information may only be obtained for a lawful purpose. Those purposes are: ensuring national security; sovereignty; territorial integrity; the security and defence of the nation; the protection of democratic institutions and the rights of Colombian residents and citizens; and the protection of natural resources and economic interests of the nation. Article 17 of the Law is entitled "Monitoring the Electromagnetic Spectrum and Intercepting Private Communications" and states:

> "Intelligence and counter-intelligence activities include monitoring the electromagnetic spectrum when this is duly established in operational orders or work assignments. Information gathered during such

> monitoring in the context of intelligence and counter-intelligence activities that does not serve to achieve the aims established in this Law shall be destroyed and may not be stored in intelligence or counter-intelligence databases. Monitoring does not constitute interception of communications.
>
> Intercepting private mobile or land-line telephone conversations, as well as private data communications shall be subject to the requirements established in Article 15 of the Constitution and the Criminal Procedure Code and may only be conducted in the context of legal proceedings."

The second paragraph states clearly that the interception of communications is not authorised by the Intelligence Law, but rather must only occur under the lawful authority of the Criminal Procedure Code, on a targeted basis, in accordance with the procedures stipulated in the Code. The provision, therefore, cannot be said to sanction the interception of communications by the intelligence or law enforcement agencies.[40]

The introduction of the law was accompanied by considerable criticism from civil society and public bodies. Because the Intelligence Law is a statutory law (ley estatutaria), a special class of laws that is superior to ordinary laws and that must pass by an absolute majority vote in Congress, it was reviewed by the Constitutional Court for compliance with the constitutional order (including with Colombia's international human rights obligations). The Intelligence Law received the assent of the Constitutional Court in early 2013.

In the course of the Constitutional Court's review, the Intelligence Law was subjected to sustained critique. The critique of the Ombudsman's Office (the Defensoría del Pueblo) went right to the heart of the legal and technical problems with the provision. In its submission to the Constitutional Court, the Ombudsman's Office remarked:

> "the expression 'monitoring does not constitute interception of communications'... is incompatible with the constitution given that this is understood as 'surveillance' or 'oversight' of the spectrum and it will therefore always involve communications. For this reason it constitutes a type of intervention, interception or interference that will fail to have judicial oversight (article 15 of the Constitution)." [41]

40 Nevertheless, there have been suggestions that the Intelligence Law may in some way authorise or cover the types of communications interceptions that various systems possessed by Colombian agencies – including PUMA and the IRS – are technically able to effect.

41 "Sentencia C 540/12 de la Corte Constitucional en la revisión del proyecto de ley de inteligencia y contrainteligencia", Constitutional Court of Colombia, 12 July 2012, http://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm

The Ombudsman's Office suggested that for the provision to be constitutional, it would need to be read such that monitoring could only be "done on communications without determining any specific person and using non-specified devices and numbers for a reasonable amount of time, no longer than strictly necessary to establish the scope of a legally authorised investigation or mission underway."

Civil society groups Dejusticia and Fundación para la Libertad de Prensa (Freedom of the Press Foundation) went further in their critique of the provision. They argued that there was no means for limiting electromagnetic spectrum "monitoring" in the way the Ombudsman's Office suggested. They explained that "sweeping the electromagnetic spectrum constitutes direct intervention in people's privacy. The lack of a judicial warrant offering legal certainty in this regard leaves individual citizens in uncertainty, fully unaware of the chance they may be under surveillance or that their personal affairs are being listened to by parties they have not authorised to do so [...]". They called for the provision to be declared unconstitutional.

The Constitutional Court's reasoning in determining the constitutionality of the provision is at best circular, and at worst factually and legally incorrect.

The Court begins by reiterating its previous declaration that the electromagnetic spectrum is "a strip of space around the Earth through which radio electric waves carrying sound or visual messages move," a statement which in itself contains factual inaccuracies (pictures do not move across the EMS). It found that the "monitoring" of the EMS consists of "conducting random, indiscriminate sweeps." This involves, the Court said:

> "incidental capturing of communications where circumstances that enable attacks to be avoided and risks to the Nation's defence and security to be avoided. Technically, it involves a sort of sweep of shadows, images and sounds represented in electromagnetic radiation and radio waves. Monitoring the electromagnetic spectrum could not involve surveillance of individuals. It does not involve selective or specific tracking of specifically considered individuals. To this extent, the monitoring of the electromagnetic spectrum as an impersonal abstract activity that cannot be confused with activities in a criminal investigation involving individuals and which is concrete [...]" (emphasis added).

The Court's decision rests on a belief that there is a means to "monitor" the spectrum that does not involve an interference with the privacy of communications. That is, that emails and text messages and phone calls carried upon the EMS can be filtered, analysed and monitored in a way which does not involve violating the integrity of the communication, and therefore the privacy of the person sending or receiving the communication.

Such a conclusion is not entirely incorrect, but it pertains to an extremely narrow set of activities. The only actions that could possibly "monitor" the EMS without interfering in any way with the privacy of communication would include heat detection tools, and direction-finding tools and antennae, for example. All other forms of EMS "monitoring" necessitate an interference (with a communication) of a type that means that it is not possible to conclude anything other than that the monitoring has resulted in the communication being intercepted.

The Court's reasoning is ultimately circular. "[M]onitoring the electromagnetic spectrum", it says, "cannot involve interception or registering private communications since this requires a "judicial warrant in the cases and with the formalities provided for by law.... Therefore, monitoring of the electromagnetic spectrum is limited by fundamental rights and subject to the system of checks and balances set forth in the Constitution (article 113). These rights cannot be violated under the pretext of conducting this activity."

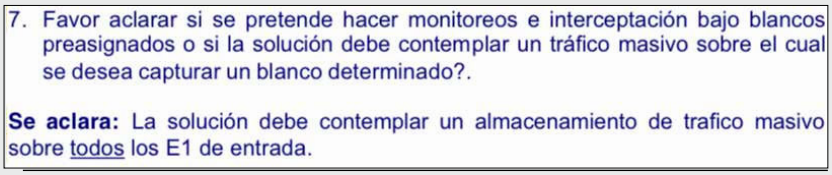
This is circular logic, purporting that the intelligence agencies's activities are not 'interception' simply because they are not empowered to conduct interception under the Constitution. Plainly, it is possible for legislators to draft unconstitutional laws. It is the court's role to assess the law's compliance with the constitutional order prior to the law coming into force, and to declare provisions constitutional or not.

In any event, even accepting the constitutional validity of the EMS provision, it is clear that the law only sanctions a narrow set of surveillance activities that do not amount to the interception of communications. That set of activities would not include the type of mass and passive monitoring that the technologies acquired by DIPOL, DAS and others would enable. Contracts and other confidential documentation obtained by Privacy International show that the surveillance tools purchased by these agencies provide access to essentially the same data on individuals as other interception platforms such as Esperanza, if not more.

Shadow System: DIPOL and The Integrated Recording System

Before PUMA, DIPOL established a mass interception system in 2005 – Colombia's first. That February, the police put out a call for tenders to provide the equipment necessary to monitor the newly developed (3G) technology mobile phones as part of the "Acquisition, Construction and Technological Development" of an Integrated Recording System (Sistema Integral de Grabación Digital, IRS).[42]

The IRS was conceived to go beyond the interception of preassigned targets (blancos preasignados) to collect 'massive' communications traffic across 16 trunk lines and generate new targets. As DIPOL clarified to companies bidding to provide this 'solution', "the solution should include mass storage of traffic over all input E1 lines" (emphasis in original).


7. Favor aclarar si se pretende hacer monitoreos e interceptación bajo blancos preasignados o si la solución debe contemplar un tráfico masivo sobre el cual se desea capturar un blanco determinado?.

Se aclara: La solución debe contemplar un almacenamiento de trafico masivo sobre todos los E1 de entrada.

"Respuesta observaciones: Contratación Directa No. 006 de 2005", Police Revolving Fund, Ministry of Defence, 25 February 2005."

A MASS SYSTEM

DIPOL sought to gather information on communications beyond known targets.

DIPOL required its Integral System to be completely passive.[43] This means that beyond the initial set-up within the service providers' architecture, DIPOL could monitor information flows without any further technical assistance from operators.

DIPOL turned to Verint and La Curacao to build its interception system. The first component, VANTAGE (acquired in June 2005), is marketed by Verint as a tool that

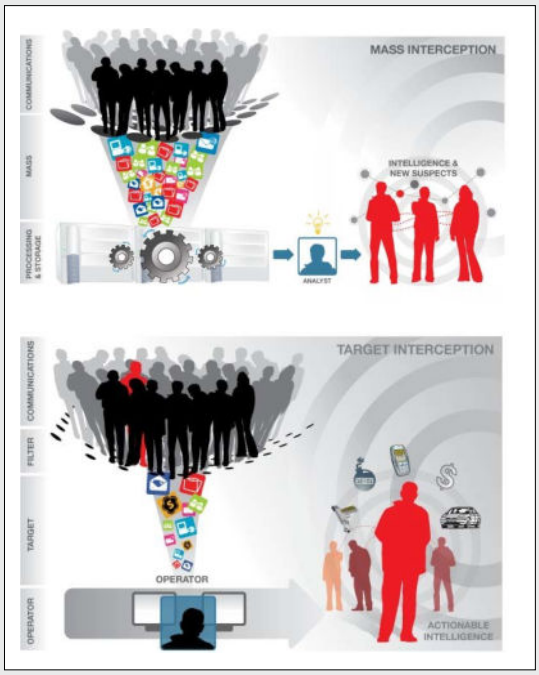
42 Adquisición construcción y desarrollo tecnológico – Equipo de Monitoreo de Telefonía Móvil Celular Nueva Tecnología – Sistema Integral de Grabación Digital – con Destino a la Policía Nacional". By 2007, Resolution 02049 cemented DIPOL's authority to conduct and coordinate information collection activities by monitoring the electromagnetic spectrum via its Intelligence Production Group.

43 Asunto; Respuesta observaciones, Adquisición construcción y desarrollo tecnológico – Equipo de Monitoreo de Telefonía Móvil Celular Nueva Tecnología – Sistema Integral de Grabación Digital – con Destino a la Policía Nacional", Police Revolving Fund, Ministry of Defence, 25 February 2005.

"helps expose unknown threats, regardless of how perpetrators communicate" [44] by intercepting, filtering and categorizing information in such a way that an analyst can search it for patterns as well as specific persons, numbers, servers, and other data of interest. In one example, VANTAGE was used by an intelligence agency in Eastern Europe to capture three million emails and 12 million webmails per day, storing the intercepts for 90 days. The number of probes in this example was the same as those purchased by Colombia's Police (16 probes),[45] though VANTAGE can be scaled up or down to suit the ambitions and the budget of the purchasing government.

In September 2005, DIPOL sought to acquire a "module for active monitoring of internet for ISP [internet service providers]." DIPOL chose Verint's solution, RELIANT – later favoured by DIJIN in its PUMA system. Like VANTAGE, it comes with monitoring centre capacity.

Verint engineers installed the relevant equipment, probes and all, imported from Israel directly by the Police and exempt from importation duties[46] in the switching centres of the service providers and connected it with DIPOL's monitoring room at its Boyacá



NEW TOOLS

DIPOL bought VANTAGE for US$ 575,000 (around 1.6 billion pesos) and RELIANT for around US$ 160,400 (372.5 million pesos). Together they form the core of a mass monitoring system that would intercept and store without warrant vast amount of communications traffic in Colombia.

44 "Vantage", Verint, 2015, https://web.archive.org/web/20140722151255/http://uk.verint.com/solutions/communications-cyber-intelligence/products/vantage/index

45 "Verint Security and Intelligence Management Solutions", Verint, November 2010, http://s3.documentcloud.org/documents/810401/1260-verint-product-description-security-and.pdf

46 "Ley 80 de 1993", Congress of the Republic of Colombia, 28 October 1993, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=304

Avenue headquarters in Bogotá, leaving La Curacao to maintain and troubleshoot the product. Analysts at its 20 workstations had, at least on paper, the capacity to record conversations of a selected target;[47] capture 100 million call data records per day and intercept 20 million SMS per day.[48] A further voice recognition capacity would generate call data automatically in a word processor form, to which analysts could manually add notes and a transcript or summary of the call. These are massive capacities that could be scaled up or down as required – for a price.

But did it work as intended? Police publicly deny that they currently[49] have the ability to tap internet traffic. Persons with direct experience of defence contracting confirm that the pressure to produce results – and the promise that 'better' technology will secure better results – led the Police to purchase equipment it did not really understand. Several individuals described the Verint system as a sort of white elephant. "He doesn't really know what he's buying" recalled one engineer after meeting with General Jairo Gordillo Rojas,[50] head of the police telematics unit, and his team. "I don't know [why they bought it] but it certainly was an opportunity that La Curacao saw. But I know that it doesn't work as well as they hoped it would."

"Each agency built their own intelligence system," says a police telematics expert. "The intelligence systems investigate themselves as well and feel a high pressure to produce positive outputs. Naturally, there is a competition." Each agency has a budget and there is no integration of the budgets, he explained. So combined with the pressure to produce intelligence, agencies buy equipment that is proposed to them with little close scrutiny into what they are buying.

The DIPOL system was separate from Esperanza. In 2005, at the development of the system, companies interested in tendering for the contract submitted questions to the contracting authority. "Will the system be connected to the Esperanza switch? If so, have you already made the high-level arrangements to make the connection with the Fiscalía?" DIPOL was clear in response: "in no place are we talking about applying this development to the Esperanza system. The bidders must limit themselves to the required specifications."

Again they asked, "for the E1 trunk probes, how many are for fixed lines and how many for mobile telephony? For the latter, do they come from the Esperanza switch?" Again, DIPOL was clear that the system would be independent: "No, they don't come from the Esperanza switch". [50]

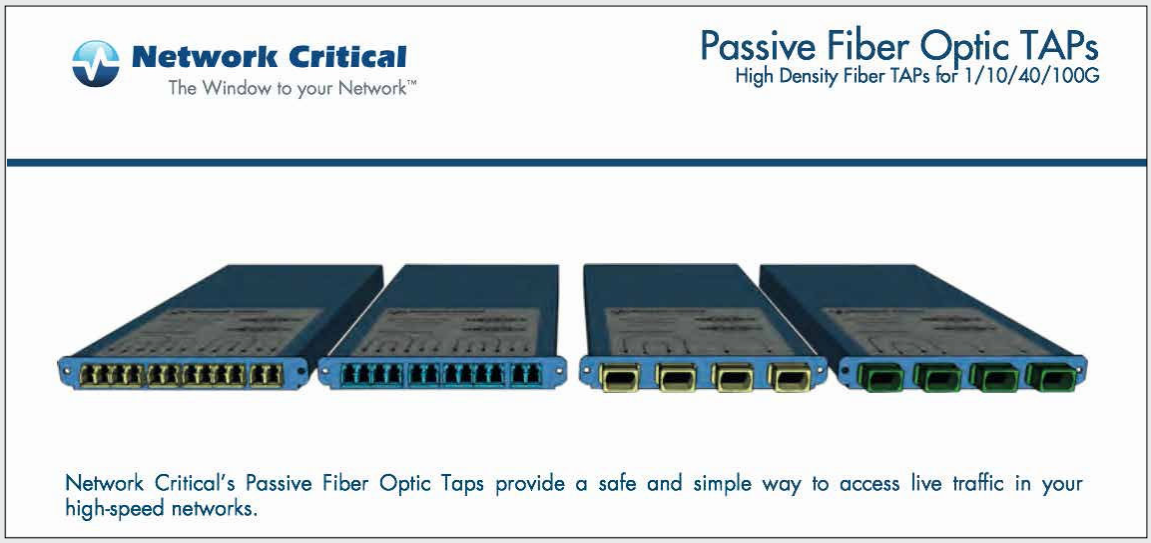
47 "Respuesta observaciones: Contratación Directa No. 006 de 2005", Police Revolving Fund, Ministry of Defence, 25 February 2005.

48 "Contrato de Compraventa No. 034 de 2005, celebrado entre el Fondo Rotatorio de la Policia y la Firma Compañía Comercial Curacao de Colombia", Police Revolving Fund, Ministry of Defence, 17 June 2005.

49 As of September 2014.

50 General Gordillo was summoned for questioning in May 2014 over alleged wiretapping and surveillance of two journalists. "Fiscalía realiza interrogatorios por supuestas 'chuzadas'", Noticias RCN, 9 May 2014, http://www.noticiasrcn.com/nacional-pais/fiscalia-realiza-interrogatorios-supuestas-chuzadas

The relationship between DIPOL and the Fiscalía under this system is unclear. Technical specifications for the Integrated Recording System (IRS) state that it would not receive information from Esperanza, and the system appears to passively receive all data passing through the respective E1 lines. However in 2006, the then manager of the Esperanza system Vladimir Floréz Beltran authenticated certificates from the bidding firms.[52] At the time, the Police was expanding the system's capacities, again using Verint technology provided by its Colombian representative, La Curacao.



TAP IT ALL

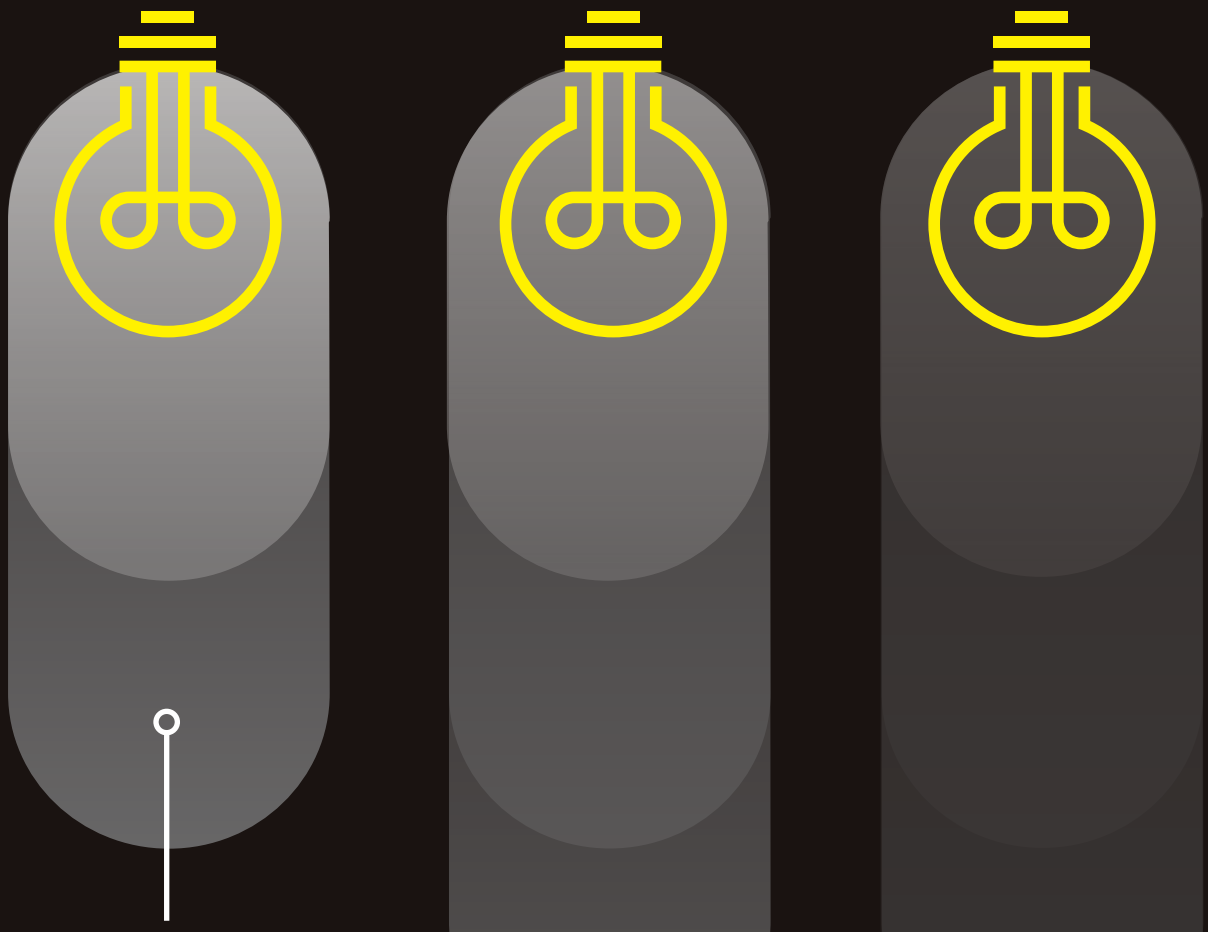
DIPOL also purchased taps for fibre optic cables in 2009. A fibre optic cable is a bundle of threads that can transmit signals modulated onto light waves, unlike traditional copper cables on which the signal is transmitted by an electric voltage. Whereas Esperanza needed the compliance of the telecommunications operator to manipulate its mobile switching centre in each case where a phone call or record was requested (thereby ensuring at least on paper that there was a formal request and justification made), DIPOL's surveillance system has been configured to connect to the DIPOL monitoring centre and feed it massive amounts of traffic. Further detail is contained in Privacy International's report Demand / Supply: Exposing the Surveillance Industry in Colombia. DIPOL was delivered three "Slimline Fiber Optic Passive TAP[s]" of various dimensions. Slimline is a trademark of the UK-headquartered company NetworkCritical which provides network monitoring technologies.[53]

51 "Adenda 02: Adquisición Sistema Integral de Grabación Digital", Directorate of Administration and Finance, Colombia National Police, 2007.

52 "Adjudicación de la Contratación Directa No. 055 de 2006", Police Revolving Fund, Ministry of Defence, 29 November 2006, https://www.contratos.gov.co/archivospuc1/ADA/115001003/06-2-16355/ADA_PROCESO_06-2-16355_115001003_31717.pdf (archived)

53 "Passive Fiber Optic TAPs High Density Fiber TAPs for 1/10/40/100G", Network Critical, 2015, http://www.networkcritical.com/NetworkCritical/media/resource-library/product-datasheets/Fiber-Optic-Break-TAP-Datasheet.pdf

Communications Surveillance Systems



Esperanza System

Data intercepted **from targeted lines** following Fiscalía request with active TSP collaboration. Accessed by DIJIN law enforcement and formerly DAS with warrant.

PUMA

Data intercepted **in bulk** from telecoms backbone without TSP collaboration beyond set-up. Technology managed by DIJIN (law enforcement), administrative oversight by Fiscalía.

Integrated Recording System

Data intercepted **in bulk** from telecoms backbone without service providers collaboration beyond set-up. Technically managed by DIPOL (intelligence). **No clear oversight.**

Tactical Tools

Tactical[54] interception technologies feature in a number of different Colombian agencies' surveillance arsenals.

While building its interception system, DIPOL purchased mobile monitoring equipment for identification and/or interception of targets in known locations. This technology is colloquially known as an 'IMSI catcher'.

An IMSI catcher transmits a strong wireless signal that entices nearby phones to connect to it, and can be retrofitted with location monitoring technologies that determine the location of a target to within one metre. These devices could be directed to target a particular individual's device by, for example, being aimed at his or her workplace. They can also be used to identify unknown persons attending demonstrations and other gatherings because many mobile phones will connect to the IMSI catcher and transmit identifying information.

DIPOL bought a 'Laguna' IMSI catcher manufactured by New Zealand technology company Spectra Group. It paid US$ 474,000 (COP$ 970.8 million) in September 2005 to the Colombian firm Maicrotel Ltd.

The Laguna interceptor is capable of targeting a relatively small amount of traffic at a fixed distance of up to 500 meters. Among the data that the Spectra equipment can record is a phone's unique identifying records. To do so does not require an analyst to actively choose which numbers to capture: "The identification of the presence of the target in an area under control and revealing their unknown identifiers is done in an automatic way with the help of special mobile phones included in the system".[55] The equipment stores the intercepted information in digital format on hard disks that could then be brought back and plugged in to the DIPOL's monitoring centre for analysis. This means that potentially all data in a particular area can be intercepted when an IMSI catcher is deployed, even if DIPOL might only intend to target a

54 We use the term 'tactical' to refer to interception technologies where the communications data and content are taken directly from the device or by signals emitted by the device, rather than from the network architecture from the service provider.

55 "Contrato de Compraventa No. 152 de 2005, Adquisición construcción y desarrollo tecnológico Equipo de Monitoreo de Telefonía Celular para Protocolo GSM con Destino a la Policía Nacional", Police Revolving Fund, Ministry of Defence, 30 September 2005.

specific building or individual.[56]

In addition, the Colombian police acquired technology from Italian company Hacking Team. The company's Remote Control System (RCS) can be used to hijack computer and mobile devices while remaining undetectable to users. By infecting a target's device, often through the use of "exploits", the RCS suite can capture data on a target's device, remotely switch on and off webcams and microphones, copy files and typed passwords. In 2014, Hacking Team had a Colombia-based field engineer and an active contract with the Colombian police. The Colombian government's use of offensive malware Hacking Team products had been suspected since researchers at the Citizen Lab identified a command and control server for the RCS suite in the country.[57]

56 Maicrotel and Star won a US$ 466,666 (COP$1.196 billion) contract in November 2006 for more mobile phone monitoring equipment, and was maintaining this equipment throughout 2009. Originally, Maicrotel Ltda in a temporary union with Star Colombia won the contract. Following a review by the tenders committee, the GSM Cellular Technology Monitoring Equipment component of the project was declared void. Eagle won the contract on appeal when several of its competitors renounced their bids none of its competitors showed up for the hearing. Its rival Eagle also won a contract (for COP$ 1.228 billion, approximately US$ 610,700) in December 2006 and for COP$329 million in December 2007. Technically, this contract was won under another bidding process but for essentially the same type of product, GSM monitoring equipment. Eagle would later win a major contract for the revamp of the DIJIN's PUMA platform.

57 "Mapping Hacking Team's "Untraceable" Spyware", The Citizen Lab, 17 February 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

DIPOL and The Silicon Valley Surveillance Company



Palantir

Pilot Proposal to DIPOL

THE PALANTIR PLATFORM

Prepared for:

[redacted]

ORACLE Colombia | Calle 100 # 13 -21 Piso 15 Bogotá

Prepared by:

Palantir Technologies Inc.
http://www.palantir.com
+1 650-815-0200

PALANTIR POC: [redacted]
Tel. +1 571 419 4226

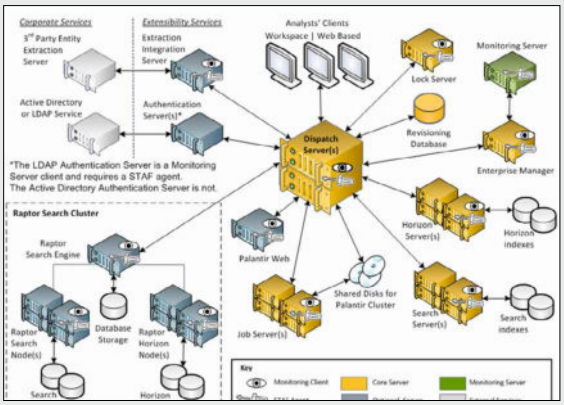
100 Hamilton Ave.
Suite 300
Palo Alto, CA 94301

1660 International Dr.
Suite 800
McLean, VA 21022

Copyright © 2012 Palantir Technologies Inc. All rights reserved. The information herein contains trade secrets and commercial or financial information which is privileged and confidential within the meaning of all relevant laws. This information shall not be disclosed without the prior written approval of Palantir Technologies. The data subject to this restriction are contained in all sheets of this proposal.

PALO ALTO	MCLEAN, VA	NEW YORK, NY	LONDON, U.K.	DELHI, INDIA	CANBERRA, AUSTRALIA
100 Hamilton Ave.	1660 International Dr.	15 Little West 12th St.	53 Chandos Pl.	Suite 8.07, 4th Floor, B Wing	Level 5, 7 London Circuit
Suite 300	Suite 800	5th Floor	Covent Garden	Statesman House Building	Canberra ACT 2601
Palo Alto, CA 94301	McLean, VA 21022	New York, NY 10014	London WC2N 4HS	Barakhamba Road	Australia
(650) 815 0200	(650) 815 0333	(646) 524 5667	+44 (207) 812 7380	New Delhi – 110001, India	+61 2 6169 4000
				+91 98 7356 5744	





Palantir proposed to set up an Integrated Intelligence Platform for DIPOL over six months in 2012. The new system would expand the existing Oracle-based intelligence platform and integrate ten police databases. Palantir is designed for the analysis of both open source information that can be scraped from the internet as well as data received from monitoring centre servers.

In 2012, DIPOL recognised that they required a platform or system to more effectively process the vast quantities of information that they were receiving. That year the Police invited tenders for a contract to provide such a platform. One of the companies that tendered for the contract was US data analysis and visualization giant Palantir. Palantir proposed an Integrated Intelligence Platform 'SI3' to DIPOL. Oracle had tried to independently pitch their own analysis solution in November 2011 before joining up with Palantir and STAR to propose a solution that would use both Palantir and Oracle technology, according to a powerpoint presentation contained in the annex.

Palantir got its initial foothold in the data visualization and analysis market with an investment from In-Q-Tel, a nonprofit venture capital firm established by the US Central Intelligence Agency (CIA).[58] The US army uses a version of Palantir software that combines drone footage with ground sensors and biometric scanners in military operations. [59]

At a cost of US$ 1.5 million, Palantir proposed a system that would allow DIPOL to ingest, categorize, tag, filter and otherwise make sense of data, mostly from internal sources with the option to include data from a certain number of external sources, for example, open-source intelligence sources such as Facebook and Twitter. Among the internal sources that Palantir proposed to integrate with the data obtained from open source intelligence were ten police databases.

In its tender, Palantir proposed to train 30 analysts and proposed to integrate Colombia's various police databases, including Oracle-based 'SI2', which hosts much of the information DIPOL recives. Images video and biometric data gained, for example through physical surveillance or by other more routine means would also, according to the tender, be added to any file. Palantir made clear that with its platform it is possible to map out the connections between datasets, and individuals, with the possibility to categorise and analyse both information and individuals.

"Palantir is a complete product suite designed to leverage DIPOL's existing information repositories and analyze data at the strategic, operational and tactical levels"

2012 Palantir proposal

While products like Palantir's are powerful tools in the fight against crime and terrorism, their use can threaten Colombians' constitutionally protected right to privacy. Palantir's algorithmic search engine is designed for an 'enormous data scale', which means

58 "Palantir Technologies", In-Q-Tel, 2015, https://www.iqt.org/iqt_portfolio/palantir-technologies/

59 "Special Forces, Marines Embrace Palantir Software", Defense Tech, 1 July 2013, http://defensetech.org/2013/07/01/special-forces-marines-embrace-palantir-software/

it can sift through millions of Colombians' data, including communications data, to isolate persons of interest based on search terms that are determined by the authorities. Palantir's system does have an internal audit function, meaning that analysts can be accorded different access privileges. Yet this audit function relies on the willingness of the very authorities seeking the information (in this case, DIPOL) to administer the platform properly, and, where appropriate, control it and their own powers.

Palantir said in response to Privacy International that although the company was part of a proposal in 2012, it did not progress past the proposal stage.

DAS: Network Probes and Tactical Interception

While DIPOL was developing 'monitoring' systems that intercept vast amounts of data apparently without any warrant, DAS was also quietly maintaining its own taps on telecommunications infrastructure. This raises the question about whether the interceptions published by Semana in early 2009 were indeed an abuse of Esperanza, as alleged, or if DAS was conducting its interceptions separately using mass automated interception technology.

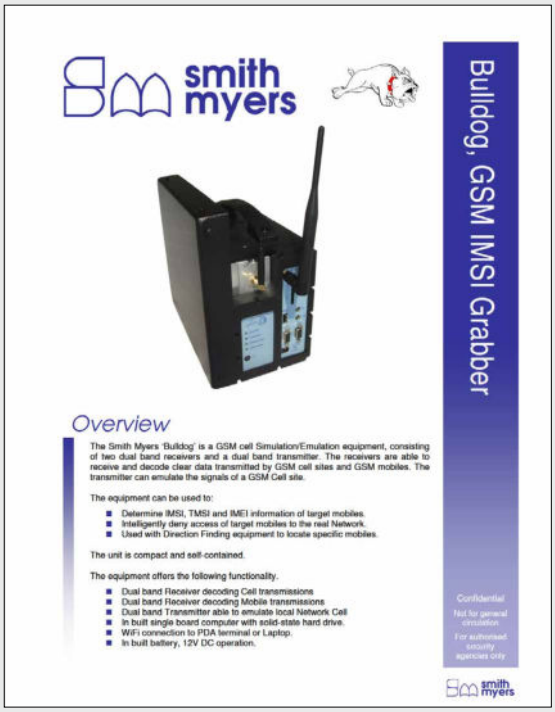
DAS had at least one monitoring centre and one internet probe. As late as August 2011, when DAS was being investigated for illegal interceptions and two months before it was formally dissolved, DAS paid for La Curacao to "ensure the full functioning and integrity of the solution system of information analysis of internet browsing information RELIANT of Verint Systems".[60] This included maintaining the "tactical probe in whatever location in the country where it is operating" suggesting that it was a probe that could be removed and reinserted to tap cables as necessary.

Was this probe and monitoring centre separate from Esperanza? DAS did have a monitoring room linked to Esperanza, the famous Sala Vino, where analysts received intercepted calls. But nowhere in the technical annex to a maintenance contract between DAS and STAR for Sala Vino, reproduced here, is there any mention made of the Verint probe. Nor is there any mention of Verint or its technology in the dozens of documents Privacy International has collected related to Esperanza. While STAR was responsible for maintaining and fixing various technical problems with the platforms of the Fiscalía-managed Esperanza, La Curacao maintained the probes and monitoring rooms of DIPOL and DAS that used technology from Verint.

STAR and La Curacao are two competitors in a saturated surveillance technology market who regularly bid against each other for contracts. These providers' technologies would have been generally incompatible or, at best, minimally compatible in order to ensure that their clients would have less incentive to use other providers. The incompatibility of Verint's solution with that provided by Esperanza would emerge later, in 2014, as one of the main reasons that the implementation of the PUMA system was stalled.

60 "Contrato de Prestación de Servicios de 2011, Celebrado entre el Fondo Rotario del Departamento Administrativo de Seguridad DAS Y Compañía Comercial Curacao de Colombia S.A.", Administrative Security Department Revolving Fund, 22 August 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-620217

DAS was also in the market for targeted tapping and forensic analysis tools. This includes location-based monitoring of calls, the 'IMSI catchers' discussed above. In May 2010, DAS reviewed quotes for British company Smith Myers' products, Nesie and Bulldog. Nesie is an IMSI catcher – similar to Spectra's 'Laguna' product that was sold to DIPOL. An analyst could also remotely operate the Nesie via an IP link.





NESIE AND BULLDOG

These mobile surveillance devices can locate and capture live phone traffic from a fixed distance; DAS looked to buy such products in 2010.

DAS also purchased 'mobile forensic units' sometime before 2010. These were work stations that could be used to copy and analyse targets' computers, phones and other devices for suspicious material and produce evidence-quality copies of it. DAS agents would have obtained these devices and fed them into the computers, ripped a copy, and taken it with them back to a fixed station[61] – possibly even their own monitoring centre.

61 DAS was originally willing to pay over COP$641 million for this. In December 2007, DAS held a hearing about the bid that was ultimately cancelled in December 2006 when no bidder was able to provide all the necessary components to the system.

A December 2010 maintenance contract[62] of this equipment showed that the DAS acquired it from La Curacao. The system used Forensic Toolkit (FTK), a computer forensics software made by US-based AccessData. That software allows an analyst to "preview a target's machine from across the network to determine relevancy prior to acquisition, but ... also acquire and fully analyze the data on the system, including the system's RAM."[63] The analysts could forensically analyse live data (system memory, logical volumes, physical devices) on a remote device from the analyst's system. Using this equipment, a minimum of 15 agents principally based in Bogotá were able to obtain the devices' passwords and analyse all emails and communications contained on the seized device.[64]

In September 2009, the DAS stated that the interceptions published by Semana "were not made from any mobile monitoring equipment of the Administrative Department of Security. ...In addition, these devices are controlled from February 22 as a preventive measure."[65] The US Congress also banned the DAS from receiving funds under various State Department schemes in 2010.[66] STAR engineers maintained technical equipment of the Sala Vino and other monitoring rooms linked to Esperanza elsewhere in Colombia throughout 2010 and DAS were contracting to buy further mobile surveillance units. Even if the particular devices DAS Director Felipe Muñoz Gómez referred to were 'under control' it is clear that DAS tapping did not stop, despite the investigations and the scandals.[67]

62 In an interesting indication of cooperation across Police and DAS, the supervisor of the project would be the Coordinator of the Technical Controls group of DIJIN.

63 "AccessData Releases Forensic Toolkit® 3.0", AccessData, 22 September 2009, https://ad-pdf.s3.amazonaws.com/FTK3_press_release.pdf

64 "Acta de Audiencia Pública de Presiciones del Contenido y Alcance del Pliego de Condiciones de la Licitación Pública No. 31 FR DE 2007", Departamento Administrativo de Seguridad, 5 December 2007, http://www.contratos.gov.co/archivospuc1/AAACL/106002000/07-1-28155/AAACL_PROCESO_07-1-28155_106002000_402105.pdf (archived)

65 "Comunicado No. 346", Departamento Administrativo de Seguridad, 21 September 2009, http://historico.presidencia.gov.co/comunicados/2009/septiembre/346.html

66 Consolidated Appropriations Act, 2010", US Congress, 30 September 2010, http://www.gpo.gov/fdsys/pkg/BILLS-111hr3288enr/pdf/BILLS-111hr3288enr.pdf

67 Since its dissolution, a new intelligence agency, the DNI, has been inaugurated about which little is publicly known. "Consulta de archivos de inteligencia del DAS, bajo control de la DNI", El Tiempo, 16 July 2014, http://www.eltiempo.com/politica/justicia/consulta-de-archivos-del-das-quedan-en-manos-de-la-dni/14256535

ANEXO No. 1

FICHA TECNICA

DESCRIPCION DEL SERVICIO DE MANTENIMIENTO

Preventivo y correctivo del equipamiento tecnológico de la Sala Vino y las estaciones remotas de las 27 seccionales del D.A.S, mediante la ayuda y el diagnostico de las fallas con visitas en sitio y de forma remota, incluyéndose: todos los costos de operación, suministro de repuestos, mano de obra con ingenieros y técnicos especializados, transporte y envió de equipos, impuestos y seguros.

El contratista procesará hoja de vida técnica para los equipos en funcionamiento en la Sala Vino y las 27 estaciones remotas de las Seccionales, evaluando el estado de funcionamiento, administración del equipo, herramientas del sistema configuración de software, hardware y redes, recursos disponibles de almacenamiento, servicios y aplicaciones, visor de sucesos y análisis de virus.

El Proponente examinará todos los requerimientos a través visitas técnicas a las instalaciones del DAS y, listado de los inventarios de Paloquemao y las estaciones remotas, de manera tal que pueda garantizar el cumplimiento del objeto del contrato. Igualmente, el oferente debe garantizar la seguridad y reserva de la información suministrada por el DAS sobre inventarios, configuración, hardware, software, redes y administración para la prestación de los servicios de mantenimiento.

ESPECIFICACIONES TECNICAS:

1. **ASISTENCIA DE DIAGNOSTICO PERMANENTE PARA SOLUCIONAR INCONVENIETNES EN TIEMPO REAL Y EN LINEA.**
   - Cobertura de servicio 24 horas por 7 días a la semana por 365 días al año, durante la vigencia del contrato, con una periodicidad de una visita mensual al equipamiento tecnológico de la Sala Vino, común tiempo de respuesta a la solicitud de la asistencia de dos (2) horas siguientes para el soporte en línea de manera física o mediante la comunicación remota segura a través de túnel de encripcion vía VPN (Red Privada Virtual) con las estaciones remotas de las seccionales
   - Asistencia con ingeniero especializado para la revisión, diagnostico y mantenimiento preventivo y correctivo para software, equipos y comunicaciones, asimismo, actualización de licencias software y hardware, instalación de parches Lincoln y Penlink , Windows , antivirus y NetOp, garantizando la operatividad del sistema de forma satisfactoria.

THE SALA VINO

Engineers from STAR maintained technical equipment of the DAS' famous interception room throughout the interceptions scandal and until its dissolution.

Legal and Technical Controls

The recent concern over the expansion of PUMA is only one chapter in what is a long story of illegal surveillance in Colombia. Various state agencies competing for independent interceptions powers have developed powerful and overlapping mass surveillance programmes without sufficient legal safeguards.

Institutional rivalry is partly to blame for the disjointed systems, although the reasons offered for these rivalries differ. A former DIJIN investigator informed Privacy International that Fiscalía's own investigators get priority in using up the interception quotas of each service provider connected to Esperanza system, so that the DAS and DIJIN investigators are limited in the number of interceptions they can request.

Yet each agency is under the same pressure to get more and more information in order to produce investigative results. Asked whether, despite the legal framework, it was nonetheless technically possible for the Police to carry out their own interceptions, the investigator said "all DIJIN interceptions go through Esperanza, otherwise it would be illegal."

"PUMA is a system that adapts remote stations that are interconnected to the Esperanza system", stated one DIJIN official when asked by Privacy International. He added "Esperanza is behind. We need to upgrade but the Prosecutor's office doesn't get the information right, or the right technology. We [DIJIN] can't upgrade because communication is broken [between the Fiscalía and Police]". The frustrating element, the police official said, is that, while the police control the wires and taps, the Fiscalía has to administer [programar] them. "We are subordinated to the administrative control of the Fiscalía office... PUMA is subordinated and controlled by Esperanza. Nothing is activated if not technically authorized by Esperanza."

Evidence set out in this report shows that interceptions can still be effected outside of the Esperanza system. While DIJIN must still submit interception requests for the Fiscalía's sign-off for its actions to be legal,[68] the Fiscalía's control is primarily administrative and legal in nature. DIJIN still has independent technical capacity to receive and store intercepted communications data from service provider networks as the Verint and now NICE technologies are designed to do.

In response to questions from a parliamentary committee about the future relationship between PUMA and the Esperanza System, the Director General of the Police José Roberto León Riaño stated that "the National Police exercises permanent functions of judicial police...it is one of the authorities that is competent to technically

68 "Asunto: Respuesta proposición N.04 de 2013", National Police of Colombia, 12 August 2013.

operate the interceptions. Consequently, it has the institutional autonomy to acquire and administer the technological developments that will permit it to effectively accomplish its constitutional and legal mandate" (emphasis added).[69]

With such a powerful passive surveillance system, the risk that illegal interceptions could reoccur is high unless there are strong technical as well legal safeguards in place. In 2010, the Fiscalía reported that its own investigators' phone communications were intercepted on the basis of false reports filed by two agents of the National Police and others of the CTI.[70] In 2013, former investigator of the Fiscalía's technical investigations unit and a number of police officers were found guilty of illegally intercepting former supreme court magistrate Iván Velásquez's communications. And this year, key files related to the DAS interceptions have disappeared off of the national archive's servers.[71]

Whether communications surveillance can be effectively regulated in the current framework is doubtful. Privacy International contacted several of the companies selling surveillance technology cited in this report about their roles in these systems.[72]

69 "Asunto: Respuesta proposición N.04 de 2013", National Police of Colombia, 12 August 2013.

70 Micrófonos ocultos, seguimientos e interceptaciones ilegales", Huellas, Fiscalía General de la Nacion, August 2010, http://www.fiscalia.gov.co/en/wp-content/uploads/2012/02/huellas-71.pdf

71 Evidence in Colombia's intelligence agency wiretapping scandal gone missing", Colombia Reports, 19 July 2014, http://colombiareports.co/evidence-colombias-intelligence-agency-wiretapping-scandal-disappeared/

72 The legal representative of the NICE-Eagle union denied having specific knowledge about the PUMA expansion contract when questioned even after it was published in 2013. Questioned specifically on wiretapping in 2011, Eagle's director Archimedes Bonilla Vega stated: "I provide equipment, but have no obligation or ability to establish whether it is being misused by them; it is the responsibility of each officer, if that were going on." "Contratos por más de US 35 millones para renovar salas de interceptación", Radio Caracol, 25 April 2014, http://www.caracol.com.co/noticias/judiciales/contratos-por-mas-de-us-35-millones-para-renovar-salas-de-interceptacion/20140425/nota/2194095.aspx

A New Phase of Chuzadas

What is PUMA's future? The project ground to a halt in August 2014, when the Attorney General, Eduardo Montealegre, warned that the project could not continue without bringing it further under the Fiscalía's control. He publicly warned against the "indiscriminate use of interception as an investigative tool in cases where the invasion of fundamental rights is not even necessary in the fight against crime.".[73] On this, Montealegre is adamant: "No other state agency (other than the Fiscalía) is empowered to order interception of communications or manage the equipment used for this" (emphasis added). PUMA equipment was reported to be in cardboard boxes at the site seen by Privacy International,[74] as a commission of police and Fiscalía officials determine its future. Nevertheless, several new contracts have been settled to set up rooms for PUMA in regional police offices including in Bucaramanga[75] and Villavicencio.[76]

Whether the Fiscalía is aware of just how extensive the 'monitoring' capacities of the police actually are, in light of the less-than-successful rollout of super-PUMA, is unclear and worrying for the privacy rights of Colombia's citizens.

Privacy International spoke to confirmed former targets of DAS surveillance and persons who strongly believe that they are still targeted by state electronic surveillance about the PUMA system.

"Beyond what's publicly available, I don't have more information on PUMA. My opinion is that PUMA affects fundamental rights. The use of this system does not respect human rights," says Reinaldo Villalba of CCAJAR, the Jose Alvear Restrepo Lawyers' Collective. CCAJAR was specifically targeted by DAS as part of a campaign of delegitimisation codenamed Transmilenio. DAS documents retrieved during the 2009 scandal contain detailed descriptions of CCAJAR employees' and families' movements, lists of their phone contacts and records of the DAS' attempts to link phone numbers with CCAJAR members. Reinaldo Villalba explains: "We

73 Fiscalía le dice 'no' a sistema de interceptación 'Puma' de la Policía", El Tiempo, 30 August 2014, http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/14462092

74 In September 2014.

75 Mantenimiento, Adquación y Dotación de la Instalaciones para el Fortalecimiento e Implementación de la Plataforma Única de Monitoreo y Análisis de la Región No. 5 Sala PUMA y Cubierta de las Instalaciones del Comando de la Policía Metropolitana de Bucaramanga", Bucaramanga Metropolitan Police, October 2014, https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-1-127391

76 Mantenimiento, Adquación y Dotación de la Instalaciones para el Fortalecimiento e Implementación de la Plataforma Única de Monitoreo y Análisis de la Regiónal No. 7 'SALA PUMA'", Meta Police, October 2014, https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-11-3000746

were certain we were being spied on... from the beginning. But what we didn't know concretely were the dimensions of the persecution. In 2009 we were truly surprised to see the thousands of files seized from the DAS, an intelligence agency that reports directly to the President of the Republic, that revealed the detailed persecution of which we were victims. They had information about each meeting we had and every person we met abroad. The persecution extended to our families, our children even minors."

Reinaldo reports that CCAJAR was tipped off about communications surveillance at various points.

"A person arrived here who I knew, she told me 'Reinaldo, I have information to which you need to give full credit. Don't call on me as a witness, as I will deny that I ever spoke to you. In the DAS they have created a group to monitor the activities of CCAJAR and other human rights NGOs. This agency is charged with annihilating them.' They didn't want to tell me the source." CCAJAR continue to face public accusations and overt attacks from senior State authorities and open threats from paramilitary groups or alleged paramilitary groups: "The illegal work of the state intelligence agencies have not stopped. We have several proven cases that show that this persecution continues".

> **"We were certain we were being spied on... from the beginning. But what we didn't know concretely were the dimensions of the persecution.."**
>
> **– Reinaldo Villalba. CCAJAR**

Is PUMA subject to sufficient safeguards to ensure that the interceptions by DAS and others via Esperanza or their own independent systems do not reoccur? Father Alberto Franco of the Inter-ecclesiastical Commission for Justice and Peace (Comisión Intereclesial Justicia y Paz, 'CIJP') is sceptical: "We have some sayings in Colombia: it's like asking your cat to guard your meat. Or the Devil to make the communion wafers." The CIJP works in the restive Urabá region to represent peasant communities. They document and litigate on the links between neo-paramilitary groups, private companies and the Colombian military. They are regularly accused of sympathizing with the FARC.

"We always assume we are being watched. It is part of our understanding," explained Father Alberto. "We think it's a tactic to wear us down. We get tipped off by people in the state. They tell us 'people are listening to you.'... One that I know told us things about discussions and conflicts internal to our organisation that no one else would have known." Proving that a particular person has had their communications surveilled is difficult. But that the Colombian state has spent, just based on the sample of contracts Privacy International has analysed, hundreds of billions of pesos over the past decade building an extensive surveillance architecture suggests that it is not just for show. Since 2008, CIJP have been receiving threats by telephone and communicating them to the police, without any prosecutions so far.

Father Alberto is sceptical of PUMA's value as a law enforcement tool without a fundamental realignment of intelligence priorities. "There may be people who want to use it [PUMA] for good internally. But people who want to follow laws have difficulties because there hasn't been a cleansing of the DAS involved in interceptions. When the institutions were changed, people were just reassigned elsewhere. Military intelligence has not been changed."

"There may be people who want to use it [PUMA] for good internally. But people who want to follow laws have difficulties."

Father Alberto Franco (CIJP)

"I don't know the PUMA system..." says Franklin Castaneda, President of the Committee of Solidarity with Political Prisoners (Comité de Solidaridad con los Presos Políticos, CSPP). "In human rights, nobody is an expert. We have had just basic advice: we just say that the state should have clear limits to the effect it has on private lives." CSPP is involved in advocacy on intelligence. It advocates that DAS files be declassified and purged as they had been used to identify and assassinate targets. Castaneda points to two ways that CSPP knew they were being spied upon: intelligence reports following the 2009 DAS scandal that mention CSPP and tip-offs from state agents that warn CSPP of legal actions that are being planned against them on the basis of internal communications and strategies. Following an attack on CSPP's servers in which CSPP's files were being copied and sent onwards to another unknown location, a digital security group helped CSPP to set up further firewalls and intrusion barriers. But CSPP's staff, like that of many human rights groups, struggle to use encryption and tools that would help to protect their work. "We all work under the assumption that we're always monitored." Will there ever be a reason to change this assumption?

Conclusion

Colombia's interception and monitoring systems operate in a legal framework that inadequately protects Colombian citizens' constitutional right to privacy. The distinction in the laws governing communication surveillance between electromagnetic spectrum monitoring and other forms of interception opens the door to the gathering of massive amounts of personal data on citizens' private communications.

Revelations of the wide scale of Colombian government agents' abuse of surveillance technologies over the past decade have shocked Colombians and the world. The steps taken by the Fiscalía to investigate these crimes and the courts' willingness to ensure accountability are positive developments.

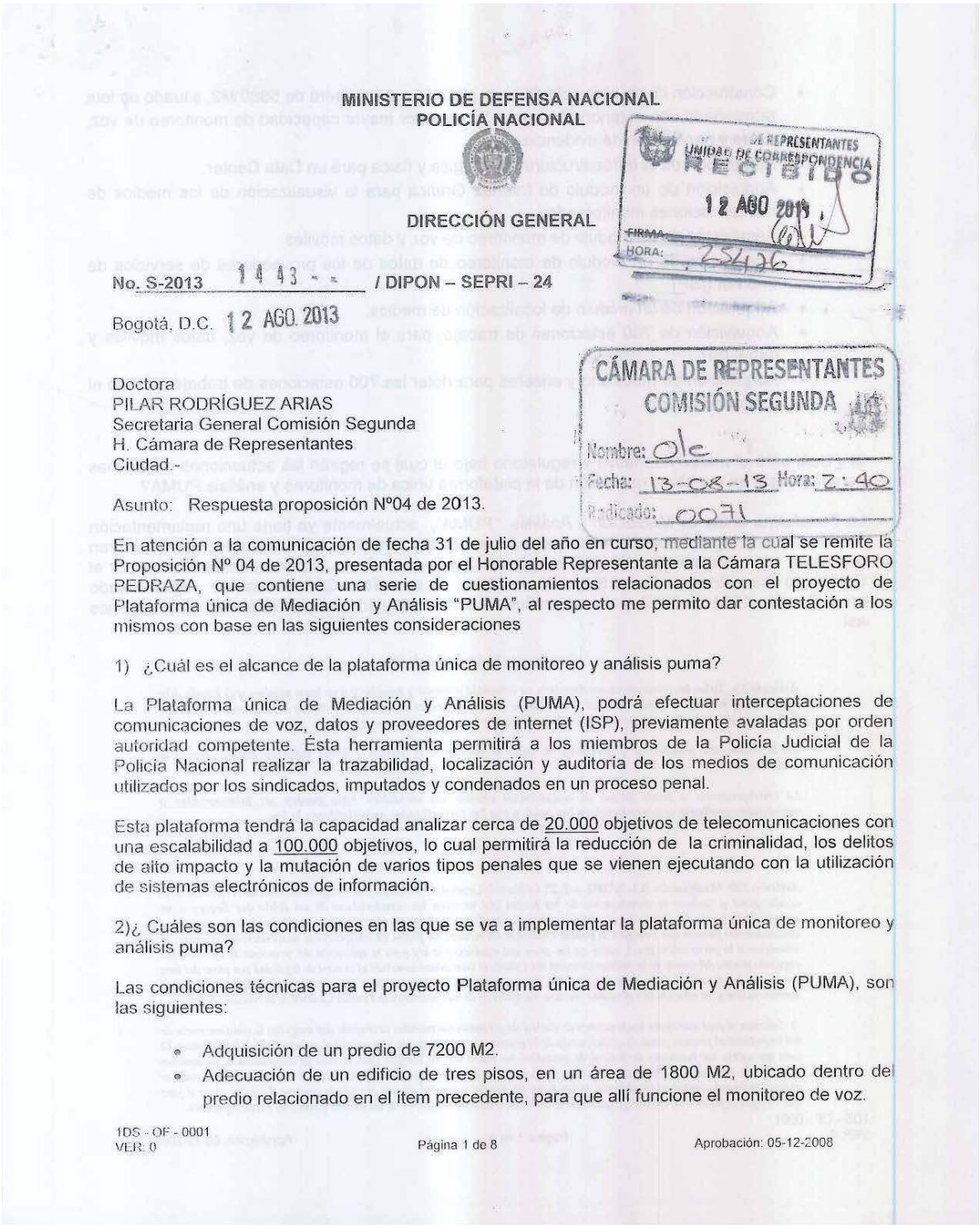
Yet effective protection against overreach in communications surveillance will not come from the technologies themselves. Most surveillance tools do not have built-in checks to prevent unlawful, arbitrary or discriminatory access to private communications data. Effective protection of the right to privacy must come in part from better laws that do not give law enforcement agencies mass surveillance capacities based on a flawed understanding of the technical process of surveillance.

The technical and legal disjuncture between the surveillance systems including the IRS, PUMA and Esperanza plus the tactical tools independently used by a number of agencies creates different standards of oversight and the potential that these will not be respected.

These loopholes must be addressed to create a system that keeps Colombians safe while respecting their right to privacy, including of those working towards a better, more democratic society.

Annexes

Page 1: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013



MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN GENERAL

CÁMARA DE REPRESENTANTES
UNIDAD DE CORRESPONDENCIA
RECIBIDO
12 AGO 2013
FIRMA:
HORA: 25426

No. S-2013 1443 - - / DIPON – SEPRI – 24

Bogotá, D.C. 12 AGO. 2013

CÁMARA DE REPRESENTANTES
COMISIÓN SEGUNDA
Nombre: Olc
Fecha: 13-08-13 Hora: 2:40
Radicado: 0071

Doctora
PILAR RODRÍGUEZ ARIAS
Secretaria General Comisión Segunda
H. Cámara de Representantes
Ciudad.-

Asunto: Respuesta proposición Nº04 de 2013.

En atención a la comunicación de fecha 31 de julio del año en curso, mediante la cual se remite la Proposición Nº 04 de 2013, presentada por el Honorable Representante a la Cámara TELESFORO PEDRAZA, que contiene una serie de cuestionamientos relacionados con el proyecto de Plataforma única de Mediación y Análisis "PUMA", al respecto me permito dar contestación a los mismos con base en las siguientes consideraciones

1) ¿Cuál es el alcance de la plataforma única de monitoreo y análisis puma?

La Plataforma única de Mediación y Análisis (PUMA), podrá efectuar interceptaciones de comunicaciones de voz, datos y proveedores de internet (ISP), previamente avaladas por orden autoridad competente. Ésta herramienta permitirá a los miembros de la Policía Judicial de la Policía Nacional realizar la trazabilidad, localización y auditoria de los medios de comunicación utilizados por los sindicados, imputados y condenados en un proceso penal.

Esta plataforma tendrá la capacidad analizar cerca de 20.000 objetivos de telecomunicaciones con una escalabilidad a 100.000 objetivos, lo cual permitirá la reducción de la criminalidad, los delitos de alto impacto y la mutación de varios tipos penales que se vienen ejecutando con la utilización de sistemas electrónicos de información.

2)¿ Cuáles son las condiciones en las que se va a implementar la plataforma única de monitoreo y análisis puma?

Las condiciones técnicas para el proyecto Plataforma única de Mediación y Análisis (PUMA), son las siguientes:

- Adquisición de un predio de 7200 M2.
- Adecuación de un edificio de tres pisos, en un área de 1800 M2, ubicado dentro del predio relacionado en el ítem precedente, para que allí funcione el monitoreo de voz.

1DS - OF - 0001
VER: 0
Página 1 de 8
Aprobación: 05-12-2008

Annexes

Page 2: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013

- Construcción de un inmueble de siete pisos, cuya área será de 5880 M2, situado en lote relacionado con anterioridad, con el fin de tener mayor capacidad de monitoreo de voz, datos y generación de evidencias.
- Adquisición de la Infraestructura tecnológica y física para un Data Center.
- Adquisición de un modulo de Interfaz Grafica para la visualización de los medios de comunicaciones monitoreados.
- Adquisición de un modulo de monitoreo de voz y datos móviles.
- Adquisición de un modulo de monitoreo de datos de los proveedores de servicios de Internet (ISP).
- Adquisición de un módulo de localización de medios.
- Adquisición de 700 estaciones de trabajo, para el monitoreo de voz, datos móviles y datos ISP.
- Adquisición de mobiliario y enseres para dotar las 700 estaciones de trabajo en todo el territorio nacional.

3) ¿Cuál será el marco normativo y regulatorio bajo el cual se regirán las actuaciones necesarias para la puesta en marcha y operación de la plataforma única de monitoreo y análisis PUMA?

La Plataforma única de Mediación y Análisis "PUMA", actualmente ya tiene una reglamentación constitucional y legal, habida cuenta que las interceptaciones de comunicaciones se encuentran reguladas por los artículos 15, 250 numerales 2 y 8 de la Carta Superior, desarrollados por el Código de Procedimiento Penal (Ley 906 de 2004), en su artículo 235, el cual fue reglamentado en el Decreto 1704 de 2012, para mayor ilustración me permito citar las referidas disposiciones así:

Constitución Política de Colombia

Artículo 15. *Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. ***Sólo pueden ser interceptadas o registradas mediante*** *orden judicial, en los casos y con* ***las formalidades que establezca la ley.***

(...)

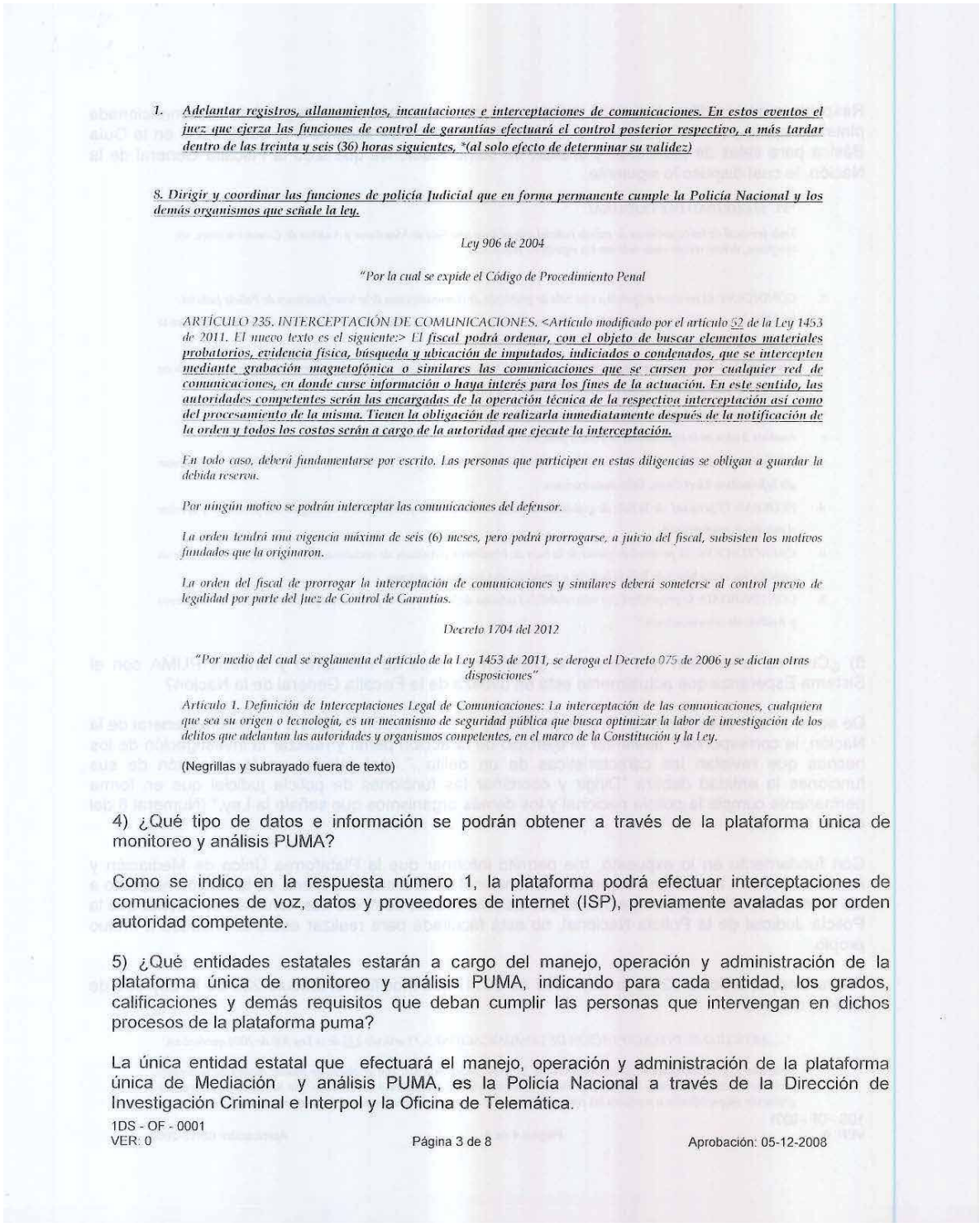
Artículo 250 Modificado. A.L. 3/2002, art. 2º. *La Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas que indiquen la posible existencia del mismo. No podrá, en consecuencia, suspender, interrumpir, ni renunciar a la persecución penal, salvo en los casos que establezca la ley para la aplicación del principio de oportunidad regulado dentro del marco de la política criminal del Estado, el cual estará sometido al control de legalidad por parte del juez que ejerza las funciones de control de garantías. Se exceptúan los delitos cometidos por miembros de la fuerza pública en servicio activo y en relación con el mismo servicio. En ejercicio de sus funciones la Fiscalía General de la Nación, deberá:*

1. Solicitar al juez que ejerza las funciones de control de garantías las medidas necesarias que aseguren la comparecencia de los imputados al proceso penal, la conservación de la prueba y la protección de la comunidad, en especial, de las víctimas. El juez que ejerza las funciones de control de garantías, no podrá ser, en ningún caso, el juez de conocimiento, en aquellos asuntos en que haya ejercido esta función. La ley podrá facultar a la Fiscalía General de la Nación para realizar excepcionalmente capturas; igualmente, la ley fijará los límites y eventos en que proceda la captura. En estos casos el juez que cumpla la función de control de garantías lo realizará a más tardar dentro de las treinta y seis (36) horas siguientes.

1DS - OF - 0001
VER: 0 Página 2 de 8 Aprobación: 05-12-2008

Annexes

Page 3: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013



1. *Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes, *(al solo efecto de determinar su validez)*

8. Dirigir y coordinar las funciones de policía judicial que en forma permanente cumple la Policía Nacional y los demás organismos que señale la ley.

Ley 906 de 2004

"Por la cual se expide el Código de Procedimiento Penal

ARTÍCULO 235. INTERCEPTACIÓN DE COMUNICACIONES. <Artículo modificado por el artículo 52 de la Ley 1453 de 2011. El nuevo texto es el siguiente:> El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación.

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron.

La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.

Decreto 1704 del 2012

"Por medio del cual se reglamenta el artículo de la Ley 1453 de 2011, se deroga el Decreto 075 de 2006 y se dictan otras disposiciones"

Artículo 1. Definición de Interceptaciones Legal de Comunicaciones: La interceptación de las comunicaciones, cualquiera que sea su origen o tecnología, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la Ley.

(Negrillas y subrayado fuera de texto)

4) ¿Qué tipo de datos e información se podrán obtener a través de la plataforma única de monitoreo y análisis PUMA?

Como se indico en la respuesta número 1, la plataforma podrá efectuar interceptaciones de comunicaciones de voz, datos y proveedores de internet (ISP), previamente avaladas por orden autoridad competente.

5) ¿Qué entidades estatales estarán a cargo del manejo, operación y administración de la plataforma única de monitoreo y análisis PUMA, indicando para cada entidad, los grados, calificaciones y demás requisitos que deban cumplir las personas que intervengan en dichos procesos de la plataforma puma?

La única entidad estatal que efectuará el manejo, operación y administración de la plataforma única de Mediación y análisis PUMA, es la Policía Nacional a través de la Dirección de Investigación Criminal e Interpol y la Oficina de Telemática.

1DS - OF - 0001
VER: 0 Página 3 de 8 Aprobación: 05-12-2008

Annexes

Page 4: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013

Respecto a los perfiles que debe cumplir el talento humano que integrará la multimencionada plataforma, me permito comunicar que estos se ajustaran de acuerdo a lo establecido en la Guía Básica para salas de monitoreo y análisis de comunicaciones que creó la Fiscalía General de la Nación, la cual dispuso lo siguiente:

"VI. SEGURIDAD DEL PERSONAL

Todo personal de los organismos de policía judicial asignados a una Sala de Monitoreo y Análisis de Comunicaciones, sin excepción, deberá reunir como mínimo los siguientes requisitos:

1. *CONDICION: El personal asignado a una Sala de grabación de comunicaciones debe tener funciones de Policía Judicial.*
2. *PERFIL: El personal asignado a una Sala de grabación de comunicaciones debe acreditar la capacitación e idoneidad para la ejecución de esta labor.*
3. *ANTIGÜEDAD: El personal asignado a una Sala de Monitoreo y Análisis de comunicaciones debe tener experiencia en actividad de policía judicial conforme a la función a desempeñar así:*

- *Coordinador de sala 4 años en la especialidad de Policía Judicial.*
- *Analista 2 años en la especialidad de Policía Judicial.*
- *Administrador de Sistemas 1 años en la especialidad de Policía Judicial y ser como mínimo Técnico certificado en Sistemas y/o Informática, Electrónica, Telecomunicaciones.*

4. *PRUEBAS: El personal de la Sala de grabación de comunicaciones debe previamente a su asignación, presentar y aprobar el estudio de confiabilidad.*
5. *CAPACITACION: El personal asignado de la Sala de Monitoreo y Análisis de comunicaciones debe contar dentro de su capacitación curso básico de Policía Judicial y conocimientos básicos en sistemas.*
6. *CONTINUIDAD: Se propenderá por una estabilidad mínima de 5 años para el personal asignado a una Sala de Monitoreo y Análisis de comunicaciones."*

6) ¿Cuál es la relación que tendrá la plataforma única de monitoreo y análisis PUMA con el Sistema Esperanza que actualmente está en cabeza de la Fiscalía General de la Nación?

De acuerdo a lo establecido en el artículo 250 de la Constitución Política a la Fiscalía General de la Nación, le corresponde: "adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito...". Así mismo, en la ejecución de sus funciones la entidad deberá "Dirigir y coordinar las funciones de policía judicial que en forma permanente cumple la policía nacional y los demás organismos que señale la Ley." (Numeral 8 del citado artículo).

Con fundamento en lo expuesto, me permito informar que la Plataforma Única de Mediación y Análisis "PUMA", tendrá una dependencia funcional de la Fiscalía General de la Nación respecto a las órdenes de interceptación emitidas por las autoridades competentes, teniendo en cuenta que la Policía Judicial de la Policía Nacional, no está facultada para realizar estas actividades a mutuo propio.

Ahora bien, el artículo 52 de la Ley 1453 de 2011, que modificó el artículo 235 de la Ley 906 de 2004, dispuso:

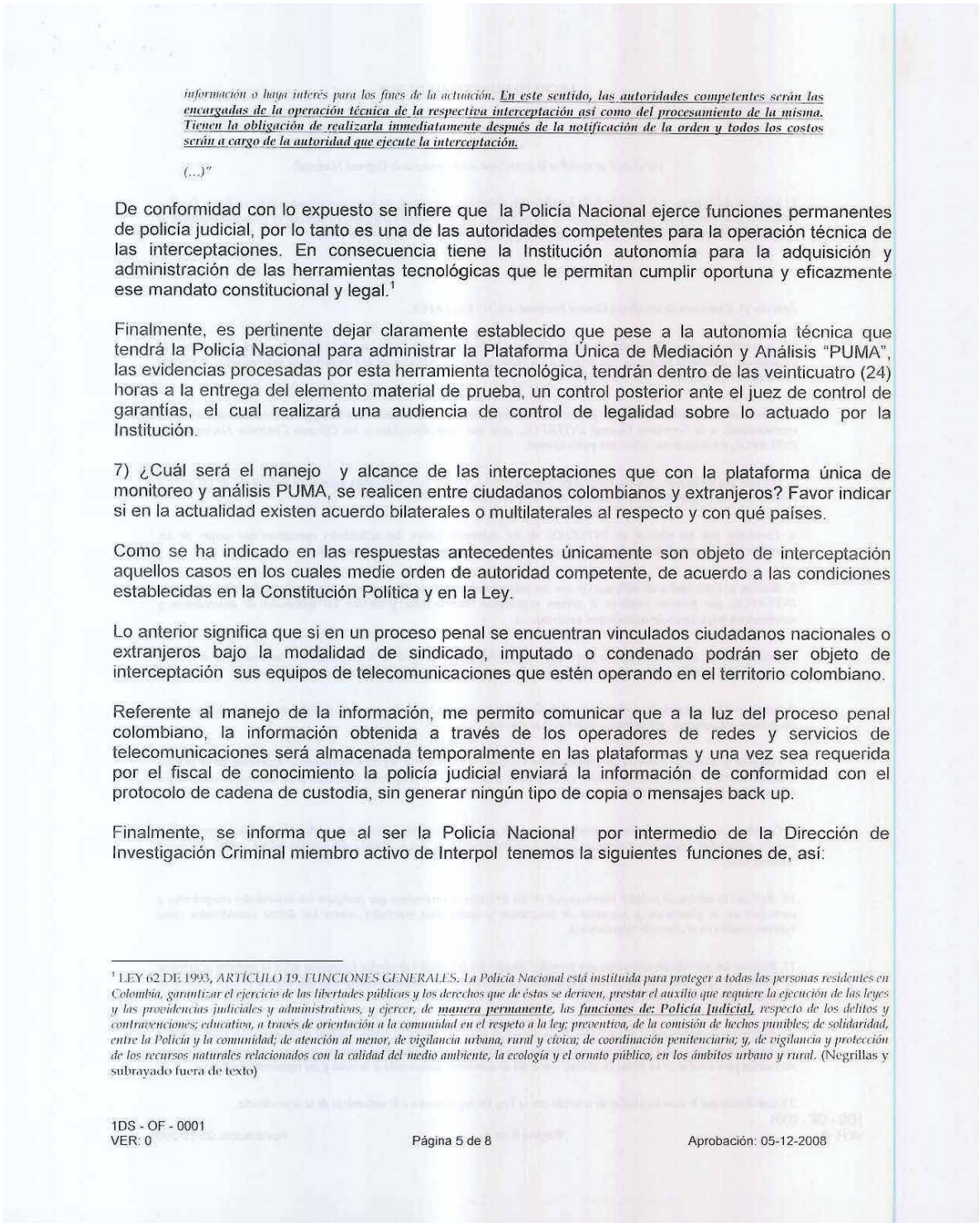
"... ARTÍCULO 52. INTERCEPTACIÓN DE COMUNICACIONES. El artículo 235 de la Ley 906 de 2004 quedará así:

***Artículo** 235. Interceptación de comunicaciones. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse*

1DS - OF - 0001
VER: 0 Página 4 de 8 Aprobación: 05-12-2008

Annexes

Page 5: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013



*información o haya interés para los fines de la actuación. **En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación.***

(...)"

De conformidad con lo expuesto se infiere que la Policía Nacional ejerce funciones permanentes de policía judicial, por lo tanto es una de las autoridades competentes para la operación técnica de las interceptaciones. En consecuencia tiene la Institución autonomía para la adquisición y administración de las herramientas tecnológicas que le permitan cumplir oportuna y eficazmente ese mandato constitucional y legal.[1]

Finalmente, es pertinente dejar claramente establecido que pese a la autonomía técnica que tendrá la Policía Nacional para administrar la Plataforma Única de Mediación y Análisis "PUMA", las evidencias procesadas por esta herramienta tecnológica, tendrán dentro de las veinticuatro (24) horas a la entrega del elemento material de prueba, un control posterior ante el juez de control de garantías, el cual realizará una audiencia de control de legalidad sobre lo actuado por la Institución.

7) ¿Cuál será el manejo y alcance de las interceptaciones que con la plataforma única de monitoreo y análisis PUMA, se realicen entre ciudadanos colombianos y extranjeros? Favor indicar si en la actualidad existen acuerdo bilaterales o multilaterales al respecto y con qué países.

Como se ha indicado en las respuestas antecedentes únicamente son objeto de interceptación aquellos casos en los cuales medie orden de autoridad competente, de acuerdo a las condiciones establecidas en la Constitución Política y en la Ley.

Lo anterior significa que si en un proceso penal se encuentran vinculados ciudadanos nacionales o extranjeros bajo la modalidad de sindicado, imputado o condenado podrán ser objeto de interceptación sus equipos de telecomunicaciones que estén operando en el territorio colombiano.

Referente al manejo de la información, me permito comunicar que a la luz del proceso penal colombiano, la información obtenida a través de los operadores de redes y servicios de telecomunicaciones será almacenada temporalmente en las plataformas y una vez sea requerida por el fiscal de conocimiento la policía judicial enviará la información de conformidad con el protocolo de cadena de custodia, sin generar ningún tipo de copia o mensajes back up.

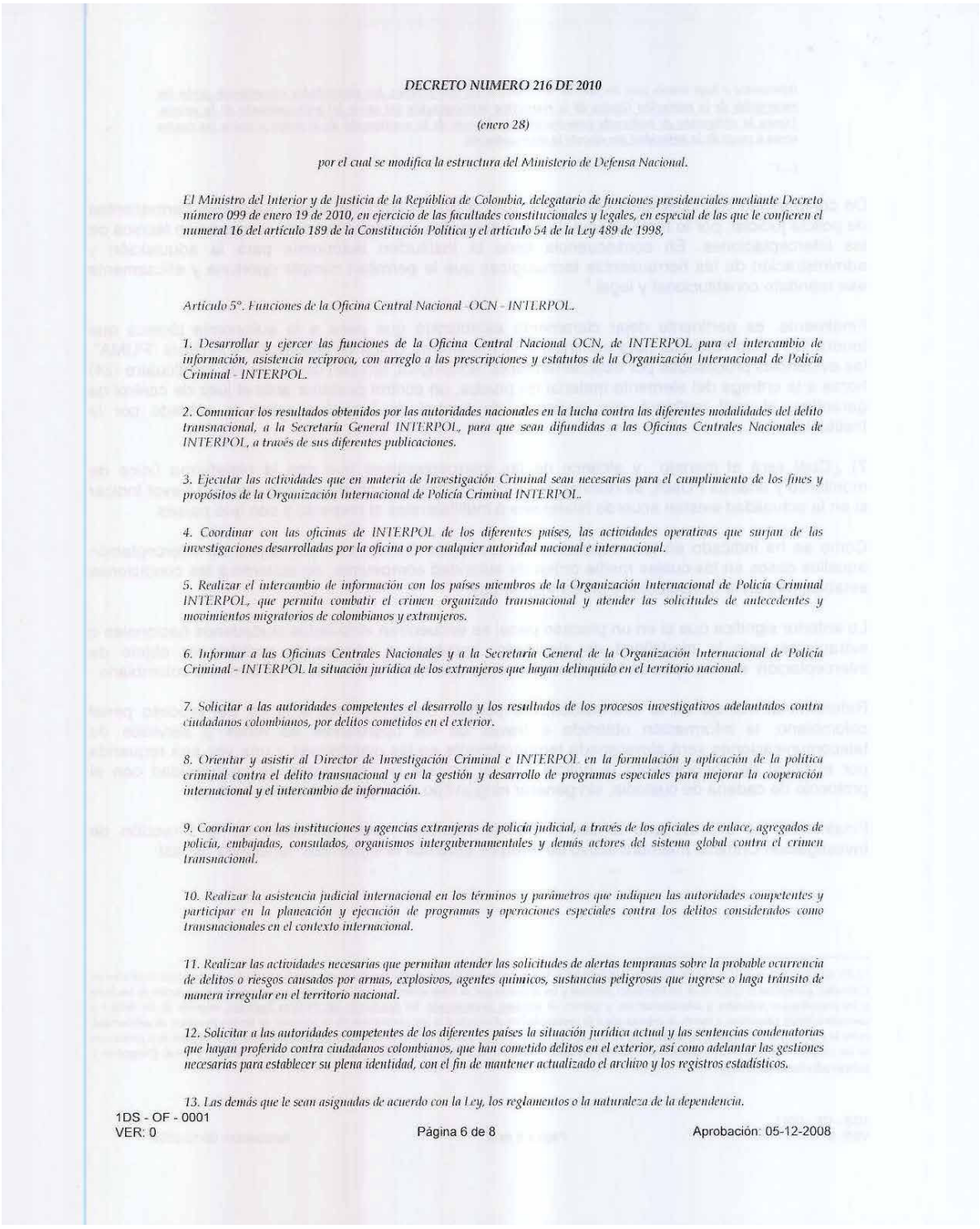
Finalmente, se informa que al ser la Policía Nacional por intermedio de la Dirección de Investigación Criminal miembro activo de Interpol tenemos la siguientes funciones de, así:

[1] LEY 62 DE 1993, *ARTÍCULO 19. FUNCIONES GENERALES. La Policía Nacional está instituida para proteger a todas las personas residentes en Colombia, garantizar el ejercicio de las libertades públicas y los derechos que de éstas se deriven, prestar el auxilio que requiere la ejecución de las leyes y las providencias judiciales y administrativos, y ejercer, de **manera permanente**, las **funciones de: Policía Judicial**, respecto de los delitos y contravenciones; educativa, a través de orientación a la comunidad en el respeto a la ley; preventiva, de la comisión de hechos punibles; de solidaridad, entre la Policía y la comunidad; de atención al menor, de vigilancia urbana, rural y cívica; de coordinación penitenciaria; y, de vigilancia y protección de los recursos naturales relacionados con la calidad del medio ambiente, la ecología y el ornato público, en los ámbitos urbano y rural.* (Negrillas y subrayado fuera de texto)

1DS - OF - 0001
VER: 0 Página 5 de 8 Aprobación: 05-12-2008

Annexes

Page 6: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013



DECRETO NUMERO 216 DE 2010

(enero 28)

por el cual se modifica la estructura del Ministerio de Defensa Nacional.

El Ministro del Interior y de Justicia de la República de Colombia, delegatario de funciones presidenciales mediante Decreto número 099 de enero 19 de 2010, en ejercicio de las facultades constitucionales y legales, en especial de las que le confieren el numeral 16 del artículo 189 de la Constitución Política y el artículo 54 de la Ley 489 de 1998,

Artículo 5°. Funciones de la Oficina Central Nacional -OCN - INTERPOL.

1. Desarrollar y ejercer las funciones de la Oficina Central Nacional OCN, de INTERPOL para el intercambio de información, asistencia recíproca, con arreglo a las prescripciones y estatutos de la Organización Internacional de Policía Criminal - INTERPOL.

2. Comunicar los resultados obtenidos por las autoridades nacionales en la lucha contra las diferentes modalidades del delito transnacional, a la Secretaría General INTERPOL, para que sean difundidas a las Oficinas Centrales Nacionales de INTERPOL, a través de sus diferentes publicaciones.

3. Ejecutar las actividades que en materia de Investigación Criminal sean necesarias para el cumplimiento de los fines y propósitos de la Organización Internacional de Policía Criminal INTERPOL.

4. Coordinar con las oficinas de INTERPOL de los diferentes países, las actividades operativas que surjan de las investigaciones desarrolladas por la oficina o por cualquier autoridad nacional e internacional.

5. Realizar el intercambio de información con los países miembros de la Organización Internacional de Policía Criminal INTERPOL, que permita combatir el crimen organizado transnacional y atender las solicitudes de antecedentes y movimientos migratorios de colombianos y extranjeros.

6. Informar a las Oficinas Centrales Nacionales y a la Secretaría General de la Organización Internacional de Policía Criminal - INTERPOL la situación jurídica de los extranjeros que hayan delinquido en el territorio nacional.

7. Solicitar a las autoridades competentes el desarrollo y los resultados de los procesos investigativos adelantados contra ciudadanos colombianos, por delitos cometidos en el exterior.

8. Orientar y asistir al Director de Investigación Criminal e INTERPOL en la formulación y aplicación de la política criminal contra el delito transnacional y en la gestión y desarrollo de programas especiales para mejorar la cooperación internacional y el intercambio de información.

9. Coordinar con las instituciones y agencias extranjeras de policía judicial, a través de los oficiales de enlace, agregados de policía, embajadas, consulados, organismos intergubernamentales y demás actores del sistema global contra el crimen transnacional.

10. Realizar la asistencia judicial internacional en los términos y parámetros que indiquen las autoridades competentes y participar en la planeación y ejecución de programas y operaciones especiales contra los delitos considerados como transnacionales en el contexto internacional.

11. Realizar las actividades necesarias que permitan atender las solicitudes de alertas tempranas sobre la probable ocurrencia de delitos o riesgos causados por armas, explosivos, agentes químicos, sustancias peligrosas que ingrese o haga tránsito de manera irregular en el territorio nacional.

12. Solicitar a las autoridades competentes de los diferentes países la situación jurídica actual y las sentencias condenatorias que hayan proferido contra ciudadanos colombianos, que han cometido delitos en el exterior, así como adelantar las gestiones necesarias para establecer su plena identidad, con el fin de mantener actualizado el archivo y los registros estadísticos.

13. Las demás que le sean asignadas de acuerdo con la Ley, los reglamentos o la naturaleza de la dependencia.

1DS - OF - 0001
VER: 0 Página 6 de 8 Aprobación: 05-12-2008

Annexes

Page 7: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013

8) ¿Sírvase informar cuáles son los fines que persigue las dos plataformas PUMA y ESPERANZA, y si a través de estas plataformas podrán tener acceso a los correos electrónicos de ciudadanos que no tengan ningún tipo de antecedente judiciales ?

Respecto a los fines que persigue la plataforma esperanza, la institución competente para proporcionar este tipo de información es la Fiscalía General de la Nación, por tal motivo este ítem será remitido a la referida entidad para que se pronuncie sobre el tema.

Ahora bien, con la implementación de la plataforma puma se pretende fortalecer la capacidad tecnológica para la interceptación de comunicaciones, como herramienta fundamental de la investigación criminal que permita garantizar la seguridad ciudadana, la reducción de la criminalidad y de los delitos de alto impacto. La modernización de éste instrumento constituye una necesidad funcional de la Policía Nacional, en consideración al ámbito de responsabilidad que en materia de seguridad ciudadana tiene la Institución y a los retos del futuro enmarcados dentro de las políticas del post conflicto.

Los objetivos específicos de la plataforma son:

- Adquirir un sistema que permita realizar la trazabilidad, georeferención precisa y auditoria garantizando un proceso ágil y transparente.
- Recopilar la evidencia digital contenida a través de los datos de las redes, ISP, telefonía celular y iden.
- Adquirir un sistema que permita tener la capacidad de monitorear cerca de 20.000 objetivos de telecomunicaciones con una escalabilidad a 100.000 objetivos.
- Adecuar 700 estaciones de trabajo para las unidades de policía judicial en el contexto local y regional .

9) ¿ Sírvase Informar a cuánto ascienden los recursos necesario para la implementación, puesta en marcha y operación de la plataforma Única de Monitoreo y Análisis PUMA, así como las unidades ejecutoras de dichos recursos y la asignación presupuestal necesaria año a año de los mismos?

La unidad ejecutora del proyecto será la Dirección Administrativa y Financiera de la Policía Nacional, el valor total del proyecto es de $100.000.000.000, distribuidos así:

RECURSOS	2013	2014
EXTRAORDINARIOS	$ 50.000.000.000	$ 50.000.000.000
TOTAL PROYECTO	$ 100.000.000.000	

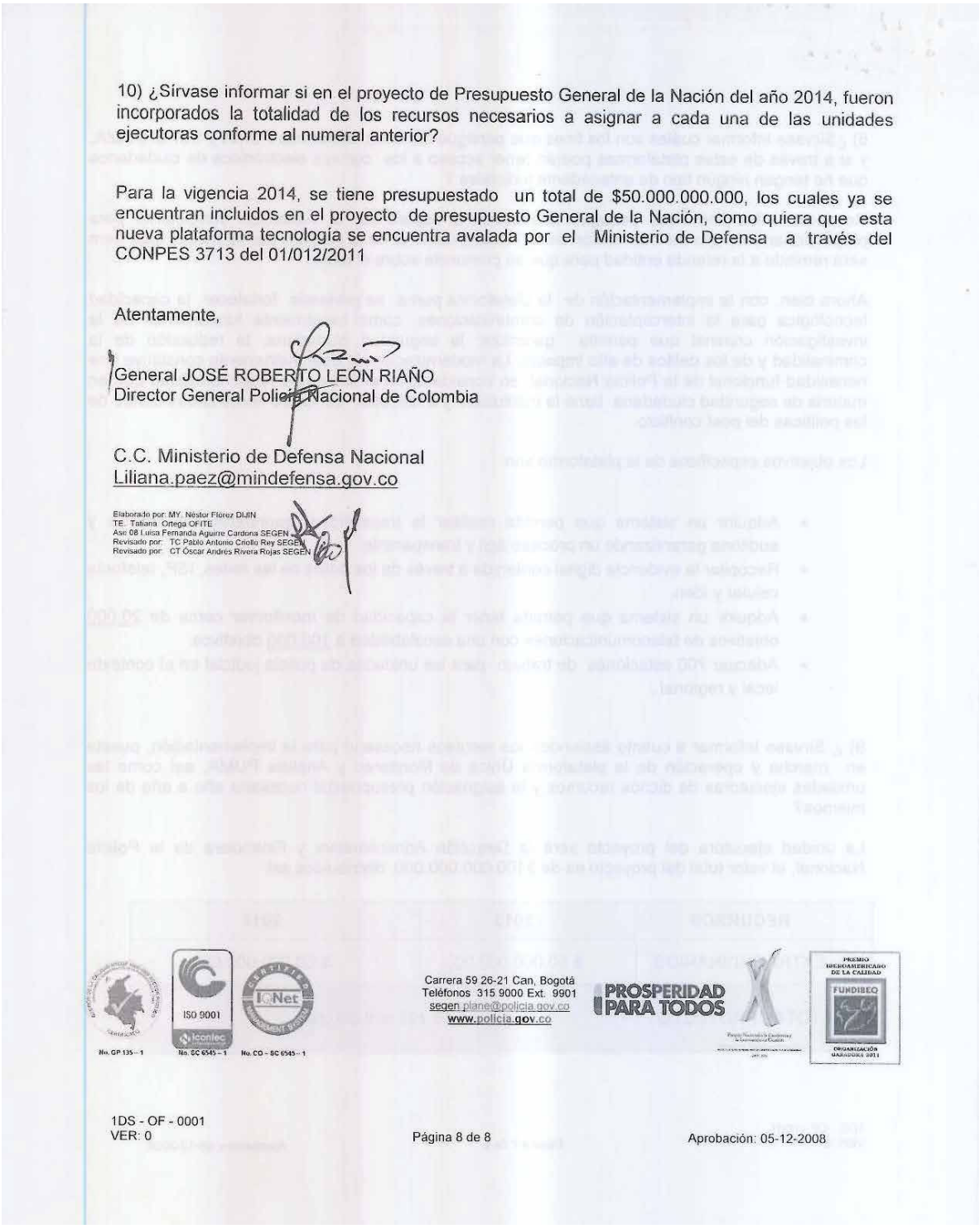
1DS - OF - 0001
VER: 0

Página 7 de 8

Aprobación: 05-12-2008

Annexes

Page 8: RTAS POLICIA NACIONAL PROP 4 DEL 30 DE JUL DE 2013



10) ¿Sírvase informar si en el proyecto de Presupuesto General de la Nación del año 2014, fueron incorporados la totalidad de los recursos necesarios a asignar a cada una de las unidades ejecutoras conforme al numeral anterior?

Para la vigencia 2014, se tiene presupuestado un total de $50.000.000.000, los cuales ya se encuentran incluidos en el proyecto de presupuesto General de la Nación, como quiera que esta nueva plataforma tecnología se encuentra avalada por el Ministerio de Defensa a través del CONPES 3713 del 01/012/2011

Atentamente,

General JOSÉ ROBERTO LEÓN RIAÑO
Director General Policía Nacional de Colombia

C.C. Ministerio de Defensa Nacional
Liliana.paez@mindefensa.gov.co

Elaborado por: MY. Néstor Flórez DIJIN
TE. Tatiana Ortega OFITE
Ase 08 Luisa Fernanda Aguirre Cardona SEGEN
Revisado por: TC Pablo Antonio Criollo Rey SEGEN
Revisado por: CT Óscar Andrés Rivera Rojas SEGEN

ISO 9001
No. GP 135 – 1
No. SC 6545 – 1
No. CO – SC 6545 – 1

Carrera 59 26-21 Can, Bogotá
Teléfonos 315 9000 Ext. 9901
segen.plane@policia.gov.co
www.policia.gov.co

PROSPERIDAD PARA TODOS

PREMIO IBEROAMERICANO DE LA CALIDAD
FUNDIBEQ
ORGANIZACIÓN GALARDONADA 2011

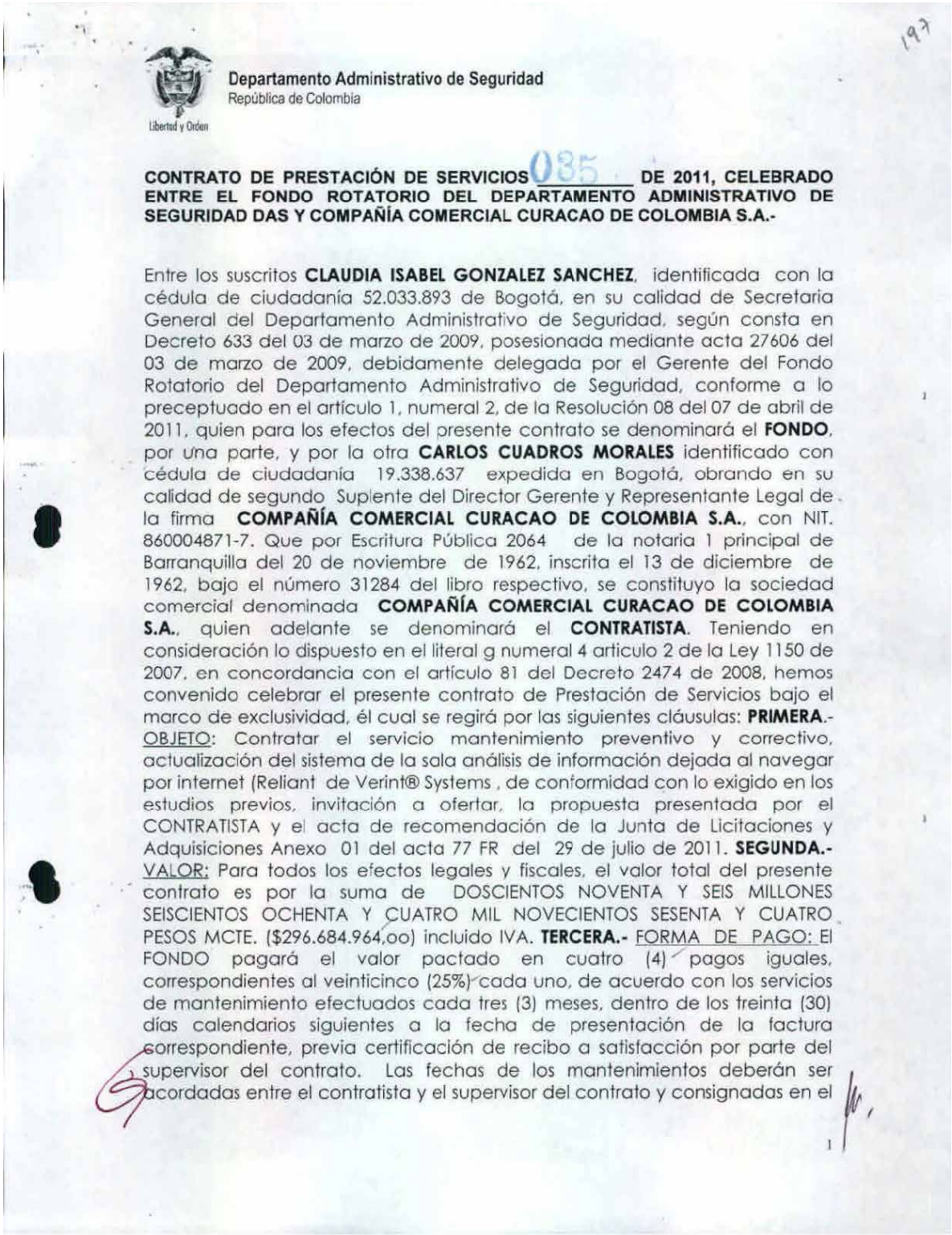
1DS - OF - 0001
VER: 0

Página 8 de 8

Aprobación: 05-12-2008

Annexes

Page 1: 2011-8/22 DAS contract Verint



197

Departamento Administrativo de Seguridad
República de Colombia

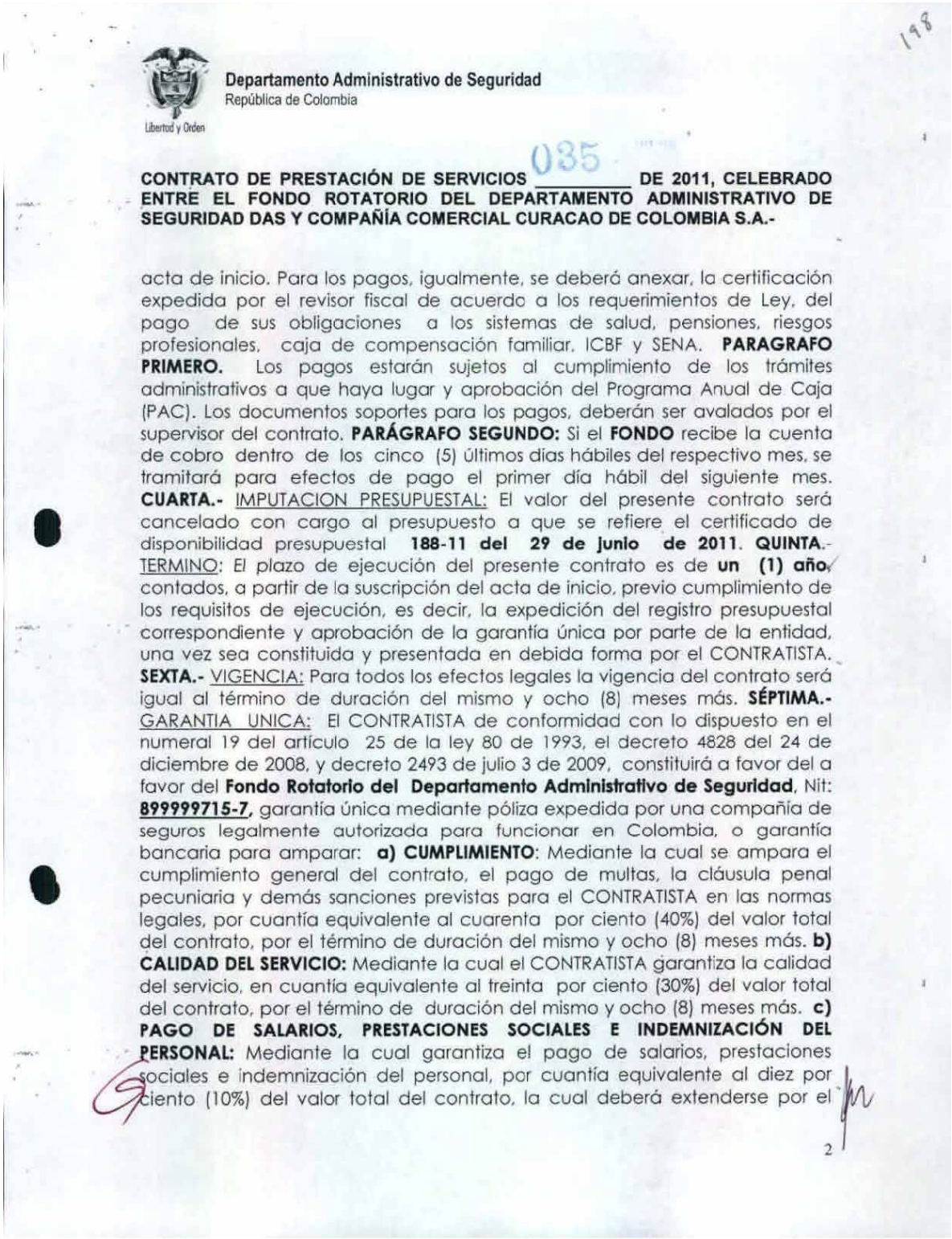
Libertad y Orden

CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

Entre los suscritos **CLAUDIA ISABEL GONZALEZ SANCHEZ**, identificada con la cédula de ciudadanía 52.033.893 de Bogotá, en su calidad de Secretaria General del Departamento Administrativo de Seguridad, según consta en Decreto 633 del 03 de marzo de 2009, posesionada mediante acta 27606 del 03 de marzo de 2009, debidamente delegada por el Gerente del Fondo Rotatorio del Departamento Administrativo de Seguridad, conforme a lo preceptuado en el artículo 1, numeral 2, de la Resolución 08 del 07 de abril de 2011, quien para los efectos del presente contrato se denominará el **FONDO**, por una parte, y por la otra **CARLOS CUADROS MORALES** identificado con cédula de ciudadanía 19.338.637 expedida en Bogotá, obrando en su calidad de segundo Suplente del Director Gerente y Representante Legal de la firma **COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.**, con NIT. 860004871-7. Que por Escritura Pública 2064 de la notaria 1 principal de Barranquilla del 20 de noviembre de 1962, inscrita el 13 de diciembre de 1962, bajo el número 31284 del libro respectivo, se constituyo la sociedad comercial denominada **COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.**, quien adelante se denominará el **CONTRATISTA**. Teniendo en consideración lo dispuesto en el literal g numeral 4 articulo 2 de la Ley 1150 de 2007, en concordancia con el artículo 81 del Decreto 2474 de 2008, hemos convenido celebrar el presente contrato de Prestación de Servicios bajo el marco de exclusividad, él cual se regirá por las siguientes cláusulas: **PRIMERA.-** OBJETO: Contratar el servicio mantenimiento preventivo y correctivo, actualización del sistema de la sala análisis de información dejada al navegar por internet (Reliant de Verint® Systems , de conformidad con lo exigido en los estudios previos, invitación a ofertar, la propuesta presentada por el CONTRATISTA y el acta de recomendación de la Junta de Licitaciones y Adquisiciones Anexo 01 del acta 77 FR del 29 de julio de 2011. **SEGUNDA.-** VALOR: Para todos los efectos legales y fiscales, el valor total del presente contrato es por la suma de DOSCIENTOS NOVENTA Y SEIS MILLONES SEISCIENTOS OCHENTA Y CUATRO MIL NOVECIENTOS SESENTA Y CUATRO PESOS MCTE. ($296.684.964,oo) incluido IVA. **TERCERA.-** FORMA DE PAGO: El FONDO pagará el valor pactado en cuatro (4) pagos iguales, correspondientes al veinticinco (25%) cada uno, de acuerdo con los servicios de mantenimiento efectuados cada tres (3) meses, dentro de los treinta (30) días calendarios siguientes a la fecha de presentación de la factura correspondiente, previa certificación de recibo a satisfacción por parte del supervisor del contrato. Las fechas de los mantenimientos deberán ser acordadas entre el contratista y el supervisor del contrato y consignadas en el

Annexes

Page 2: 2011-8/22 DAS contract Verint



198

Departamento Administrativo de Seguridad
República de Colombia

Libertad y Orden

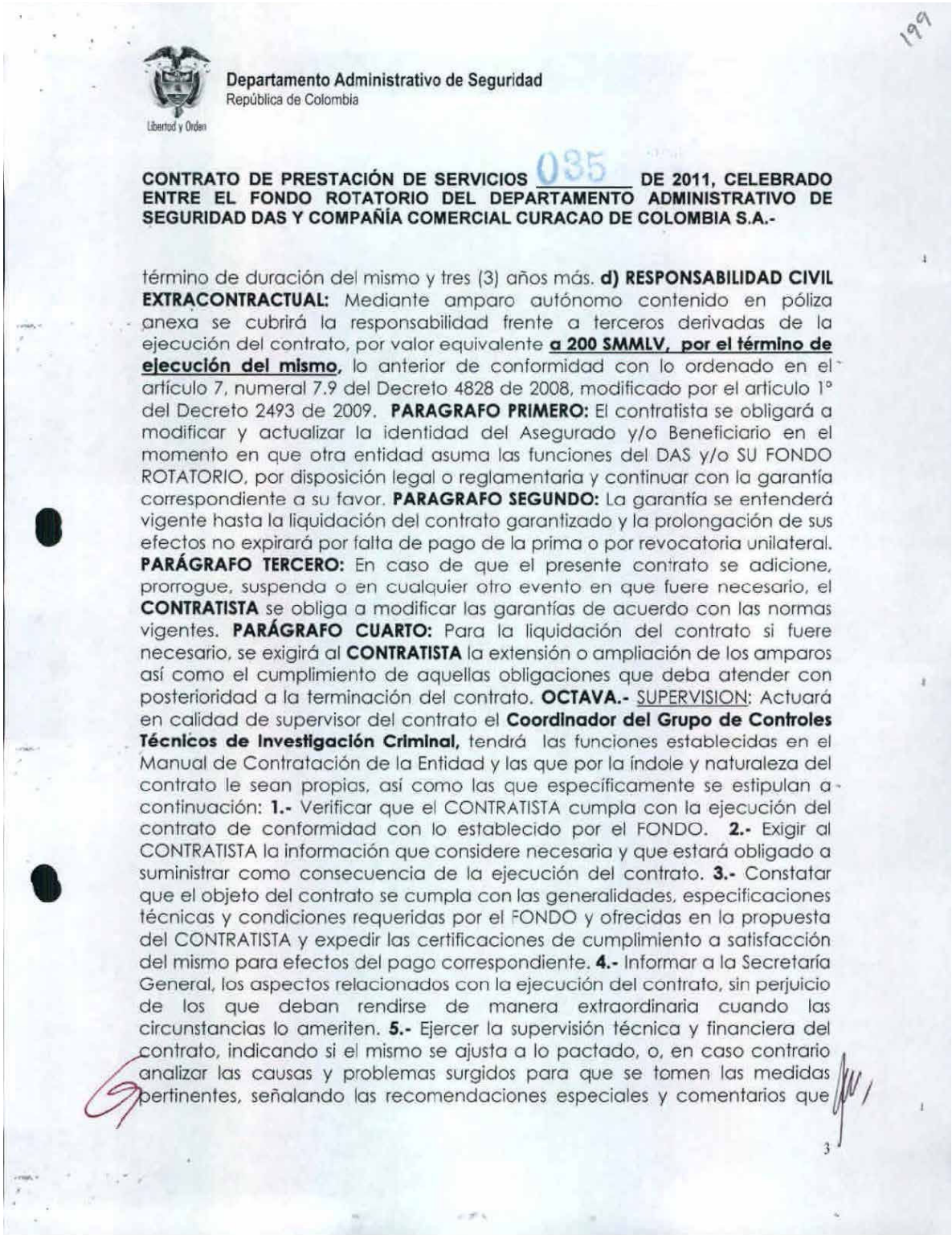
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

acta de inicio. Para los pagos, igualmente, se deberá anexar, la certificación expedida por el revisor fiscal de acuerdo a los requerimientos de Ley, del pago de sus obligaciones a los sistemas de salud, pensiones, riesgos profesionales, caja de compensación familiar, ICBF y SENA. **PARAGRAFO PRIMERO.** Los pagos estarán sujetos al cumplimiento de los trámites administrativos a que haya lugar y aprobación del Programa Anual de Caja (PAC). Los documentos soportes para los pagos, deberán ser avalados por el supervisor del contrato. **PARÁGRAFO SEGUNDO:** Si el **FONDO** recibe la cuenta de cobro dentro de los cinco (5) últimos días hábiles del respectivo mes, se tramitará para efectos de pago el primer día hábil del siguiente mes. **CUARTA.-** IMPUTACION PRESUPUESTAL: El valor del presente contrato será cancelado con cargo al presupuesto a que se refiere el certificado de disponibilidad presupuestal **188-11 del 29 de junio de 2011. QUINTA.-** TERMINO: El plazo de ejecución del presente contrato es de **un (1) año**, contados, a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de ejecución, es decir, la expedición del registro presupuestal correspondiente y aprobación de la garantía única por parte de la entidad, una vez sea constituida y presentada en debida forma por el CONTRATISTA. **SEXTA.-** VIGENCIA: Para todos los efectos legales la vigencia del contrato será igual al término de duración del mismo y ocho (8) meses más. **SÉPTIMA.-** GARANTIA UNICA: El CONTRATISTA de conformidad con lo dispuesto en el numeral 19 del artículo 25 de la ley 80 de 1993, el decreto 4828 del 24 de diciembre de 2008, y decreto 2493 de julio 3 de 2009, constituirá a favor del a favor del **Fondo Rotatorio del Departamento Administrativo de Seguridad**, Nit: **899999715-7**, garantía única mediante póliza expedida por una compañía de seguros legalmente autorizada para funcionar en Colombia, o garantía bancaria para amparar: **a) CUMPLIMIENTO**: Mediante la cual se ampara el cumplimiento general del contrato, el pago de multas, la cláusula penal pecuniaria y demás sanciones previstas para el CONTRATISTA en las normas legales, por cuantía equivalente al cuarenta por ciento (40%) del valor total del contrato, por el término de duración del mismo y ocho (8) meses más. **b) CALIDAD DEL SERVICIO:** Mediante la cual el CONTRATISTA garantiza la calidad del servicio, en cuantía equivalente al treinta por ciento (30%) del valor total del contrato, por el término de duración del mismo y ocho (8) meses más. **c) PAGO DE SALARIOS, PRESTACIONES SOCIALES E INDEMNIZACIÓN DEL PERSONAL:** Mediante la cual garantiza el pago de salarios, prestaciones sociales e indemnización del personal, por cuantía equivalente al diez por ciento (10%) del valor total del contrato, la cual deberá extenderse por el

2

Annexes

Page 3: 2011-8/22 DAS contract Verint



199

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

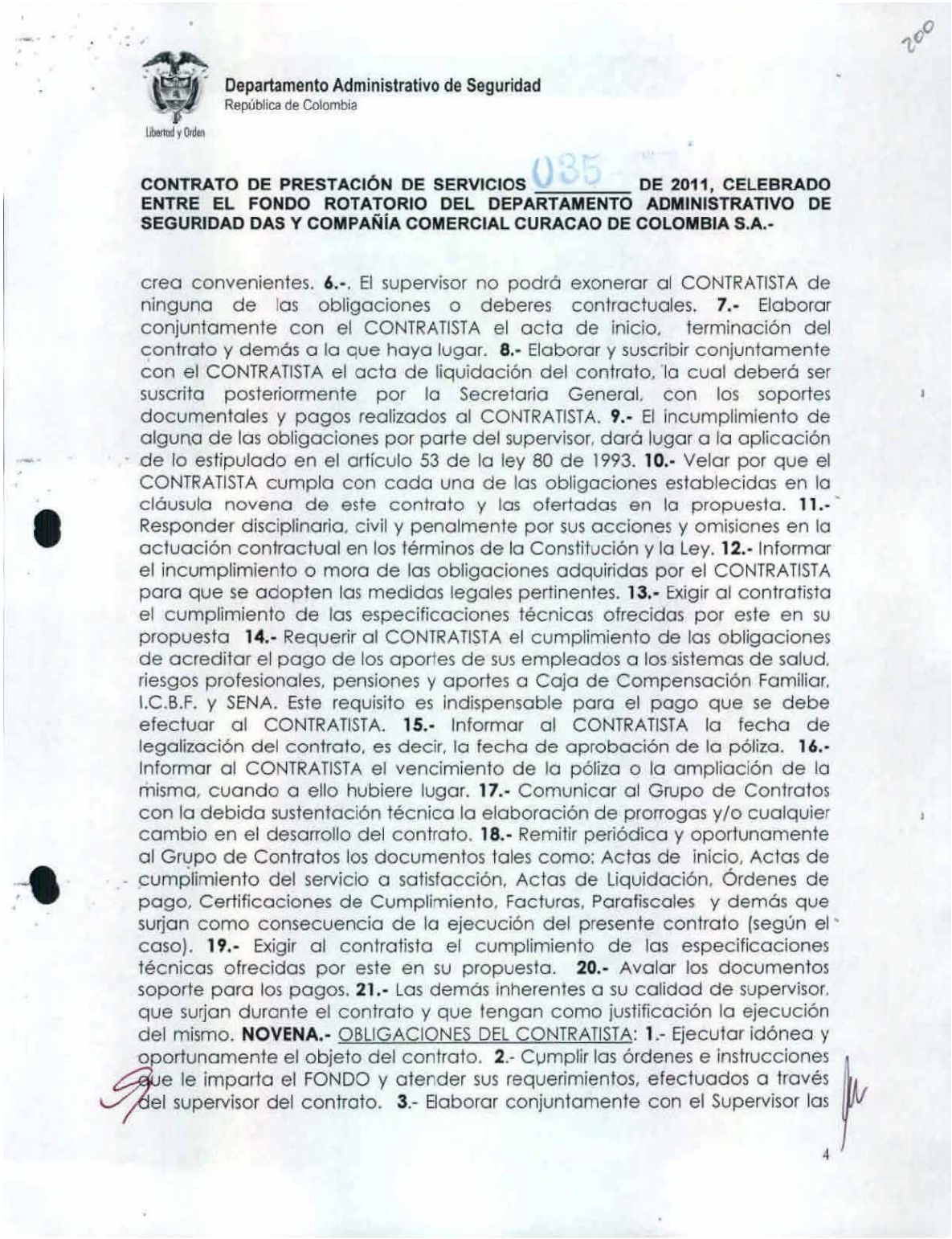
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

término de duración del mismo y tres (3) años más. **d) RESPONSABILIDAD CIVIL EXTRACONTRACTUAL:** Mediante amparo autónomo contenido en póliza anexa se cubrirá la responsabilidad frente a terceros derivadas de la ejecución del contrato, por valor equivalente **a 200 SMMLV, por el término de ejecución del mismo,** lo anterior de conformidad con lo ordenado en el artículo 7, numeral 7.9 del Decreto 4828 de 2008, modificado por el artículo 1° del Decreto 2493 de 2009. **PARAGRAFO PRIMERO:** El contratista se obligará a modificar y actualizar la identidad del Asegurado y/o Beneficiario en el momento en que otra entidad asuma las funciones del DAS y/o SU FONDO ROTATORIO, por disposición legal o reglamentaria y continuar con la garantía correspondiente a su favor. **PARAGRAFO SEGUNDO:** La garantía se entenderá vigente hasta la liquidación del contrato garantizado y la prolongación de sus efectos no expirará por falta de pago de la prima o por revocatoria unilateral. **PARÁGRAFO TERCERO:** En caso de que el presente contrato se adicione, prorrogue, suspenda o en cualquier otro evento en que fuere necesario, el **CONTRATISTA** se obliga a modificar las garantías de acuerdo con las normas vigentes. **PARÁGRAFO CUARTO:** Para la liquidación del contrato si fuere necesario, se exigirá al **CONTRATISTA** la extensión o ampliación de los amparos así como el cumplimiento de aquellas obligaciones que deba atender con posterioridad a la terminación del contrato. **OCTAVA.-** SUPERVISION: Actuará en calidad de supervisor del contrato el **Coordinador del Grupo de Controles Técnicos de Investigación Criminal,** tendrá las funciones establecidas en el Manual de Contratación de la Entidad y las que por la índole y naturaleza del contrato le sean propias, así como las que específicamente se estipulan a continuación: **1.-** Verificar que el CONTRATISTA cumpla con la ejecución del contrato de conformidad con lo establecido por el FONDO. **2.-** Exigir al CONTRATISTA la información que considere necesaria y que estará obligado a suministrar como consecuencia de la ejecución del contrato. **3.-** Constatar que el objeto del contrato se cumpla con las generalidades, especificaciones técnicas y condiciones requeridas por el FONDO y ofrecidas en la propuesta del CONTRATISTA y expedir las certificaciones de cumplimiento a satisfacción del mismo para efectos del pago correspondiente. **4.-** Informar a la Secretaría General, los aspectos relacionados con la ejecución del contrato, sin perjuicio de los que deban rendirse de manera extraordinaria cuando las circunstancias lo ameriten. **5.-** Ejercer la supervisión técnica y financiera del contrato, indicando si el mismo se ajusta a lo pactado, o, en caso contrario analizar las causas y problemas surgidos para que se tomen las medidas pertinentes, señalando las recomendaciones especiales y comentarios que

3

Annexes

Page 4: 2011-8/22 DAS contract Verint



Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

200

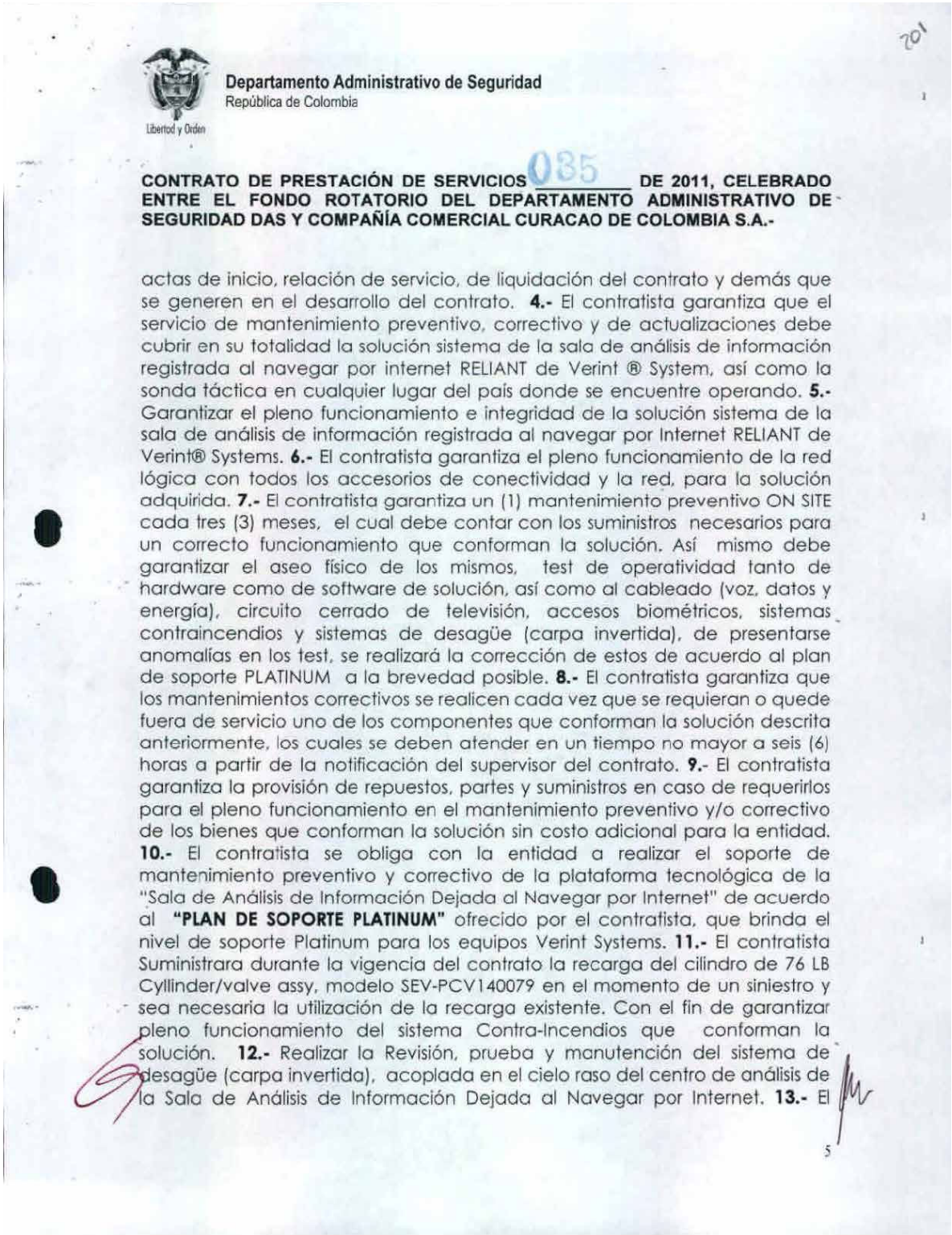
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

crea convenientes. **6.-**. El supervisor no podrá exonerar al CONTRATISTA de ninguna de las obligaciones o deberes contractuales. **7.-** Elaborar conjuntamente con el CONTRATISTA el acta de inicio, terminación del contrato y demás a la que haya lugar. **8.-** Elaborar y suscribir conjuntamente con el CONTRATISTA el acta de liquidación del contrato, la cual deberá ser suscrita posteriormente por la Secretaria General, con los soportes documentales y pagos realizados al CONTRATISTA. **9.-** El incumplimiento de alguna de las obligaciones por parte del supervisor, dará lugar a la aplicación de lo estipulado en el artículo 53 de la ley 80 de 1993. **10.-** Velar por que el CONTRATISTA cumpla con cada una de las obligaciones establecidas en la cláusula novena de este contrato y las ofertadas en la propuesta. **11.-** Responder disciplinaria, civil y penalmente por sus acciones y omisiones en la actuación contractual en los términos de la Constitución y la Ley. **12.-** Informar el incumplimiento o mora de las obligaciones adquiridas por el CONTRATISTA para que se adopten las medidas legales pertinentes. **13.-** Exigir al contratista el cumplimiento de las especificaciones técnicas ofrecidas por este en su propuesta **14.-** Requerir al CONTRATISTA el cumplimiento de las obligaciones de acreditar el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a Caja de Compensación Familiar, I.C.B.F. y SENA. Este requisito es indispensable para el pago que se debe efectuar al CONTRATISTA. **15.-** Informar al CONTRATISTA la fecha de legalización del contrato, es decir, la fecha de aprobación de la póliza. **16.-** Informar al CONTRATISTA el vencimiento de la póliza o la ampliación de la misma, cuando a ello hubiere lugar. **17.-** Comunicar al Grupo de Contratos con la debida sustentación técnica la elaboración de prorrogas y/o cualquier cambio en el desarrollo del contrato. **18.-** Remitir periódica y oportunamente al Grupo de Contratos los documentos tales como: Actas de inicio, Actas de cumplimiento del servicio a satisfacción, Actas de Liquidación, Órdenes de pago, Certificaciones de Cumplimiento, Facturas, Parafiscales y demás que surjan como consecuencia de la ejecución del presente contrato (según el caso). **19.-** Exigir al contratista el cumplimiento de las especificaciones técnicas ofrecidas por este en su propuesta. **20.-** Avalar los documentos soporte para los pagos. **21.-** Las demás inherentes a su calidad de supervisor, que surjan durante el contrato y que tengan como justificación la ejecución del mismo. **NOVENA.-** OBLIGACIONES DEL CONTRATISTA: **1**.- Ejecutar idónea y oportunamente el objeto del contrato. **2**.- Cumplir las órdenes e instrucciones que le imparta el FONDO y atender sus requerimientos, efectuados a través del supervisor del contrato. **3**.- Elaborar conjuntamente con el Supervisor las

4

Annexes

Page 5: 2011-8/22 DAS contract Verint



201

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

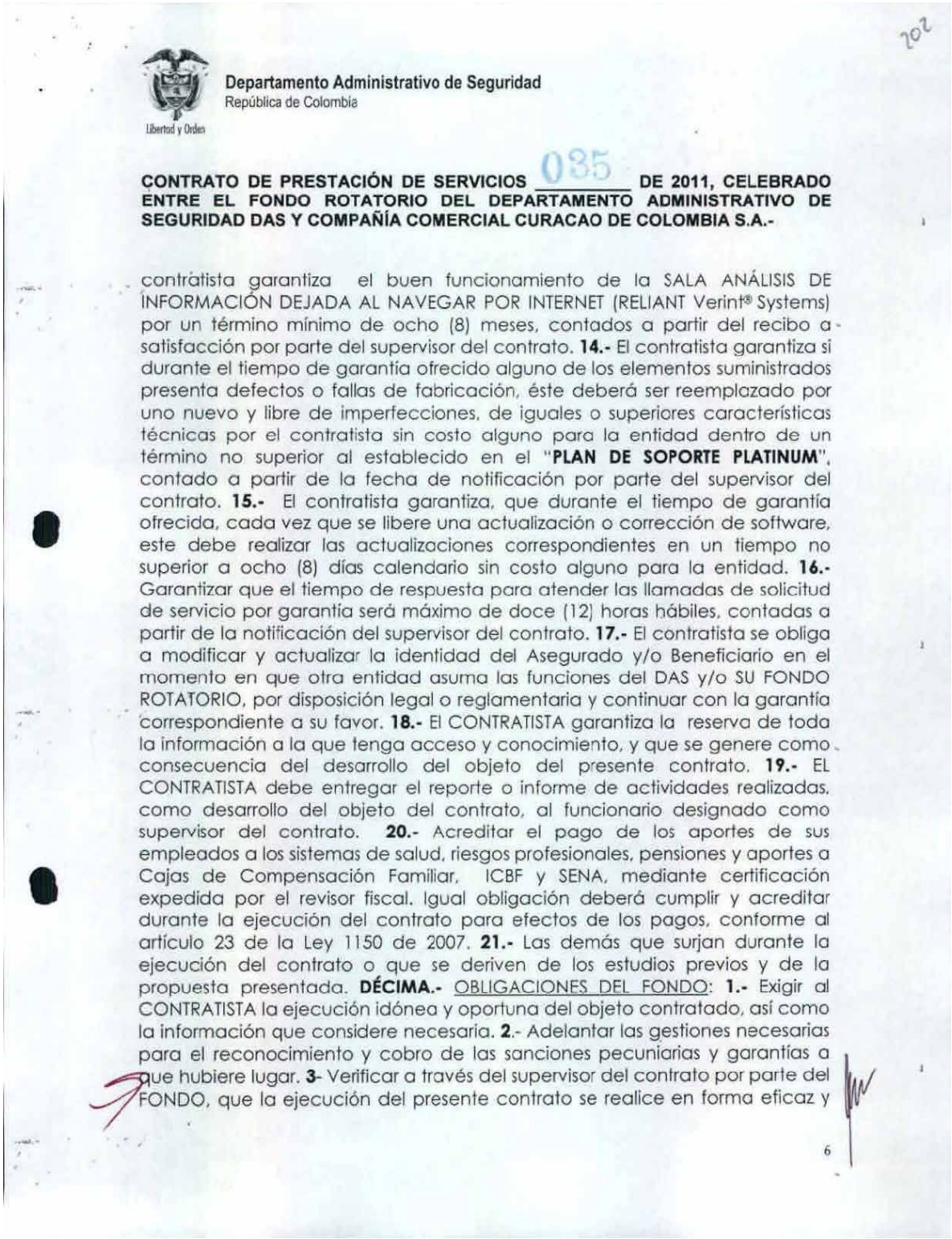
CONTRATO DE PRESTACIÓN DE SERVICIOS 085 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

actas de inicio, relación de servicio, de liquidación del contrato y demás que se generen en el desarrollo del contrato. **4.-** El contratista garantiza que el servicio de mantenimiento preventivo, correctivo y de actualizaciones debe cubrir en su totalidad la solución sistema de la sala de análisis de información registrada al navegar por internet RELIANT de Verint ® System, así como la sonda táctica en cualquier lugar del país donde se encuentre operando. **5.-** Garantizar el pleno funcionamiento e integridad de la solución sistema de la sala de análisis de información registrada al navegar por Internet RELIANT de Verint® Systems. **6.-** El contratista garantiza el pleno funcionamiento de la red lógica con todos los accesorios de conectividad y la red, para la solución adquirida. **7.-** El contratista garantiza un (1) mantenimiento preventivo ON SITE cada tres (3) meses, el cual debe contar con los suministros necesarios para un correcto funcionamiento que conforman la solución. Así mismo debe garantizar el aseo físico de los mismos, test de operatividad tanto de hardware como de software de solución, así como al cableado (voz, datos y energía), circuito cerrado de televisión, accesos biométricos, sistemas contraincendios y sistemas de desagüe (carpa invertida), de presentarse anomalías en los test, se realizará la corrección de estos de acuerdo al plan de soporte PLATINUM a la brevedad posible. **8.-** El contratista garantiza que los mantenimientos correctivos se realicen cada vez que se requieran o quede fuera de servicio uno de los componentes que conforman la solución descrita anteriormente, los cuales se deben atender en un tiempo no mayor a seis (6) horas a partir de la notificación del supervisor del contrato. **9.-** El contratista garantiza la provisión de repuestos, partes y suministros en caso de requerirlos para el pleno funcionamiento en el mantenimiento preventivo y/o correctivo de los bienes que conforman la solución sin costo adicional para la entidad. **10.-** El contratista se obliga con la entidad a realizar el soporte de mantenimiento preventivo y correctivo de la plataforma tecnológica de la "Sala de Análisis de Información Dejada al Navegar por Internet" de acuerdo al **"PLAN DE SOPORTE PLATINUM"** ofrecido por el contratista, que brinda el nivel de soporte Platinum para los equipos Verint Systems. **11.-** El contratista Suministrara durante la vigencia del contrato la recarga del cilindro de 76 LB Cyllinder/valve assy, modelo SEV-PCV140079 en el momento de un siniestro y sea necesaria la utilización de la recarga existente. Con el fin de garantizar pleno funcionamiento del sistema Contra-Incendios que conforman la solución. **12.-** Realizar la Revisión, prueba y manutención del sistema de desagüe (carpa invertida), acoplada en el cielo raso del centro de análisis de la Sala de Análisis de Información Dejada al Navegar por Internet. **13.-** El

5

Annexes

Page 6: 2011-8/22 DAS contract Verint



202

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

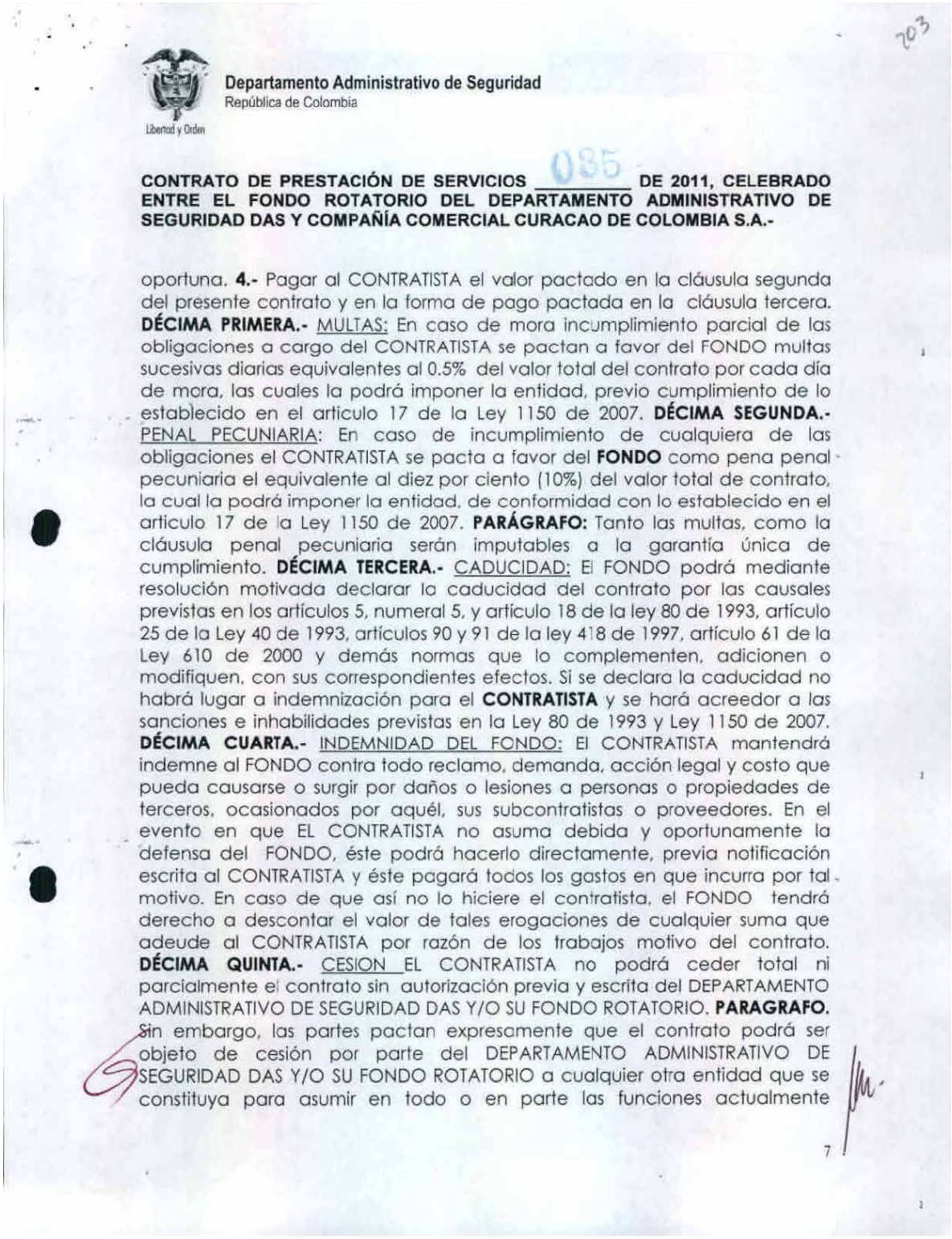
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

contratista garantiza el buen funcionamiento de la SALA ANÁLISIS DE INFORMACIÓN DEJADA AL NAVEGAR POR INTERNET (RELIANT Verint® Systems) por un término mínimo de ocho (8) meses, contados a partir del recibo a satisfacción por parte del supervisor del contrato. **14.-** El contratista garantiza si durante el tiempo de garantía ofrecido alguno de los elementos suministrados presenta defectos o fallas de fabricación, éste deberá ser reemplazado por uno nuevo y libre de imperfecciones, de iguales o superiores características técnicas por el contratista sin costo alguno para la entidad dentro de un término no superior al establecido en el "**PLAN DE SOPORTE PLATINUM**", contado a partir de la fecha de notificación por parte del supervisor del contrato. **15.-** El contratista garantiza, que durante el tiempo de garantía ofrecida, cada vez que se libere una actualización o corrección de software, este debe realizar las actualizaciones correspondientes en un tiempo no superior a ocho (8) días calendario sin costo alguno para la entidad. **16.-** Garantizar que el tiempo de respuesta para atender las llamadas de solicitud de servicio por garantía será máximo de doce (12) horas hábiles, contadas a partir de la notificación del supervisor del contrato. **17.-** El contratista se obliga a modificar y actualizar la identidad del Asegurado y/o Beneficiario en el momento en que otra entidad asuma las funciones del DAS y/o SU FONDO ROTATORIO, por disposición legal o reglamentaria y continuar con la garantía correspondiente a su favor. **18.-** El CONTRATISTA garantiza la reserva de toda la información a la que tenga acceso y conocimiento, y que se genere como consecuencia del desarrollo del objeto del presente contrato. **19.-** EL CONTRATISTA debe entregar el reporte o informe de actividades realizadas, como desarrollo del objeto del contrato, al funcionario designado como supervisor del contrato. **20.-** Acreditar el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a Cajas de Compensación Familiar, ICBF y SENA, mediante certificación expedida por el revisor fiscal. Igual obligación deberá cumplir y acreditar durante la ejecución del contrato para efectos de los pagos, conforme al artículo 23 de la Ley 1150 de 2007. **21.-** Las demás que surjan durante la ejecución del contrato o que se deriven de los estudios previos y de la propuesta presentada. **DÉCIMA.-** OBLIGACIONES DEL FONDO: **1.-** Exigir al CONTRATISTA la ejecución idónea y oportuna del objeto contratado, así como la información que considere necesaria. **2.**- Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones pecuniarias y garantías a que hubiere lugar. **3**- Verificar a través del supervisor del contrato por parte del FONDO, que la ejecución del presente contrato se realice en forma eficaz y

6

Annexes

Page 7: 2011-8/22 DAS contract Verint



203

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

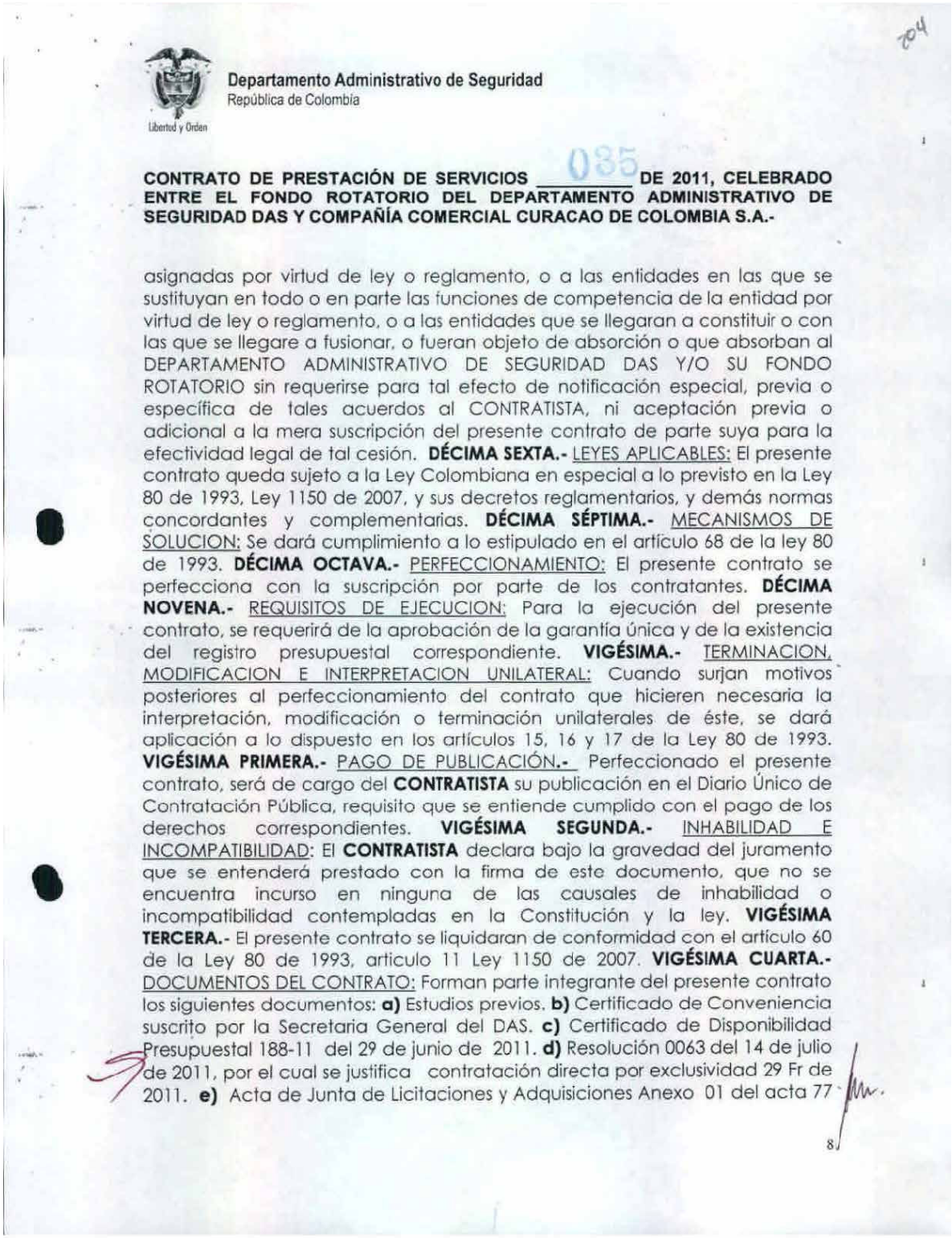
CONTRATO DE PRESTACIÓN DE SERVICIOS 085 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

oportuna. **4.-** Pagar al CONTRATISTA el valor pactado en la cláusula segunda del presente contrato y en la forma de pago pactada en la cláusula tercera. **DÉCIMA PRIMERA.-** MULTAS: En caso de mora incumplimiento parcial de las obligaciones a cargo del CONTRATISTA se pactan a favor del FONDO multas sucesivas diarias equivalentes al 0.5% del valor total del contrato por cada día de mora, las cuales la podrá imponer la entidad, previo cumplimiento de lo establecido en el articulo 17 de la Ley 1150 de 2007. **DÉCIMA SEGUNDA.-** PENAL PECUNIARIA: En caso de incumplimiento de cualquiera de las obligaciones el CONTRATISTA se pacta a favor del **FONDO** como pena penal pecuniaria el equivalente al diez por ciento (10%) del valor total de contrato, la cual la podrá imponer la entidad, de conformidad con lo establecido en el articulo 17 de la Ley 1150 de 2007. **PARÁGRAFO:** Tanto las multas, como la cláusula penal pecuniaria serán imputables a la garantía única de cumplimiento. **DÉCIMA TERCERA.-** CADUCIDAD: El FONDO podrá mediante resolución motivada declarar la caducidad del contrato por las causales previstas en los artículos 5, numeral 5, y artículo 18 de la ley 80 de 1993, artículo 25 de la Ley 40 de 1993, artículos 90 y 91 de la ley 418 de 1997, artículo 61 de la Ley 610 de 2000 y demás normas que lo complementen, adicionen o modifiquen, con sus correspondientes efectos. Si se declara la caducidad no habrá lugar a indemnización para el **CONTRATISTA** y se hará acreedor a las sanciones e inhabilidades previstas en la Ley 80 de 1993 y Ley 1150 de 2007. **DÉCIMA CUARTA.-** INDEMNIDAD DEL FONDO: El CONTRATISTA mantendrá indemne al FONDO contra todo reclamo, demanda, acción legal y costo que pueda causarse o surgir por daños o lesiones a personas o propiedades de terceros, ocasionados por aquél, sus subcontratistas o proveedores. En el evento en que EL CONTRATISTA no asuma debida y oportunamente la defensa del FONDO, éste podrá hacerlo directamente, previa notificación escrita al CONTRATISTA y éste pagará todos los gastos en que incurra por tal motivo. En caso de que así no lo hiciere el contratista, el FONDO tendrá derecho a descontar el valor de tales erogaciones de cualquier suma que adeude al CONTRATISTA por razón de los trabajos motivo del contrato. **DÉCIMA QUINTA.-** CESION EL CONTRATISTA no podrá ceder total ni parcialmente el contrato sin autorización previa y escrita del DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y/O SU FONDO ROTATORIO. **PARAGRAFO.** Sin embargo, las partes pactan expresamente que el contrato podrá ser objeto de cesión por parte del DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y/O SU FONDO ROTATORIO a cualquier otra entidad que se constituya para asumir en todo o en parte las funciones actualmente

7

Annexes

Page 8: 2011-8/22 DAS contract Verint



Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

204

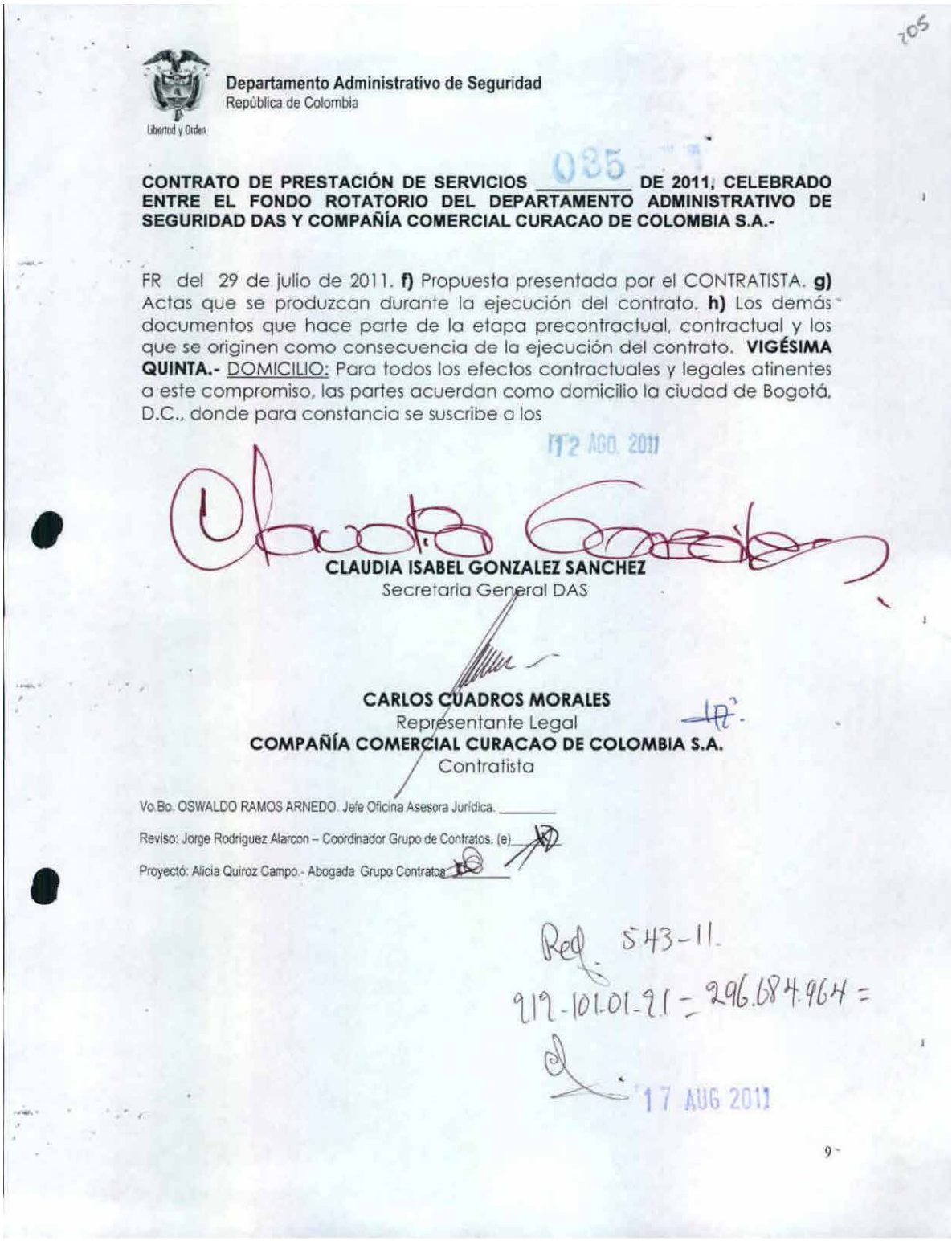
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

asignadas por virtud de ley o reglamento, o a las entidades en las que se sustituyan en todo o en parte las funciones de competencia de la entidad por virtud de ley o reglamento, o a las entidades que se llegaran a constituir o con las que se llegare a fusionar, o fueran objeto de absorción o que absorban al DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y/O SU FONDO ROTATORIO sin requerirse para tal efecto de notificación especial, previa o específica de tales acuerdos al CONTRATISTA, ni aceptación previa o adicional a la mera suscripción del presente contrato de parte suya para la efectividad legal de tal cesión. **DÉCIMA SEXTA.-** LEYES APLICABLES: El presente contrato queda sujeto a la Ley Colombiana en especial a lo previsto en la Ley 80 de 1993, Ley 1150 de 2007, y sus decretos reglamentarios, y demás normas concordantes y complementarias. **DÉCIMA SÉPTIMA.-** MECANISMOS DE SOLUCION: Se dará cumplimiento a lo estipulado en el artículo 68 de la ley 80 de 1993. **DÉCIMA OCTAVA.-** PERFECCIONAMIENTO: El presente contrato se perfecciona con la suscripción por parte de los contratantes. **DÉCIMA NOVENA.-** REQUISITOS DE EJECUCION: Para la ejecución del presente contrato, se requerirá de la aprobación de la garantía única y de la existencia del registro presupuestal correspondiente. **VIGÉSIMA.-** TERMINACION, MODIFICACION E INTERPRETACION UNILATERAL: Cuando surjan motivos posteriores al perfeccionamiento del contrato que hicieren necesaria la interpretación, modificación o terminación unilaterales de éste, se dará aplicación a lo dispuesto en los artículos 15, 16 y 17 de la Ley 80 de 1993. **VIGÉSIMA PRIMERA.-** PAGO DE PUBLICACIÓN.- Perfeccionado el presente contrato, será de cargo del **CONTRATISTA** su publicación en el Diario Único de Contratación Pública, requisito que se entiende cumplido con el pago de los derechos correspondientes. **VIGÉSIMA SEGUNDA.-** INHABILIDAD E INCOMPATIBILIDAD: El **CONTRATISTA** declara bajo la gravedad del juramento que se entenderá prestado con la firma de este documento, que no se encuentra incurso en ninguna de las causales de inhabilidad o incompatibilidad contempladas en la Constitución y la ley. **VIGÉSIMA TERCERA.-** El presente contrato se liquidaran de conformidad con el artículo 60 de la Ley 80 de 1993, articulo 11 Ley 1150 de 2007. **VIGÉSIMA CUARTA.-** DOCUMENTOS DEL CONTRATO: Forman parte integrante del presente contrato los siguientes documentos: **a)** Estudios previos. **b)** Certificado de Conveniencia suscrito por la Secretaria General del DAS. **c)** Certificado de Disponibilidad Presupuestal 188-11 del 29 de junio de 2011. **d)** Resolución 0063 del 14 de julio de 2011, por el cual se justifica contratación directa por exclusividad 29 Fr de 2011. **e)** Acta de Junta de Licitaciones y Adquisiciones Anexo 01 del acta 77

8

Annexes

Page 9: 2011-8/22 DAS contract Verint



705

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

FR del 29 de julio de 2011. **f)** Propuesta presentada por el CONTRATISTA. **g)** Actas que se produzcan durante la ejecución del contrato. **h)** Los demás documentos que hace parte de la etapa precontractual, contractual y los que se originen como consecuencia de la ejecución del contrato. **VIGÉSIMA QUINTA.-** DOMICILIO: Para todos los efectos contractuales y legales atinentes a este compromiso, las partes acuerdan como domicilio la ciudad de Bogotá, D.C., donde para constancia se suscribe a los

12 AGO. 2011

CLAUDIA ISABEL GONZALEZ SANCHEZ
Secretaria General DAS

CARLOS CUADROS MORALES
Representante Legal
COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.
Contratista

Vo.Bo. OSWALDO RAMOS ARNEDO. Jefe Oficina Asesora Jurídica. _____

Reviso: Jorge Rodriguez Alarcon – Coordinador Grupo de Contratos. (e) _____

Proyectó: Alicia Quiroz Campo.- Abogada Grupo Contratos _____

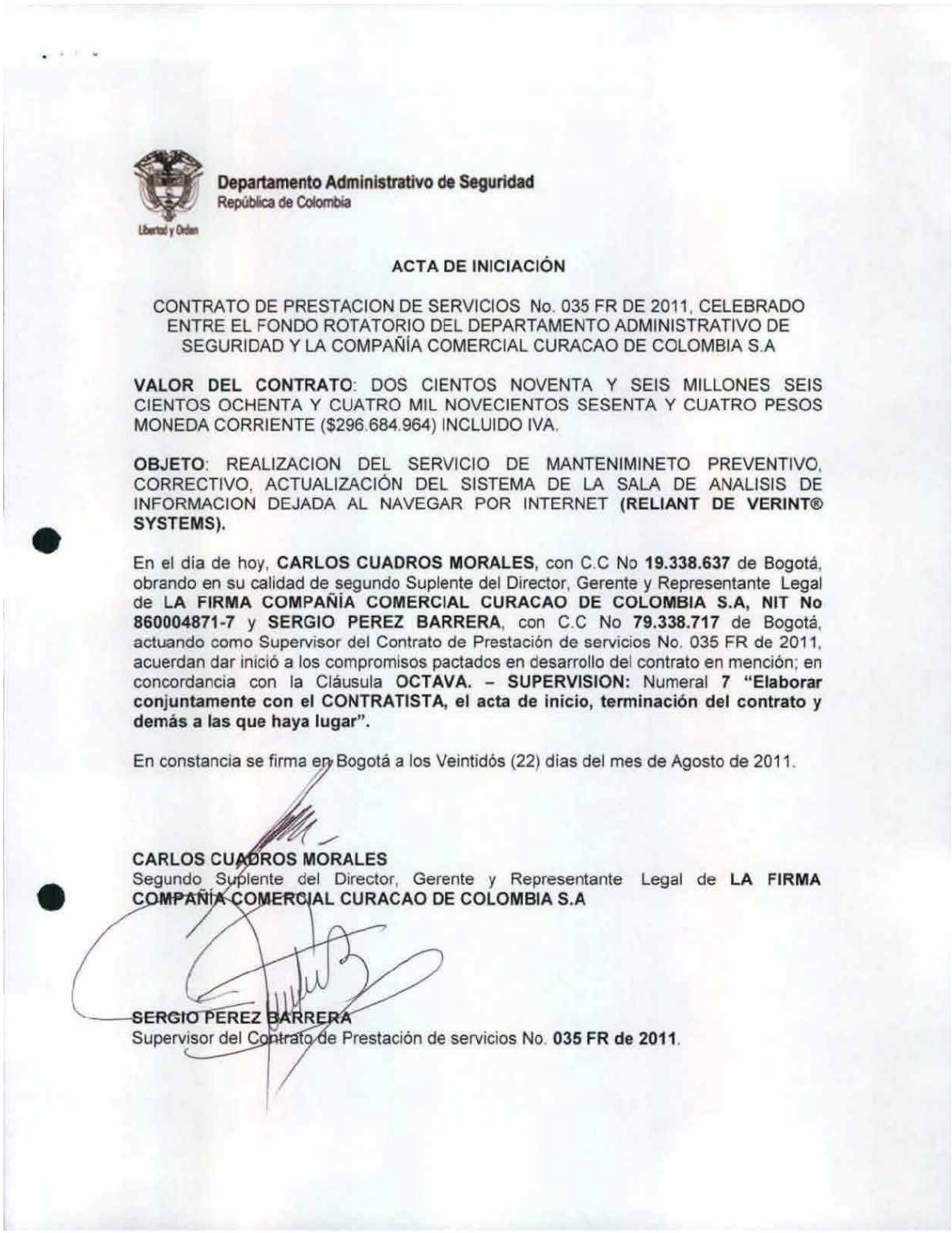
Rad. 543-11.
919-101.01-21 = 296.684.964 =

17 AUG 2011

9

Annexes

Page 10: 2011-8/22 DAS contract Verint



Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

ACTA DE INICIACIÓN

CONTRATO DE PRESTACION DE SERVICIOS No. 035 FR DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD Y LA COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A

VALOR DEL CONTRATO: DOS CIENTOS NOVENTA Y SEIS MILLONES SEIS CIENTOS OCHENTA Y CUATRO MIL NOVECIENTOS SESENTA Y CUATRO PESOS MONEDA CORRIENTE ($296.684.964) INCLUIDO IVA.

OBJETO: REALIZACION DEL SERVICIO DE MANTENIMINETO PREVENTIVO, CORRECTIVO, ACTUALIZACIÓN DEL SISTEMA DE LA SALA DE ANALISIS DE INFORMACION DEJADA AL NAVEGAR POR INTERNET **(RELIANT DE VERINT® SYSTEMS).**

En el día de hoy, **CARLOS CUADROS MORALES**, con C.C No **19.338.637** de Bogotá, obrando en su calidad de segundo Suplente del Director, Gerente y Representante Legal de **LA FIRMA COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A, NIT No 860004871-7** y **SERGIO PEREZ BARRERA**, con C.C No **79.338.717** de Bogotá, actuando como Supervisor del Contrato de Prestación de servicios No. 035 FR de 2011, acuerdan dar inició a los compromisos pactados en desarrollo del contrato en mención; en concordancia con la Cláusula **OCTAVA. – SUPERVISION:** Numeral **7 "Elaborar conjuntamente con el CONTRATISTA, el acta de inicio, terminación del contrato y demás a las que haya lugar".**

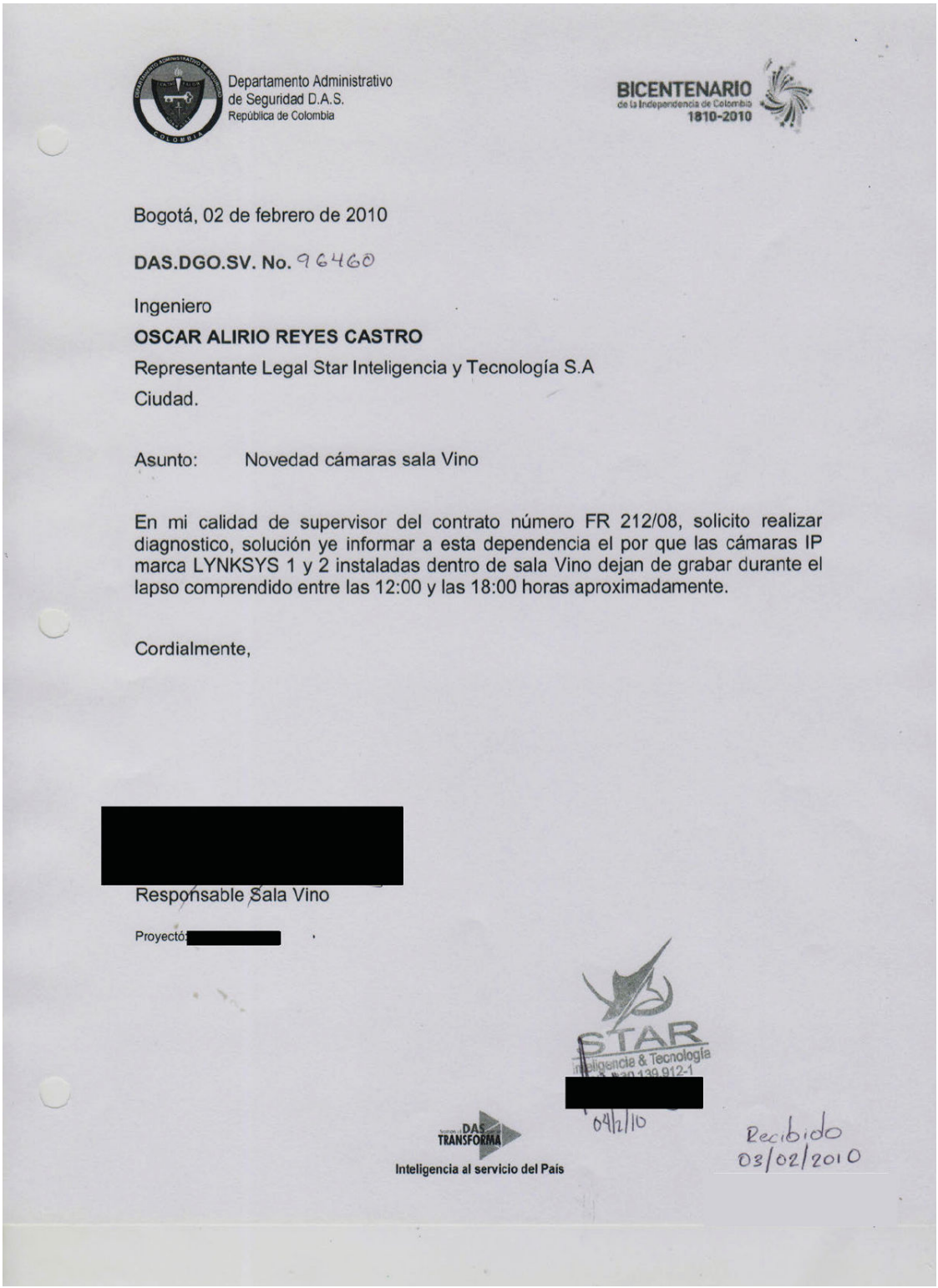
En constancia se firma en Bogotá a los Veintidós (22) dias del mes de Agosto de 2011.

CARLOS CUADROS MORALES
Segundo Suplente del Director, Gerente y Representante Legal de **LA FIRMA COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A**

SERGIO PEREZ BARRERA
Supervisor del Contrato de Prestación de servicios No. **035 FR de 2011**.

Annexes

Annex - Error Messages



Departamento Administrativo
de Seguridad D.A.S.
República de Colombia

BICENTENARIO
de la Independencia de Colombia
1810-2010

Bogotá, 02 de febrero de 2010

DAS.DGO.SV. No. 96460

Ingeniero
OSCAR ALIRIO REYES CASTRO
Representante Legal Star Inteligencia y Tecnología S.A
Ciudad.

Asunto: Novedad cámaras sala Vino

En mi calidad de supervisor del contrato número FR 212/08, solicito realizar diagnostico, solución ye informar a esta dependencia el por que las cámaras IP marca LYNKSYS 1 y 2 instaladas dentro de sala Vino dejan de grabar durante el lapso comprendido entre las 12:00 y las 18:00 horas aproximadamente.

Cordialmente,

[redacted]

Responsable Sala Vino

Proyectó: [redacted]

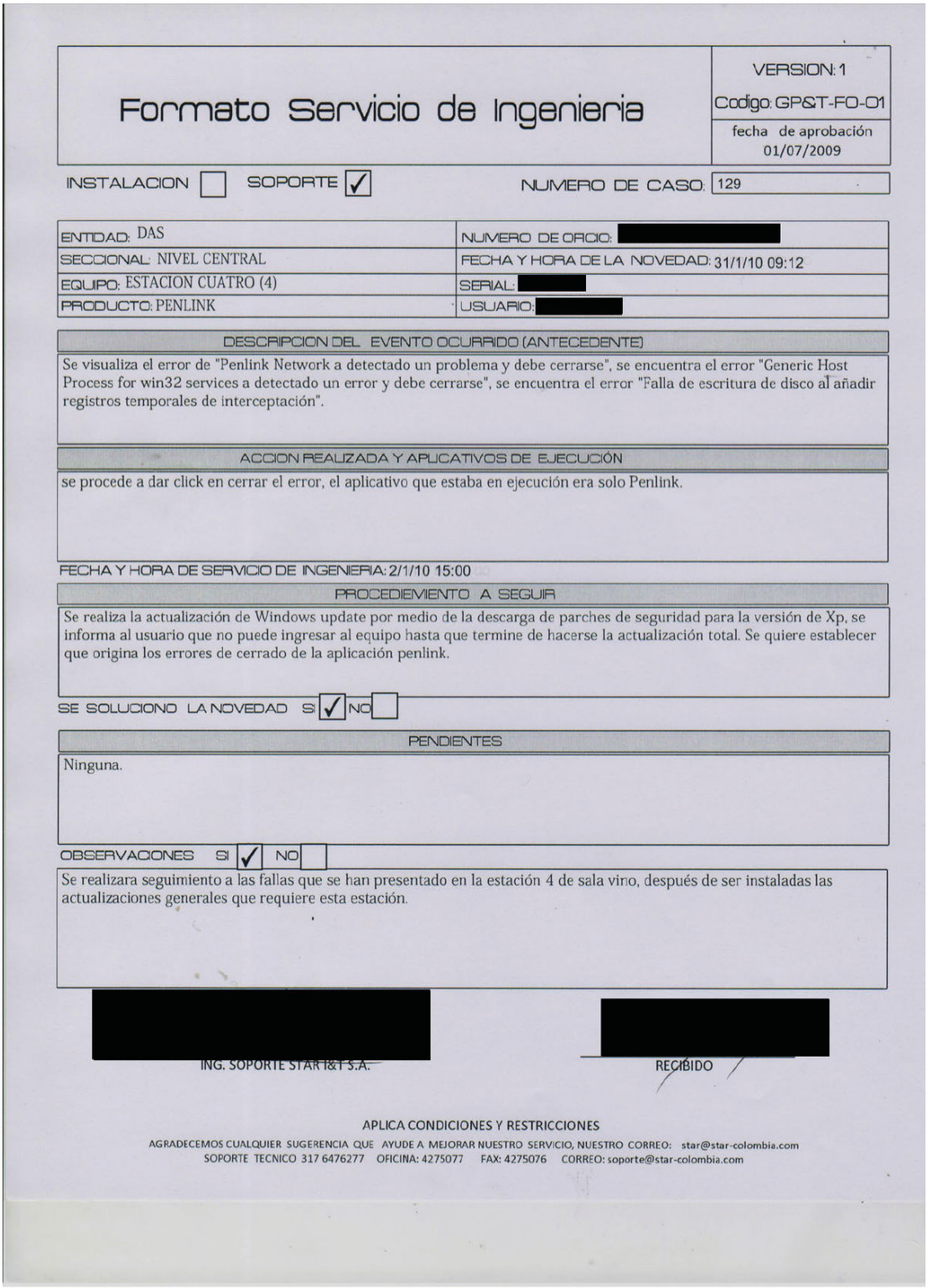
STAR
Inteligencia & Tecnología
[redacted]
04/2/10

DAS TRANSFORMA
Inteligencia al servicio del País

Recibido
03/02/2010

Annexes

Annex - Error Messages



Formato Servicio de Ingenieria

VERSION: 1
Codigo: GP&T-FO-01
fecha de aprobación 01/07/2009

INSTALACION ☐ SOPORTE ☑ NUMERO DE CASO: 129

ENTIDAD: DAS	NUMERO DE ORDIO: [redacted]
SECCIONAL: NIVEL CENTRAL	FECHA Y HORA DE LA NOVEDAD: 31/1/10 09:12
EQUIPO: ESTACION CUATRO (4)	SERIAL: [redacted]
PRODUCTO: PENLINK	USUARIO: [redacted]

DESCRIPCION DEL EVENTO OCURRIDO (ANTECEDENTE)

Se visualiza el error de "Penlink Network a detectado un problema y debe cerrarse", se encuentra el error "Generic Host Process for win32 services a detectado un error y debe cerrarse", se encuentra el error "Falla de escritura de disco al añadir registros temporales de interceptación".

ACCION REALIZADA Y APLICATIVOS DE EJECUCIÓN

se procede a dar click en cerrar el error, el aplicativo que estaba en ejecución era solo Penlink.

FECHA Y HORA DE SERVICIO DE INGENIERIA: 2/1/10 15:00

PROCEDIEMIENTO A SEGUIR

Se realiza la actualización de Windows update por medio de la descarga de parches de seguridad para la versión de Xp, se informa al usuario que no puede ingresar al equipo hasta que termine de hacerse la actualización total. Se quiere establecer que origina los errores de cerrado de la aplicación penlink.

SE SOLUCIONO LA NOVEDAD SI ☑ NO ☐

PENDIENTES

Ninguna.

OBSERVACIONES SI ☑ NO ☐

Se realizara seguimiento a las fallas que se han presentado en la estación 4 de sala vino, después de ser instaladas las actualizaciones generales que requiere esta estación.

[redacted]
ING. SOPORTE STAR I&T S.A.

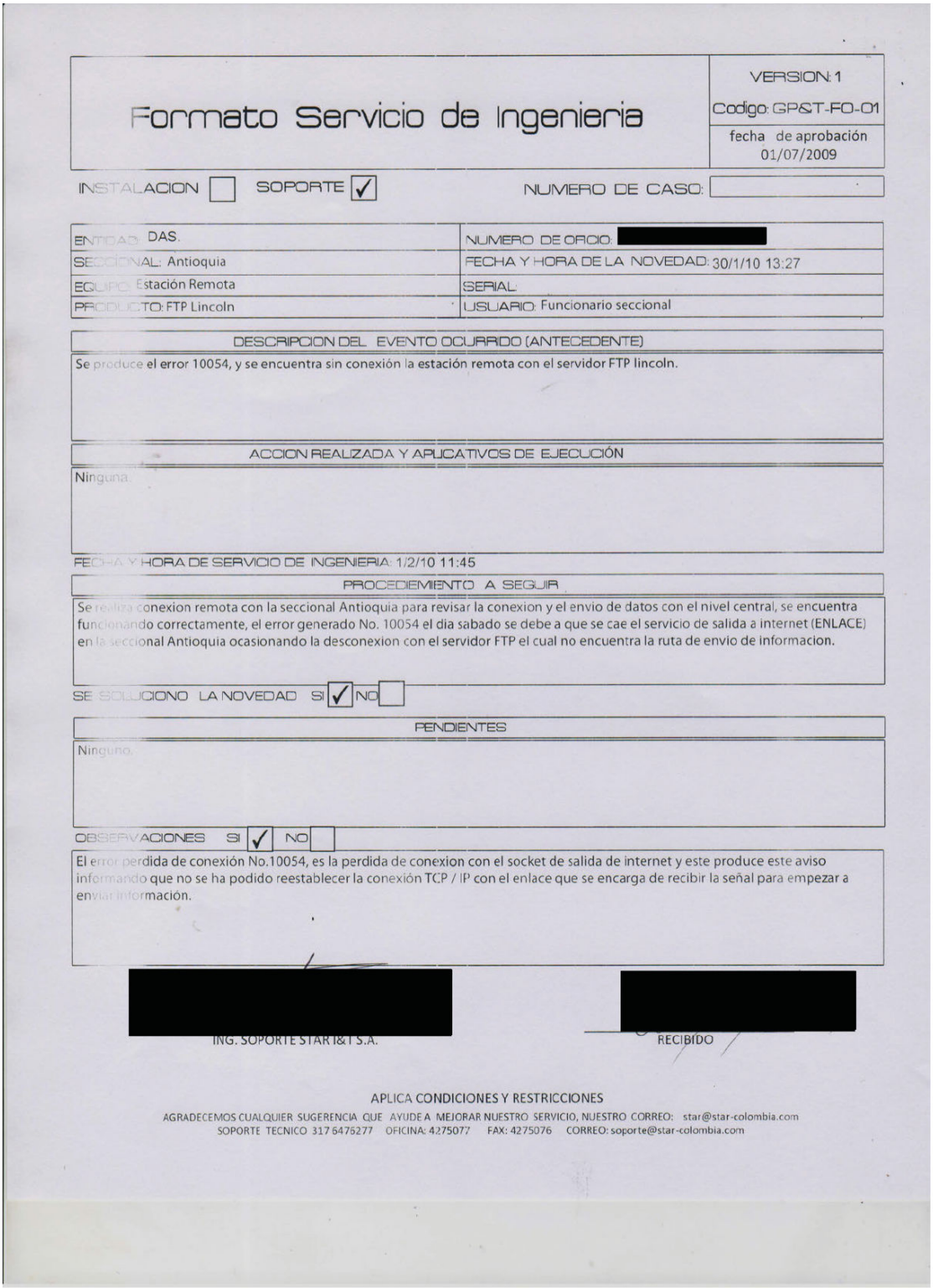
[redacted]
RECIBIDO

APLICA CONDICIONES Y RESTRICCIONES

AGRADECEMOS CUALQUIER SUGERENCIA QUE AYUDE A MEJORAR NUESTRO SERVICIO, NUESTRO CORREO: star@star-colombia.com
SOPORTE TECNICO 317 6476277 OFICINA: 4275077 FAX: 4275076 CORREO: soporte@star-colombia.com

Annexes

Annex - Error Messages



Formato Servicio de Ingenieria

VERSION: 1
Codigo: GP&T-FO-01
fecha de aprobación 01/07/2009

INSTALACION ☐ SOPORTE ☑ NUMERO DE CASO:

ENTIDAD: DAS.	NUMERO DE ORDIO: [redacted]
SECCIONAL: Antioquia	FECHA Y HORA DE LA NOVEDAD: 30/1/10 13:27
EQUIPO: Estación Remota	SERIAL:
PRODUCTO: FTP Lincoln	USUARIO: Funcionario seccional

DESCRIPCION DEL EVENTO OCURRIDO (ANTECEDENTE)

Se produce el error 10054, y se encuentra sin conexión la estación remota con el servidor FTP lincoln.

ACCION REALIZADA Y APLICATIVOS DE EJECUCIÓN

Ninguna.

FECHA Y HORA DE SERVICIO DE INGENIERIA: 1/2/10 11:45

PROCEDIEMIENTO A SEGUIR

Se realiza conexion remota con la seccional Antioquia para revisar la conexion y el envio de datos con el nivel central, se encuentra funcionando correctamente, el error generado No. 10054 el dia sabado se debe a que se cae el servicio de salida a internet (ENLACE) en la seccional Antioquia ocasionando la desconexion con el servidor FTP el cual no encuentra la ruta de envio de informacion.

SE SOLUCIONO LA NOVEDAD SI ☑ NO ☐

PENDIENTES

Ninguno.

OBSERVACIONES SI ☑ NO ☐

El error perdida de conexión No.10054, es la perdida de conexion con el socket de salida de internet y este produce este aviso informando que no se ha podido reestablecer la conexión TCP / IP con el enlace que se encarga de recibir la señal para empezar a enviar información.

[redacted]
ING. SOPORTE STAR I&T S.A.

[redacted]
RECIBIDO

APLICA CONDICIONES Y RESTRICCIONES

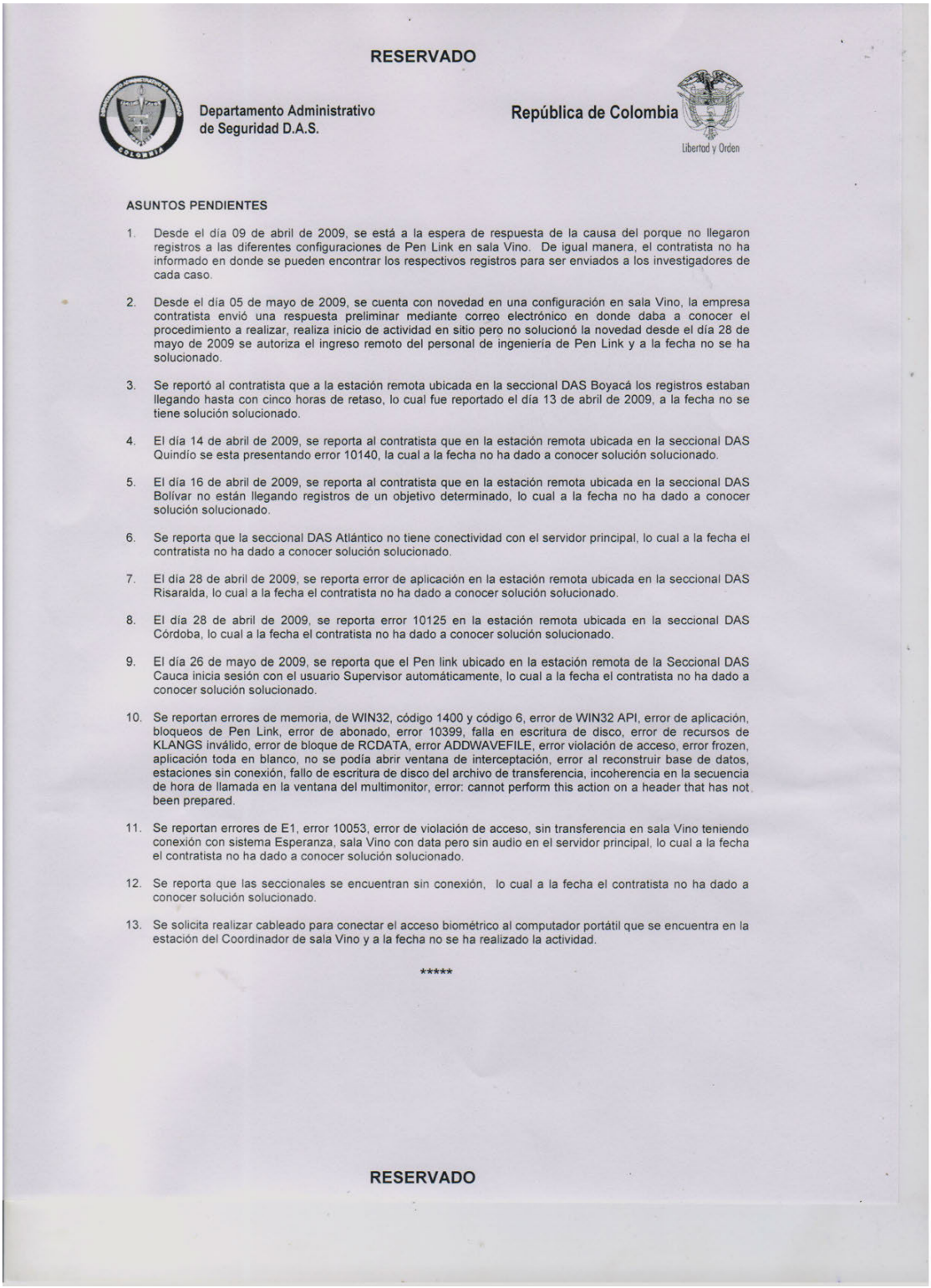
AGRADECEMOS CUALQUIER SUGERENCIA QUE AYUDE A MEJORAR NUESTRO SERVICIO, NUESTRO CORREO: star@star-colombia.com
SOPORTE TECNICO 317 6475277 OFICINA: 4275077 FAX: 4275076 CORREO: soporte@star-colombia.com

Annexes

Annex - Error Messages

Annexes

Annex - Error Messages



RESERVADO

Departamento Administrativo de Seguridad D.A.S.

República de Colombia

Libertad y Orden

ASUNTOS PENDIENTES

1. Desde el día 09 de abril de 2009, se está a la espera de respuesta de la causa del porque no llegaron registros a las diferentes configuraciones de Pen Link en sala Vino. De igual manera, el contratista no ha informado en donde se pueden encontrar los respectivos registros para ser enviados a los investigadores de cada caso.
2. Desde el día 05 de mayo de 2009, se cuenta con novedad en una configuración en sala Vino, la empresa contratista envió una respuesta preliminar mediante correo electrónico en donde daba a conocer el procedimiento a realizar, realiza inicio de actividad en sitio pero no solucionó la novedad desde el día 28 de mayo de 2009 se autoriza el ingreso remoto del personal de ingeniería de Pen Link y a la fecha no se ha solucionado.
3. Se reportó al contratista que a la estación remota ubicada en la seccional DAS Boyacá los registros estaban llegando hasta con cinco horas de retaso, lo cual fue reportado el día 13 de abril de 2009, a la fecha no se tiene solución solucionado.
4. El día 14 de abril de 2009, se reporta al contratista que en la estación remota ubicada en la seccional DAS Quindío se esta presentando error 10140, la cual a la fecha no ha dado a conocer solución solucionado.
5. El día 16 de abril de 2009, se reporta al contratista que en la estación remota ubicada en la seccional DAS Bolívar no están llegando registros de un objetivo determinado, lo cual a la fecha no ha dado a conocer solución solucionado.
6. Se reporta que la seccional DAS Atlántico no tiene conectividad con el servidor principal, lo cual a la fecha el contratista no ha dado a conocer solución solucionado.
7. El día 28 de abril de 2009, se reporta error de aplicación en la estación remota ubicada en la seccional DAS Risaralda, lo cual a la fecha el contratista no ha dado a conocer solución solucionado.
8. El día 28 de abril de 2009, se reporta error 10125 en la estación remota ubicada en la seccional DAS Córdoba, lo cual a la fecha el contratista no ha dado a conocer solución solucionado.
9. El día 26 de mayo de 2009, se reporta que el Pen link ubicado en la estación remota de la Seccional DAS Cauca inicia sesión con el usuario Supervisor automáticamente, lo cual a la fecha el contratista no ha dado a conocer solución solucionado.
10. Se reportan errores de memoria, de WIN32, código 1400 y código 6, error de WIN32 API, error de aplicación, bloqueos de Pen Link, error de abonado, error 10399, falla en escritura de disco, error de recursos de KLANGS inválido, error de bloque de RCDATA, error ADDWAVEFILE, error violación de acceso, error frozen, aplicación toda en blanco, no se podía abrir ventana de interceptación, error al reconstruir base de datos, estaciones sin conexión, fallo de escritura de disco del archivo de transferencia, incoherencia en la secuencia de hora de llamada en la ventana del multimonitor, error: cannot perform this action on a header that has not been prepared.
11. Se reportan errores de E1, error 10053, error de violación de acceso, sin transferencia en sala Vino teniendo conexión con sistema Esperanza, sala Vino con data pero sin audio en el servidor principal, lo cual a la fecha el contratista no ha dado a conocer solución solucionado.
12. Se reporta que las seccionales se encuentran sin conexión, lo cual a la fecha el contratista no ha dado a conocer solución solucionado.
13. Se solicita realizar cableado para conectar el acceso biométrico al computador portátil que se encuentra en la estación del Coordinador de sala Vino y a la fecha no se ha realizado la actividad.

*****

RESERVADO

Annexes

Annex - Palantir presentation with Star Inteligencia

