PRIVACY INTERNATIONAL

Un estado en la sombra: vigilancia y orden público en Colombia

INFORME ESPECIAL

Un estado en la sombra: vigilancia y orden público en Colombia

XXXXXXXXXXXX
Agosto 2015

PRIVACY INTERNATIONAL

www.privacyinternational.org

Bogotá desde el cerro de Monserrate. Crédito: Privacy International (2014).

Índice

Siglas y términos clave

3G	Tercera generación de tecnología de telefonía móvil
4G	Cuarta generación de tecnología de telefonía móvil
ASFADDES	Asociación de Familiares de Detenidos Desaparecidos
CAJAR	Colectivo de Abogados José Alvear Restrepo
CALEA	Communications Assistance for Law Enforcement Act (Ley de Asistencia de Comunicaciones para el Cumplimiento de la Ley) de Estados Unidos
Chuzadas	Término con que se conocen popularmente las interceptaciones y la vigilancia ilegales
CIA	Central Intelligence Agency (Organismo Central de Información) de Estados Unidos
CIJP	Comisión Intereclesial de Justicia y Paz
CSPP	Comité de Solidaridad con los Presos Políticos
CTI	Cuerpo Técnico de Investigación de la Fiscalía
DAS	Departamento Administrativo de Seguridad
DEA	Drugs Enforcement Agency (Administración para el Control de Drogas) de Estados Unidos
DIASE	Dirección Antisecuestro y Antiextorsión
DIJIN	Dirección de Investigación Criminal e INTERPOL
DIPOL	Dirección de Inteligencia Policial
DNI	Dirección Nacional de Inteligencia
E1	Enlace de telecomunicaciones concebido para transmitir comunicaciones de voz y datos
ELN	Ejército de Liberación Nacional
EMS	(Electromagnetic spectrum) espectro electromagnético
Esperanza	Plataforma de interceptación de comunicaciones gestionada por la Fiscalía
ETSI	European Telecommunications Standards Institute (Instituto Europeo de Normas de Telecomunicaciones)
FARC	Fuerzas Armadas Revolucionarias de Colombia
Fiscalía	Fiscalía General de la Nación
GAULA	Grupos de Acción Unificada por la Libertad Personal
IMSI	(International Mobile Subscriber Identity) identidad internacional del abonado móvil
INTERPOL	Organización Internacional de Policía Criminal
IP	Protocolo de Internet
ISP	(Internet service provider) proveedor de servicios de Internet
ONG	Organización no gubernamental
PGP	Pretty Good Privacy, programa de cifrado de datos
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
PUMA	Plataforma Única de Monitoreo y Análisis, sistema de vigilancia administrado por la DIJIN
RCS	Remote Control System (Sistema de Control Remoto), solución de vigilancia de Hacking Team
SIGD	Sistema Integral de Grabación Digital, sistema de vigilancia de las comunicaciones administrado por la DIPOL
SIJIN	Seccional de Investigación Criminal
SMS	(Short message service) servicio de mensajes cortos
TSP	(Telecommunications service provider) proveedor de servicios de telecomunicaciones
VoIP	(Voice over Internet Protocol) protocolo de voz a través de Internet

Resumen ejecutivo

El afán del gobierno por someter a vigilancia las comunicaciones de la ciudadanía va a menudo más allá de la ley. Los poderes irrestrictos de vigilancia amenazan el derecho a la privacidad y otros derechos fundamentales. Hacen imposible la gobernanza democrática. Los ciudadanos temen hablar, pensar y organizarse libremente cuando se enfrentan a un espionaje de sus comunicaciones desproporcionado, injusto y llevado a cabo por motivos políticos.

El gobierno colombiano ha reformado su legislación sobre vigilancia, cuestionado sus capacidades técnicas, e incluso disuelto uno de sus organismos de seguridad tras conocerse el uso indebido de los sistemas de vigilancia. Esta investigación de Privacy International, basada en testimonios y documentos confidenciales, muestra que las recientes reformas se han visto menoscabadas por el despliegue subrepticio de sistemas de vigilancia automatizada y masiva de las comunicaciones, llevado a cabo por varios organismos del Estado fuera del ámbito de lo proscrito por la deficiente legislación colombiana sobre actividades de inteligencia.

La azarosa historia de Colombia es bien conocida. Más de 220.000 personas han perdido la vida desde 1958 en un conflicto brutal, como consecuencia del cual millones más se han visto desplazadas internamente y más de 25.000 han desaparecido, según algunas estimaciones.

La vigilancia de las comunicaciones es parte integrante del conflicto. Las escuchas telefónicas han ayudado a localizar a líderes del grupo rebelde de las FARC. En 2002 se supo que se habían intervenido alrededor de 2.000 líneas telefónicas, entre ellas las de grupos que representaban a familias de las personas desaparecidas. En 2007 se destituyó a 11 generales de la Policía tras saberse que el organismo estaba haciendo escuchas a políticos de la oposición, periodistas, abogados y activistas. En 2009 se reveló que el Departamento Administrativo de Seguridad (DAS) había sometido a vigilancia y hostigamiento a más de 600 figuras públicas. En 2014, la revista Semana reveló que la unidad del ejército colombiano con el nombre en clave de “Andrómeda” había estado espiando durante más de un año al equipo negociador del gobierno en las conversaciones de paz entabladas con las FARC. Los escándalos han conmocionado a la sociedad civil y a los ciudadanos de a pie de Colombia y los han movilizado. Pero también los ha reafirmado en su convencimiento de que se los está monitoreando siempre.

Los principales organismos de Colombia que monitorean las comunicaciones compiten por recursos y capacidades. Debido a ello coexisten sin control sistemas de vigilancia, que se prestan para ser utilizados indebidamente.

El sistema de interceptación de las comunicaciones más notorio de Colombia es Esperanza, que recibe mucho apoyo de la Administración para el Control de Drogas (DEA) de Estados Unidos. La Fiscalía General de la Nación (Fiscalía) gestiona y administra la plataforma, que puede conseguir datos y contenido de llamadas de telefonía móvil y fija. Esperanza, al que tienen acceso varias autoridades policiales,

está conectado a los operadores de telecomunicaciones del país. Se utiliza con el fin de conseguir elementos probatorios para entablar acciones judiciales caso por caso. Es necesario que un agente de la Fiscalía solicite materialmente que se intercepte un registro telefónico concreto, para que esto suceda. Otras salvaguardias incorporadas al sistema Esperanza son su mecanismo de presentación electrónica de órdenes judiciales y los jueces de control de garantías. No obstante, como muestra la presente investigación, Esperanza adolecía de varias vulnerabilidades de seguridad, y su restricción del acceso a datos sólo para objetivos concretos predefinidos y en virtud de una orden judicial era un punto de fricción para otras autoridades policiales.

Pero, aparte de Esperanza, en Colombia existen muchos otros sistemas de interceptación de las comunicaciones, que funcionan ilegalmente o con dudosa justificación legal. La Dirección de Investigación Criminal e INTERPOL (DIJIN) ha creado la Plataforma Única de Monitoreo y Análisis (PUMA), sistema de monitoreo telefónico y de Internet vinculado directamente a la infraestructura de red los proveedores de servicios por una sonda que copia enormes cantidades de datos y los envía directamente al centro de monitoreo de la DIJIN. PUMA tienen capacidad para interceptar y almacenar potencialmente todas las comunicaciones que pasan por sus sondas. Los proveedores de servicios de comunicaciones conocen su existencia y han colaborado en su instalación, pero están excluidos de su funcionamiento diario.

PUMA fue adquirido en 2007. En 2013, la Policía presentó propuestas para su ampliación, alegando que de este modo el sistema podría captar el triple de datos y llamadas telefónicas. La ampliación de PUMA incluía un módulo de monitoreo para proveedores de servicios de Internet (PSI) y hasta 700 estaciones de trabajo en todo el país. Sin embargo, la falta de acuerdo entre la Fiscalía y la Policía acerca de su gestión impidió la ampliación, por lo que el proyecto quedó en suspenso. De todos modos, todavía se están negociando nuevos contratos.

Mientras la Fiscalía y la DIJIN desplegaban Esperanza y PUMA, respectivamente, la Dirección de Inteligencia Policial (DIPOL) adquirió y desplegó su propio sistema de vigilancia masiva y automatizada de las comunicaciones, el Sistema Integral de Grabación Digital (SIGD). Establecido 2005, el SIGD monitorea el tráfico masivo de comunicaciones por líneas E1 y el tráfico de telefonía móvil 3G. Al igual que PUMA, está instalado con el conocimiento de los proveedores de servicios, y el monitoreo se hace sin su conocimiento. Tras analizar la tecnología, consideramos que el sistema puede recopilar 100 millones de registros de datos de llamada al día e interceptar 20 millones de SMS diarios. Este enorme almacén de datos se procesa y combina luego otros tipos de datos, como imágenes, vídeo y datos biométricos.

Este tipo de vigilancia masiva y automatizada no está autorizada de forma expresa por la legislación colombiana. Si bien la Fiscalía podría autorizar la interceptación de las comunicaciones con el fin de buscar elementos probatorios para entablar acciones judiciales, como establecen la Constitución y el Código de Procedimiento Penal, el ejercicio de tal facultad no concuerda con el tipo de monitoreo y análisis en masa y pasivo de Internet y telefónico que PUMA y el SIGD hacen posible.

Las tecnologías que sirven de base a ambos sistemas recopilan y almacenan datos de comunicaciones de manera automática y pasiva, por medio de un conjunto de

sondas vinculadas a un centro de monitoreo. Gracias a ello, la DIPOL y la DIJIN están realizando interceptaciones masivas de comunicaciones sin autoridad legal expresa, y, en el caso de la DIPOL, sin ninguna autoridad legal en absoluto para interceptar comunicaciones.

En el presente informe se establece también que los organismos del gobierno colombiano llevan a cabo vigilancia selectiva. La DIPOL tiene actualmente la capacidad de desplegar falsas estaciones base de telefonía móvil, que pueden monitorear el uso de los teléfonos e interceptar comunicaciones sin la participación de los proveedores de servicios y no necesariamente con el conocimiento de las autoridades judiciales; el DAS también tenía anteriormente tal tecnología. Se sabe que la policía colombiana ha contratado los servicios de empresas de piratería informática y software malicioso (malware) para tener acceso a ordenadores y teléfonos móviles.

En este informe se llega a la conclusión de que los organismos están creando sus propios sistemas de vigilancia en la sombra, sin escrutinio suficiente ni base legal.

Recomendaciones

A la Policía Nacional de Colombia:

- Desclasificar y publicar todos los documentos de contratación de tecnologías para las que la información sobre las capacidades técnicas es de dominio público.
- Desclasificar y publicar todos los documentos de contratación relacionados con la ampliación de la Plataforma Única de Monitoreo y Análisis (PUMA).
- Desclasificar y publicar todos los documentos de contratación relacionados con el Sistema Integral de Grabación Digital con destino a la Policía Nacional
- Confirmar públicamente la existencia de todo contrato con empresas de piratería informática y software malicioso, como la empresa italiana Hacking Team, que esté en vigor en la actualidad o lo haya estado en los últimos 10 años, y especificar la naturaleza de tales contratos.

A la Fiscalía General de la Nación:

- Examinar las repercusiones de los datos presentados aquí acerca de la adquisición y mantenimiento por el DAS de una sonda de interceptación de Verint y de tecnologías de vigilancia táctica tecnológicamente independientes, como dispositivos IMSI catchers, para establecer la presunta conducta ilegal del DAS antes de su disolución.

A la comisión legal de seguimiento a las actividades de inteligencia y contrainteligencia del Senado:

- Celebrar una audiencia para determinar la naturaleza, tipo y número de actividades de monitoreo llevadas a cabo por los organismos nacionales de policía y de inteligencia de Colombia en virtud del artículo 17 de la Ley de Inteligencia de 2003 y recomendar en consecuencia las debidas reformas.
- Realizar una investigación para determinar si las salvaguardias que establece la Ley 1621 de 2013 son suficientes para evitar prácticas indebidas y mantener la confianza pública.
- Realizar una investigación para determinar hasta qué punto se utiliza en la actualidad la tecnología descrita en el presente informe, prestando atención en particular a las instituciones con acceso a este tipo de tecnologías.
- Pedir una revisión de los contratos, documentos de contratación y políticas existentes para su entrega a comités del Congreso a fin de que conozcan y examinen las capacidades de vigilancia existentes.

- Realizar una investigación para determinar si la obligación de los proveedores de servicios de telecomunicaciones de conservar los datos durante un mínimo de cinco años, establecida por el Decreto 1704 de 2012, es proporcional.
- Publicar todo informe de transparencia que proporcione a la comisión la Dirección Nacional de Inteligencia (DNI) en relación con sus actividades.
- Publicar las conclusiones de las investigaciones antedichas.

A la Procuraduría General de la Nación:

- Investigar si los miembros de la DIJIN y la DIPOL encargados de la contratación han actuado dentro del ámbito de su mandato legal, especialmente al contratar, adquirir y desplegar tecnologías de vigilancia.
- Publicar las conclusiones de las investigaciones antedichas.

Al Superintendente Delegado para la Protección de Datos Personales:

- Determinar qué repercusiones puede tener la revelación de la vigilancia masiva en Colombia en el cumplimiento de la legislación sobre protección de datos.
- Publicar las conclusiones de la investigación antedicha.

A la Defensoría del Pueblo:

- Determinar si el despliegue de PUMA por la Fiscalía y la Policía es compatible con las obligaciones nacionales e internacionales contraídas por Colombia en materia de derechos humanos.
- Publicar las conclusiones de la investigación antedicha.

El Capitolio Nacional de Colombia, sede del Congreso Nacional, en la plaza de Bolívar, Bogotá. Crédito: Privacy International (2014).

Introducción

A lo largo del último decenio, el Estado colombiano ha estado creando una arquitectura de vigilancia masiva, sin autoridad legal clara ni salvaguardias adecuadas contra el uso indebido, y sin que haya habido tampoco posibilidades suficientes de escrutinio público. En un país donde se ha visto utilizar de manera habitual la vigilancia de las comunicaciones para someter a hostigamiento a quienes critican las políticas del gobierno, controlar en todo momento a los funcionarios públicos y comprometer las iniciativas de resolución pacífica del persistente conflicto armado, la ampliación del Estado de vigilancia en la sombra de Colombia es un grave motivo de preocupación.

El presente documento de Privacy International es el primero de dos informes donde se saca a la luz la arquitectura de vigilancia de Colombia. La organización pone de relieve en él las deficiencias jurídicas y las condiciones políticas que han dado lugar a la ampliación de las capacidades de vigilancia masiva, así como las consecuencias de ésta para Colombia, basándose para ello en archivos públicos, en documentos que eran anteriormente confidenciales y en el testimonio de personas relacionadas directamente con estos sistemas de interceptación.

Las capacidades de vigilancia del Estado colombiano han aumentado paralelamente a las operaciones militares emprendidas contra las principales guerrillas del país.[1] No obstante, en los informes sobre desapariciones forzadas y ejecuciones extrajudiciales abundan los indicios de interceptación ilegal de comunicaciones privadas, y se han producido varios escándalos en el país por el ejercicio indebido de las capacidades de interceptación por parte de diversos organismos públicos.

Desde finales de la década de 1990, la interceptación legal de comunicaciones en redes colombianas se efectúa por medio de Esperanza, sistema de interceptación que gestiona la Fiscalía General de la Nación (Fiscalía) y al que tienen acceso la Policía y, antes de su disolución, el Departamento Administrativo de Seguridad (DAS).

Desde el punto de vista de su funcionamiento, Esperanza es un sistema de interceptación selectiva, que se basa en solicitudes activas de usuarios humanos, los administradores de la Fiscalía, para “encargar” a los proveedores de servicios de

1 En este informe se tratan las capacidades de monitoreo e interceptación de las comunicaciones de los organismos encargados de hace cumplir la ley y los servicios de inteligencia colombianos, no de las fuerzas armadas. En Colombia, la Policía y el Ejército son dos elementos de la “fuerza pública”, que depende del Ministerio de Defensa. Las fuerzas armadas de Colombia realizan considerables actividades de interceptación y monitoreo en el curso de sus operaciones contra los grupos armados. Privacy International tiene información sobre estas capacidades que prefiere no revelar en este momento por razones de seguridad.

Colombia enviar los registros de datos y audio de llamadas de telefonía fija y móvil, solicitados específicamente. Esta actividad está aprobada expresamente por la Constitución y el Código de Procedimiento Penal de Colombia.

En los últimos años se ha intentado ampliar la capacidad de interceptación de las comunicaciones de Colombia de manera que no esté limitada al uso de Esperanza y abarque también la interceptación automatizada y en gran escala del tráfico telefónico y de correo electrónico en la troncal de la infraestructura de telecomunicaciones del país. Este tipo de interceptación es vigilancia masiva. Potencialmente, permite barrer, filtrar, monitorear y analizar todas las comunicaciones antes de almacenarlas para su posterior examen o borrado. A diferencia de las formas tradicionales de interceptación selectiva, como Esperanza, cuando la empresa de telecomunicaciones o el proveedor de servicios facilitan la interceptación de una determinada línea o número de teléfono, la interceptación masiva permite tomar en masa todos los cables, colocando una sonda directamente en el cable.

Colombia ha adquirido capacidades de vigilancia masiva públicamente y en la sombra. La materialización más pública del intento del gobierno de ampliar sus capacidades de vigilancia es la Plataforma Única de Monitoreo y Análisis (PUMA). Presentada en 2007 como sistema administrado y costeado por la Dirección de Investigación Criminal e INTERPOL (DIJIN), PUMA tiene por objeto interceptar, almacenar y analizar cantidades masivas de tráfico telefónico. En una actualización del sistema de 2014 se incluyeron capacidades de vigilancia masiva del tráfico de Internet. Preocupado por la posibilidad de que el creciente sistema de la Policía violara innecesariamente derechos fundamentales, el fiscal general pidió una suspensión del proyecto en espera de un examen interagencial en agosto de 2014.[2]

La Policía ha descrito PUMA como simple modernización y ampliación de las actuales capacidades legales de interceptación de Esperanza. Lo cierto es que PUMA realiza una forma de vigilancia completamente distinta y mucho más invasiva. No sólo es preocupante desde la perspectiva de la transparencia y la rendición de cuentas, sino que también se plantean serias dudas con respecto a la base legal del sistema. La interceptación sólo es legal en Colombia si se realiza en virtud de una orden judicial y tras las formalidades que establece la ley. En casos excepcionales, la Fiscalía puede proceder a interceptar las comunicaciones sin orden judicial, pero se requiere entonces autoridad judicial ex post para utilizar los datos. El Código de Procedimiento Penal dispone que la Fiscalía interceptará las comunicaciones únicamente con la finalidad de obtener elementos probatorios en procedimientos judiciales. La interceptación masiva o automatizada de las comunicaciones con fines de recopilación de información de inteligencia no está contemplada ni autorizada expresamente en la legislación colombiana, sin embargo la DIJIN afirma que la adquisición de PUMA –que permite la interceptación masiva y automatizada de las comunicaciones– es legal.

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

Privacy International puede también revelar que la Policía colombiana ha participado además en la creación de una arquitectura de interceptación en la sombra sin autoridad legal clara ni escrutinio público, y que, antes de su disolución, el DAS tenía capacidad técnica para realizar interceptaciones de comunicaciones al margen de Esperanza. La Dirección de Inteligencia Policial (DIPOL) intercepta enormes volúmenes de señales de comunicaciones que viajan por la troncal de telecomunicaciones de Colombia a través de sondas de red conectadas a una plataforma para centro de monitoreo llamada Sistema Integral de Grabación Digital (SIGD). Este centro de monitoreo recibe, procesa y retiene datos recopilados por diversos sistemas de vigilancia, como monitoreo de Internet, monitoreo de ubicación, monitoreo de teléfonos y audio vigilancia. Una vez recopilados, estos datos son analizados por potentes ordenadores que muestran conexiones entre personas, sus conversaciones y eventos, y elaboran perfiles de las personas y sus contactos.

Además de la Policía, también están adquiriendo estas capacidades intrusivas otros organismos del Estado. El DAS, disuelto en 2011 tras revelarse una investigación de los medios de comunicación que sus agentes habían realizado interceptaciones ilegales, tenía sus propias capacidades de interceptación de redes. El DAS adquirió en algún momento, antes de 2010, una sonda de red que parece que operaba con independencia del sistema Esperanza. La DIPOL, la DIJIN y otros organismos, incluido el DAS hasta su disolución, también han utilizado dispositivos de interceptación de comunicaciones móviles (conocidos genéricamente como IMSI catchers), que permiten la interceptación localizada indiscriminada de todas las llamadas de teléfonos móviles y mensajes de texto en un lugar específico. Asimismo, en 2012, la DIPOL negoció una potencial compra de potente tecnología de inteligencia de código abierto de Palantir, empresa estadounidense de análisis de datos. Esa tecnología le habría permitido aprovechar sus bases de datos ya existentes para analizar y procesar cantidades inmensas de datos y comunicaciones. Además, la Policía adquirió programas de intrusión de la empresa italiana Hacking Team que le permitían la explotación –hackeo y posterior control– selectiva y a distancia de dispositivos de particulares.

Los organismos del Estado que adquieren estas capacidades lo hacen no sólo al margen del escrutinio público, sino también sin autorización legal clara. Ninguno de los organismos anteriormente mencionados está facultado para realizar actividades de interceptación sin solicitar previamente autorización judicial y cumplir las formalidades establecidas por la ley. El Código de Procedimiento Penal dispone que la interceptación de las comunicaciones sólo puede efectuarse por orden del fiscal, en el marco de una investigación judicial y con el fin de buscar elementos probatorios. La Ley de Inteligencia de 2013 confiere amplios poderes de monitoreo del espectro electromagnético, pero tales poderes no autorizan el tipo de interceptación masiva y automatizada de las comunicaciones que efectúan PUMA y el SIGD.

En general, la proliferación de las interceptaciones con la justificación de la recopilación de información de inteligencia es sumamente preocupante. La vigilancia es un instrumento de control político. Las autoridades públicas suelen decir a la

ciudadanía colombiana que la interceptación de sus comunicaciones está sujeta a rigurosas salvaguardias.[3] Entre las salvaguardias incorporadas al sistema Esperanza figura un mecanismo de presentación electrónica de órdenes judiciales y los jueces de control de garantías, protecciones ambas que tienen por objeto controlar la interceptación ilegal.

Sin embargo, incluso el sistema de interceptación legal más estrictamente regulado de Colombia, Esperanza, ha sido utilizado de manera indebida por los organismos del Estado. Como se ha explicado anteriormente, la Fiscalía está investigando en la actualidad al DAS, porque se denunció que sus agentes habían hecho uso indebido de Esperanza presentando solicitudes fraudulentas de interceptación para conseguir acceso ilegal a comunicaciones de particulares. Se denunció que posteriormente los agentes del DAS rastrearon y sometieron a hostigamiento e intimidaciones a periodistas, activistas y políticos colombianos. Sin embargo, estas denuncias de uso indebido no impidieron al DAS comprar e instalar más equipos de vigilancia.

En esta investigación se ha determinado que la policía y los servicios de inteligencia y de seguridad del país fueron y son capaces de realizar actividades de interceptación en gran escala al margen de marco legal colombiano existente. La rivalidad entre diversas autoridades policiales y organismos de inteligencia, cada uno de los cuales actúa con distinto presupuesto y mandato legal, crea una situación en la que el tráfico de comunicaciones de los colombianos está siendo recopilado pasivamente por sistemas distintos, descoordinados y, a menudo, en competencia. Un marco legal excesivamente amplio y muy poco sólido desde el punto técnico hace posible la interceptación de las comunicaciones sin las debidas salvaguardias.

3 En febrero de 2011, el ministro colombiano de Defensa, Juan Carlos Pinzón Bueno, manifestó: "Los colombianos pueden estar seguros que el uso de estas herramientas [tecnologías de vigilancia de las comunicaciones] por parte del Estado se realizan con total apego a la Ley y siempre buscando la seguridad de todos los colombianos", 5 de febrero de 2011, http://www.policia.gov.co/portal/pls/portal/JOHN.NOTICIAS_NUEVAS_DETALLADAS.SHOW?p_arg_names=identificador&p_arg_values=356593

Vigilancia e inseguridad

Las capacidades de vigilancia de los organismos colombianos de inteligencia y policiales han ido en aumento a media que se han ampliado las operaciones militares contra la mayor guerrilla del país, las Fuerzas Armadas Revolucionarias de Colombia (FARC), y su primo pequeño, el Ejército de Liberación Nacional (ELN).[4] El conflicto armado colombiano es el más largo en su género del hemisferio occidental y lo largo de sus más de 50 años han participado en él diversos agentes. Grupos paramilitares, que actuaban a veces en colaboración con partes del Estado, se desmovilizaron oficialmente a mediados de la década de 2000. También se desmovilizaron varias guerrillas de izquierdas en diversas etapas del conflicto. Desde 1958, el conflicto se ha cobrado la vida de casi 220.000 personas,[5] en su mayoría civiles. En el periodo comprendido entre 1985 y 2012 se vieron desplazas internamente 5,7 millones de personas[6] y desaparecieron 25.000.[7]

Álvaro Uribe, partidario de la línea dura, fue elegido presidente en 2002, tras unas fallidas conversaciones de paz que habían permitido a las FARC ampliar su influencia territorial. Durante sus dos mandatos aplicó una "política de seguridad democrática" que tenía por objeto recuperar el control del territorio y eliminar el narcotráfico. Esa política extendió la presencia del ejército a zonas donde anteriormente no había estado activo y aumentó los gastos en defensa, pues se empleó y adiestró a mayor número de soldados y policías y se mejoraron las capacidades de inteligencia. Gran parte de esta actividad se financió por medio del Plan Colombia, programa de Estados Unidos en el marco del cual, entre 2000 y 2011, se proporcionó ayuda a Colombia por valor de más de 8.000 millones de dólares estadounidenses, destinados en su gran parte a las fuerzas militares.[8]

En 2007, con las FARC debilitadas militarmente a causa de una campaña militar constante, el gobierno de Uribe emprendió un plan de seguimiento de la política de seguridad democrática, dirigido a consolidar lo conseguido en el plano militar

4 El Departamento de Estado de Estados Unidos ha incluido a ambos grupos en su lista de organizaciones terroristas extranjeras. 2015, http://www.state.gov/j/ct/rls/other/des/123085.htm

5 Estadísticas del conflicto armado en Colombia, Centro Nacional de Memoria Histórica, http://www.centrodememoriahistorica.gov.co/micrositios/informeGeneral/estadisticas.html

6 "2015 UNHCR country operations profile – Colombia", ACNUR, 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 de mayo de 2014, http://colombiareports.co/ngos-organize-commemoration-week-25000-forcibly-disappeared-colombia/

8 "The Colombia Strategic Development Initiative", Departamento de Estado de Estados Unidos, 14 de abril de 2012, http://www.state.gov/p/wha/rls/fs/2012/187926.htm

mediante el establecimiento de gobernanza civil y la prestación de servicios sociales en zonas remotas.[9] El sucesor de Uribe, Juan Manuel Santos, ha aplicado en gran medida el mismo planteamiento de consolidación. En 2012, Santos entabló conversaciones de paz con las FARC, y los negociadores han llegado ya a acuerdos en varias áreas. Los escándalos de interceptación de las comunicaciones, o "chuzadas", son una característica de la política colombiana en materia de seguridad desde la década de 1990. Las autoridades han estado interviniendo teléfonos al menos desde 1971[10], y la vigilancia ha desempeñado una importante función en las operaciones contra las FARC en los últimos años. Según la información disponible, en 2011 las llamadas de teléfono intervenidas fueron decisivas para localizar al líder supremo de la FARC, Alfonso Cano, que murió posteriormente en un ataque militar.[11] Al parecer, el ejército utilizó el sistema de interceptación Esperanza para localizar al jefe militar de las FARC, Mono Jojoy, a quien también mataron posteriormente.[12]

No obstante, en los informes sobre desapariciones forzadas y ejecuciones extrajudiciales abundan las denuncias de interceptación ilegal de comunicaciones privadas. En estas interceptaciones ilegales han participado distintos organismos. En un caso famoso, los Grupos de Acción Unificada por la Libertad Personal (GAULA), que son unidades conjuntas de la Policía y el ejército, interceptaron ilegalmente más de 2.000 líneas telefónicas, según la Fiscalía en 2002.[13] La afectada fue la Asociación de Familiares de Detenidos Desaparecidos (ASFADDES), al menos dos de cuyos miembros habían desaparecido también ese año. En 2007 se destituyó a 11 generales de la DIPOL tras saberse que el organismo había intervenido los teléfonos de influyentes políticos de la oposición, periodistas, abogados y activistas.[14] En 2014, el semanario colombiano Semana denunció que una unidad del ejército colombiano con el nombre en clave de "Andrómeda" había estado espiando durante más de un año al equipo negociador del gobierno en las conversaciones de paz entabladas con la guerrilla de las FARC.[15]

9 "Política de Consolidación de la Seguridad Democrática", Ministerio de Defensa Nacional de Colombia, 2007, http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Home/Politica_de_Consolidacion_de_la_Seguridad_Democratica.pdfMinistry 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

10 Según el testimonio que el ex director del DAS, Carlos Arzayus, prestó ante la Corte Suprema de Justicia en mayo de 2010. "Un ex director del DAS confirma seguimientos desde 1971 y revela nuevos nombres de personas espiadas", El Diario Exterior, 4 de mayo de 2010, http://www.eldiarioexterior.com/articulo.asp?idarticulo=26464&accion=ext

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

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

13 "Informe sobre Derechos Humanos: Colombia", Departamento de Estado de Estados Unidos, 4 de marzo de 2002, http://www.acnur.org/t3/uploads/media/COI_53.pdf

14 "El DAS-gate y las 'chuzadas', vuelve y juega", El Espectador, 21 de febrero de 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 de febrero de 2014, http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

Pero el más notorio de los escándalos de interceptación afecta al DAS y fue revelado por Semana en febrero de 2009. Los grupos especiales de inteligencia estratégica del DAS sometieron a vigilancia selectiva a alrededor de 600[16] figuras públicas, entre las que había parlamentarios, periodistas, activistas y abogados de derechos humanos y jueces. Según los archivos recuperados en el curso de una investigación de la Fiscalía,[17] el DAS interceptó llamadas telefónicas, tráfico de mensajes de correo electrónico y listas de contactos nacionales e internacionales y utilizó esta información para compilar perfiles psicológicos de los afectados y someter a vigilancia física tanto a ellos como a sus familias, incluidos niños.

La vigilancia de las comunicaciones era un elemento esencial de los abusos del DAS. Las líneas de teléfono del periodista Hollman Morris estuvieron bajo vigilancia casi constante. Morris se vio obligado a exiliarse en varias ocasiones posteriormente. Claudia Duque, abogada y periodista que había trabajado con el Colectivo de Abogados José Alvear Restrepo (CAJAR), sobrevivió a intentos de secuestro y recibió amenazas explícitas de violencia por teléfono; los archivos del DAS sobre ella contenían extensos indicios de vigilancia de las comunicaciones y física.[18] La interceptación ilegal era de tal magnitud, que en el juicio del ex director del DAS en 2011 se recusó a siete magistrados de la Corte Suprema de Justicia porque había indicios de que incluso ellos habían sido espiados ilegalmente.[19]

Aunque al DAS había capeado anteriores escándalos sobre abusos purgando públicamente sus filas, las revelaciones de Semana fueron la gota que colmó el vaso. En el primer discurso que pronunció tras el escándalo, el entonces presidente Álvaro Uribe anunció que ya no se permitía a los servicios de inteligencia del DAS interceptar ninguna conversación telefónica sin autorización de la Policía.[20]

Ante tantos escándalos, el DAS fue disuelto en octubre de 2011. Varios ex directores del organismo fueron declarados culpables de interceptación ilegal y delitos conexos. Fernando Tabares, ex director del DAS, fue declarado culpable de haber intervenido ilegalmente teléfonos de partidarios de la oposición al gobierno en

16 "Más de 600 personas habrían sido 'chuzadas' ilegalmente por el DAS, según investigadores", Caracol Radio, 17 de abril de 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 de junio de 2009, http://www.eltiempo.com/archivo/documento/CMS-5436047

18 "Former security operatives charged in journalist's torture in Colombia", IFEX, 18 de marzo de 2013, https://www.ifex.org/colombia/2013/03/18/security_charged/ y "Colombian official convicted of 'psychological torture' of journalist", Comité para la Protección de los Periodistas (CPJ), 22 de diciembre de 2014, https://cpj.org/2014/12/colombian-official-convicted-of-psychological-tort.php

19 "7 judges withdrawn from wiretap trial", Colombia Reports, 12 de agosto de 2011, http://colombiareports.co/former-das-director-convicted-wiretapping-scandal/

20 No obstante, las investigaciones del DAS basadas en interceptaciones de llamadas telefónicas continuarían, y las salas de monitoreo del organismo seguirían en funcionamiento. "Uribe forbids DAS to independently wiretap suspects", Colombia Reports, 26 de febrero de 2009, http://colombiareports.co/uribe-forbids-das-to-independently-wiretap-suspects/

2010.[21] María del Pilar Hurtado, que dirigió el DAS en 2008, es la autoridad de mayor rango declarada culpable de vigilancia ilegal.[22] En 2011 se estableció un nuevo organismo, la Dirección Nacional de Inteligencia (DNI), para dirigir el sector de la inteligencia y la contrainteligencia dentro de la estructura general del Estado.[23]

Se ha denunciado que el DAS llevaba a cabo las interceptaciones ilegales haciendo uso indebido del sistema Esperanza.[24] Durante la investigación de la Fiscalía, las autoridades del DAS negaron saber que tenían capacidades de interceptación independientes,[25] pero en el presente informe se demuestra que el organismo poseía esas capacidades, al menos en la segunda mitad de la década de 2000. La investigación se centró en cambio en si el DAS tenía o no acceso a Esperanza durante el periodo en que se cometieron los abusos.[26] El presente informe muestra que, desde el punto de vista técnico, el DAS podía interceptar comunicaciones telefónicas y de correo electrónico de manera autónoma, sin depender del sistema Esperanza.

21 "7 judges withdrawn from wiretap trial", Colombia Reports, 12 de agosto de 2011, http://colombiareports.co/former-das-director-convicted-wiretapping-scandal/

22 "'Chuzadas' del DAS: crimen y castigo", Semana, 28 de febrero de 2009, http://www.semana.com/nacion/articulo/chuzadas-del-das-crimen-castigo/419365-3

23 "Preguntas frecuentes", Dirección Nacional de Inteligencia, 2011, http://www.dni.gov.co/index.php?idcategoria=202

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

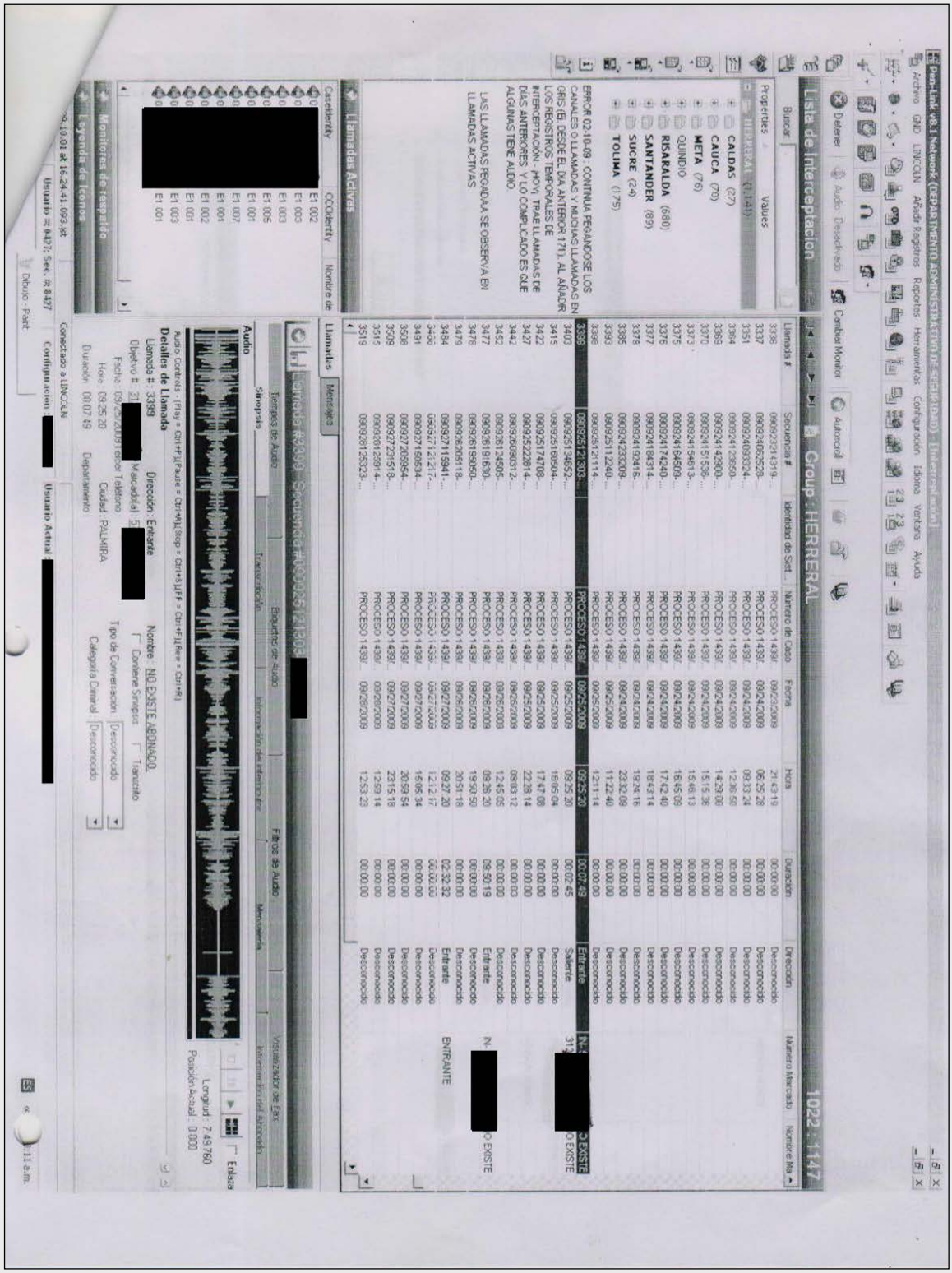
25 "Texto de la sentencia en el caso de las escuchas ilegales del DAS", Juzgado Tercero Penal de Circuito Especializado de Descongestión de Bogotá D.C., 30 de noviembre de 2012, http://www.derechos.org/nizkor/colombia/doc/das299.html#373

26 "Texto de la sentencia en el caso de las escuchas ilegales del DAS", Juzgado Tercero Penal de Circuito Especializado de Descongestión de Bogotá D.C., 30 de noviembre de 2012, http://www.derechos.org/nizkor/colombia/doc/das299.html#373

Esperanza

A principios de la década de 2004, funcionarios de la Fiscalía se reunieron con funcionarios de la Administración para el Control de Drogas (DEA) de Estados Unidos para desarrollar el sistema, que se estableció originalmente en 2004 como "Proyecto Esperanza" y se formalizó en 2005 en virtud el Convenio Interadministrativo 038 de 2005 como sistema conjunto de interceptación de la Fiscalía, la Policía y el DAS.

La interceptación por medio de Esperanza consiste en captar comunicaciones de particulares selectivamente, con el conocimiento y la cooperación del proveedor de servicios de telecomunicaciones, y está autorizada de manera expresa por la legislación colombiana. Esperanza permite a la Fiscalía conectarse a los servidores de los proveedores de servicios de telecomunicaciones para recibir y descomponer en paquetes información de llamadas en tiempo real a fin de transmitirla a una sala central de monitoreo. La señal se envía luego a otras salas de monitoreo controladas por el Cuerpo Técnico de Investigación (CTI) de la Fiscalía, la Policía y el DAS, cuando éste estaba operativo.



QUÉ VEÍA EL DAS

Los analistas consultaban la interfaz del sistema, software de la empresa estadounidense Pen-Link, y veían información de llamadas en tiempo real del teléfono del objetivo.

Esperanza se poya en una plataforma "a medida" montada por la empresa colombiana STAR Inteligencia & Tecnología. STAR es además el proveedor exclusivo de varios productos de empresas británicas y estadounidenses que son también componentes importantes del sistema Esperanza. Se examinan más detenidamente las empresas en el segundo informe de Privacy International, Demand/Supply: Exposing the Surveillance Industry in Colombia ("Oferta y demanda: al descrubeirto la industria de la vigilancia en Colombia").

Crédito: STAR I & T, http://star-it.co/esp/esp_Octopus.html, accessed June 2015)

Octopus es una de las suites de interceptación de la firma de STAR, un switch de interconexión que recibe señales de diferentes protocolos, incluidos GSM (teléfonos móviles), IP (Internet) y protocolos de interceptación legal ETSI y CALEA, y los envía a su destino, un centro de monitoreo de de las autoridades policiales. Credit: STAR I & T, http://star-it.co/esp/esp_Octopus.html, accessed June 2015).

Las interceptaciones por medio de Esperanza se efectúan de la siguiente manera: primero un analista debe presentar a un agente de la Fiscalía un documento de solicitud de interceptación de una determina línea. En ese documento debe exponerse el motivo que justifica la interceptación. El agente de la Fiscalía debe autorizarla y solicitar el direccionamiento de la llamada a través del sistema Esperanza al centro principal de monitorio de la Fiscalía, el "Búnker", situado en su sótano, que debe direccionarlo entonces a cualquiera de las otras salas de monitoreo. Esperanza estaba conectado en 2012 al menos a 20 salas, identificadas por colores. Al menos seis de estas salas recibían apoyo económico y técnico de la DEA, cuyos analistas compartían el espacio de trabajo con sus colegas colombianos[27] La embajada de Estados Unidos está a pocos metros.

27 "Acta nº 448-2009 de Consejo Superior, 3 de Septiembre de 2009", Consejo Superior del Poder Judicial, 3 de septiembre de 2009, http://vlex.co.cr/vid/-456419578

Un arcoíris de salas

Un arcoíris de salas. Las salas conocidas de interceptación de Esperanza tienen nombres de colores; hay 4 principales en la sede central, 15 en las direcciones seccionales de la Fiscalía y 8 salas más de análisis especializado.

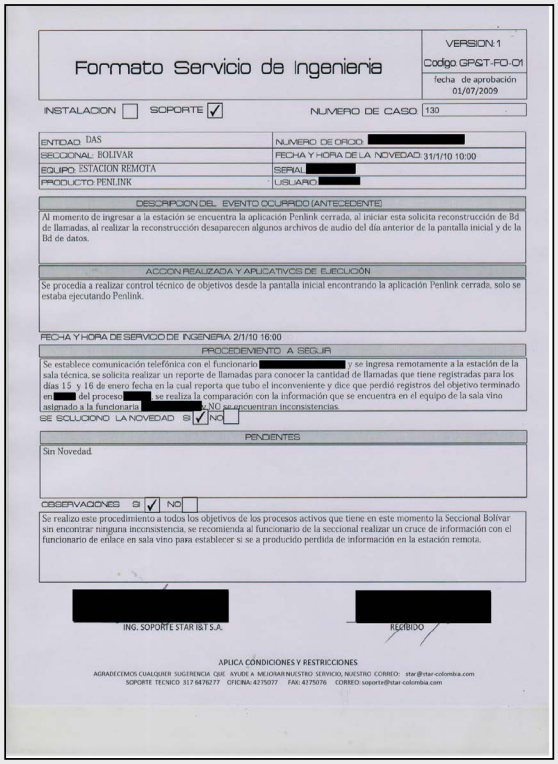
LA SALA ZAFIRO

Situada en Bogotá, calle 18A, No. 69 B, Zafiro es una de las salas de monitoreo y análisis del Cuerpo Técnico de Investigación de la Fiscalía.

Crédito: PI September 2014

Esperanza no ha funcionado siempre según lo previsto. A mediados de 2009, las conexiones entre las salas se interrumpían de manera habitual. Los miembros de la Policía y el DAS enviaban mensajes de pánico solicitando ayuda.

Un resumen de más de 20 denuncias del DAS sobre problemas con el acceso a los datos interceptados se incluye como anexo. Los técnicos de STAR realizaron decenas de visitas a las salas de monitoreo del DAS en 2009 y 2010 para solucionar problemas y hacer mejoras en las plataformas en las que se analizaban los datos interceptados en el sistema Esperanza. A pesar del gran número de fallos técnicos conocidos de Esperanza y de las revelaciones sobre la vigilancia ilegal por parte del DAS de periodistas, activistas y funcionarios públicos, que son de dominio público desde 2008, se ha ampliado continuamente la capacidad del sistema.



Formato Servicio de Ingeniería

VERSION 1
Codigo 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 SEGUIR

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 dias 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 ☐

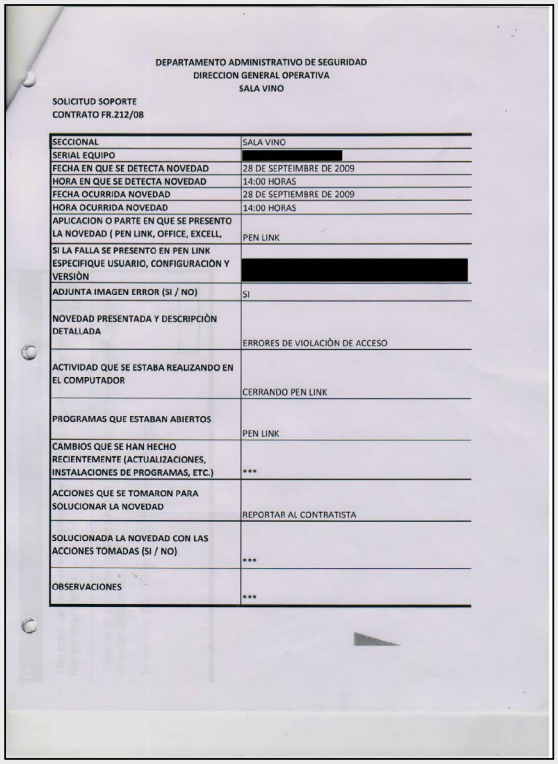
Se realizo este procedimiento a todos los objetivos de los procesos activos que tiene en este momento la Seccional Bolivar sin encontrar ninguna inconsistencia, se recomienda al funcionario de la seccional realizar un cruce de irformación con el funcionario de enlace en sala vino para establecer si se 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 317 6476277 OFICINA 4275077 FAX: 4275076 CORREO soporte@star-colombia.com



DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD
DIRECCION GENERAL OPERATIVA
SALA VINO

SOLICITUD SOPORTE
CONTRATO FR.212/08

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, CONFIGURACIÒN Y VERSIÒN	[redacted]
ADJUNTA IMAGEN ERROR (SI / NO)	SI
NOVEDAD PRESENTADA Y DESCRIPCIÒN DETALLADA	ERRORES DE VIOLACIÒN 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	***

SOLUCIÓN DE PROBLEMAS

Las conexiones entre Esperanza y las salas de los tres organismos se interrumpían de manera habitual.

En la actualidad, Esperanza tiene todavía limitaciones. La Policía se quejó en 2010 de que no podía interceptar mensajes de voz, mensajes de Blackberry ni comunicaciones basadas en el protocolo de Internet (IP).[28] Las autoridades policiales conocen bien estas limitaciones. Ya en 2007, las limitaciones de Esperanza sirvieron de justificación para la adquisición inicial de tecnología nueva y de mayor capacidad, a saber: PUMA. En 2013, los problemas que presentaba aún Esperanza se utilizaron como excusa para la ampliación de PUMA: la Policía quería un sistema de interceptación basado en una tecnología distinta y suministrada por otras empresas.

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

PUMA y la interceptación masiva

El sistema PUMA (Plataforma Única de Monitoreo y Análisis) está basado en tecnologías mucho más potentes e invasivas que las de Esperanza. Esperanza es un switch en el que es necesario que un agente de la Fiscalía solicite a distancia al proveedor de servicios que le envíe información de una determinada línea intervenida. Sin esta solicitud, que se presenta en formato electrónico sobre la base de la aprobación de una solicitud por escrito de interceptación, no puede efectuarse la interceptación.

PUMA, en cambio, intercepta y almacena potencialmente todas las comunicaciones transmitas por los cables de alto volumen que componen la troncal de la que todos los colombianos dependen para hablar entre ellos y enviarse mensajes. No tiene la limitación del número de analistas disponibles para "encargar" a los proveedores de servicios que envíen información ni de los cupos de interceptación por proveedor. La tecnología de PUMA sólo está limitada por la capacidad de almacenaje de los servidores de su centro de monitoreo y la capacidad de las sondas colocadas en los cables de la troncal.

PUMA está vinculado directamente a la infraestructura de red de los proveedores de servicios, por medio de una sondas que direccionan directamente todos los datos al centro de monitoreo de las autoridades policiales, sin necesidad de que lo facilite de nuevo el proveedor de servicios. En la actualidad, PUMA puede interceptar, almacenar y analizar cantidades masivas de tráfico telefónico, y está previsto que crezca y pueda también interceptar el tráfico de Internet.

"Ha habido un crecimiento exponencial de la distancia entre la capacidad técnica de los delincuentes y la nuestra", manifestó un miembro de la DIJIN hablando de la adquisición la PUMA en 2014. El sistema se alojó físicamente en la sede de la Dirección Antisecuestro y Extorsión de la Policía. Los analistas del Grupo de Procesamiento de Señales, Voces e Imágenes de la DIJIN[29] recibían los datos en su instalación principal. En 2007, al principio, PUMA tenía ocho salas de monitoreo repartidas por toda Colombia en sus seccionales de Medellín, Bucaramanga, Cúcuta, Pereira, Villavicencio, Neiva, Cali y Barranquilla. Desde estas salas, los analistas de la Seccional de Investigación Criminal (SIJIN), de la DIJIN, y los Grupos de Acción Unificada por la Libertad Personal (GAULA) monitoreaban las llamadas interceptadas.[30] Asimismo, entre 2011 y 2013, se añadieron en algún momento varias estaciones de trabajo para agentes de la DIPOL.

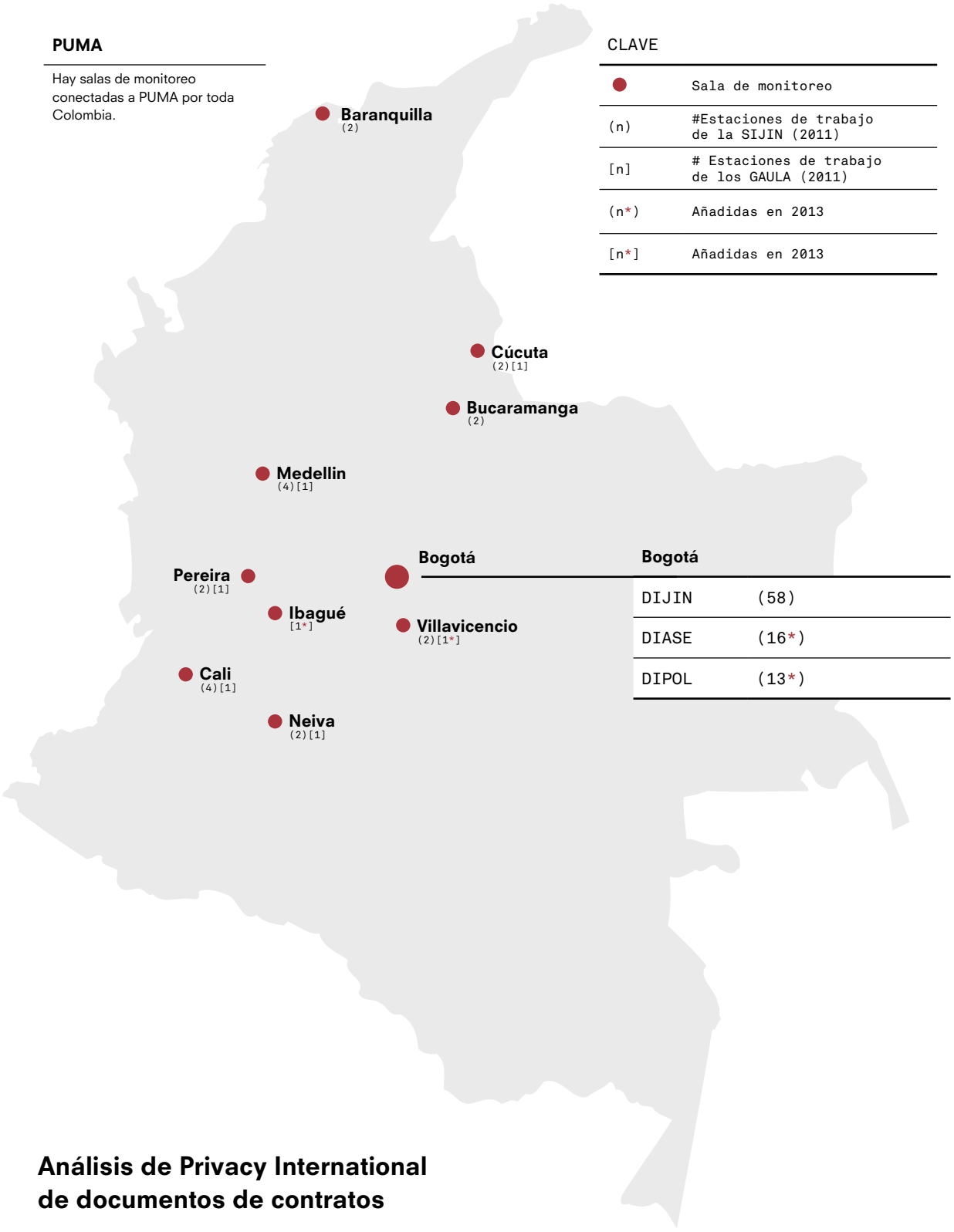
29 "Plan Estadístico de la Policía Nacional", 2008, http://www.policia.gov.co/portal/page/portal/HOME/Lineamientos/Tomo%205.1%20PLAN%20ESTADISTICO.pdf

30 "Resolución No 02049 del 15 Jun. 2007," Policía Nacional de Colombia, 15 de junio de 2007, http://www.policia.gov.co/portal/page/portal/INSTITUCION/normatividad/resoluciones/RESOLUCI%D3N%202049%20DIPOL%20%20150607.doc

Plataforma Única de Monitoreo y Análisis (PUMA)

PUMA

Hay salas de monitoreo conectadas a PUMA por toda Colombia.



CLAVE	
●	Sala de monitoreo
(n)	#Estaciones de trabajo de la SIJIN (2011)
[n]	# Estaciones de trabajo de los GAULA (2011)
(n*)	Añadidas en 2013
[n*]	Añadidas en 2013

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

Análisis de Privacy International de documentos de contratos

PUMA funcionaba con tecnología patentada de la empresa israelí-estadounidense de soluciones de inteligencia Verint Systems, utilizando fundamentalmente la plataforma para centro de monitoreo RELIANT de la empresa.

Tras concluir la Policía los contratos iniciales con la Compañía Comercial Curacao de Colombia ("La Curacao"), representante legal y único distribuidor autorizado de Verint Systems en Colombia,[31] los técnicos de Verint colocaron 16 sondas "IP-PROBER"[32] en las troncales. Los proveedores de servicios conocían su existencia y ayudaron a instalar las conexiones, pero no participaban en su funcionamiento diario, según ex empleados de Verint.

Las sondas interceptan datos y los reenvían a los centros de monitoreo de PUMA. La Curacao obtuvo contratos posteriores de instalación y mantenimiento de hardware y software para PUMA de 2008 a 2013.[33] Los técnicos de La Curacao eran seleccionados por la DIPOL[34] y mantenían el centro de datos, los servidores y los sistemas de almacenamiento de datos de los centros de monitoreo. Incluso actualizaron las contraseñas de administrador en los servidores PUMA en 2011.[35]

En 2011, el coste mensual del mantenimiento de PUMA ascendía a 22 millones de pesos (alrededor de 12.500 dólares estadounidenses).[36] El sistema había crecido hasta tener 83 estaciones de trabajo en total, 58 de ellas en la sede de la DIJIN en Bogotá. En 2013, la Policía anunció un gran plan de ampliación de PUMA para convertirlo en el principal sistema de interceptación de Colombia.

31 "Resolución No. 0589 del 18 Jun. 2013", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 18 de junio de 2013.

32 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10124- 10", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 1 de septiembre de 2010, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-378033

33 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10124- 10", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 1 de septiembre de 2010, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-378033

"Contrato de Compraventa Celebrado entre la Dirección de Investigación Criminal y la Firma Compañía Comercial Curacao de Colombia S.A.", Dirección Administrativa y Financiera, Policía Nacional de Colombia, abril de 2008, https://www.contratos.gov.co/archivospuc1/C/116001000/07-2- 88996/C_PROCESO_07-2-88996_116001000_446982.pdf (archivado)

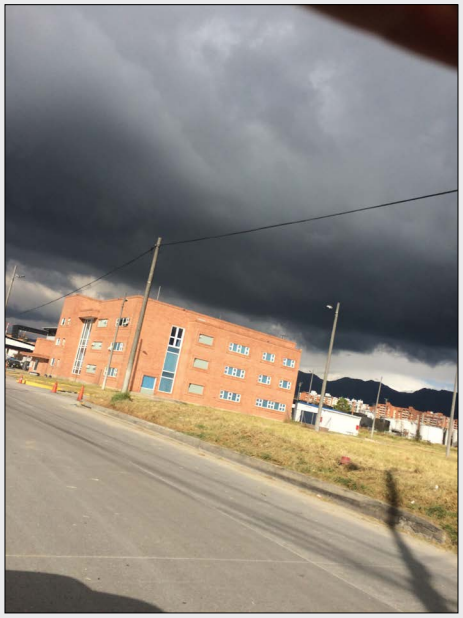
"Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 31 de agosto de 2010, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

34 "Contrato de Prestación de Servicios PN-DIRAF 06-7-10037- 13", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 23 de junio de 2013, https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=13-12-1778484

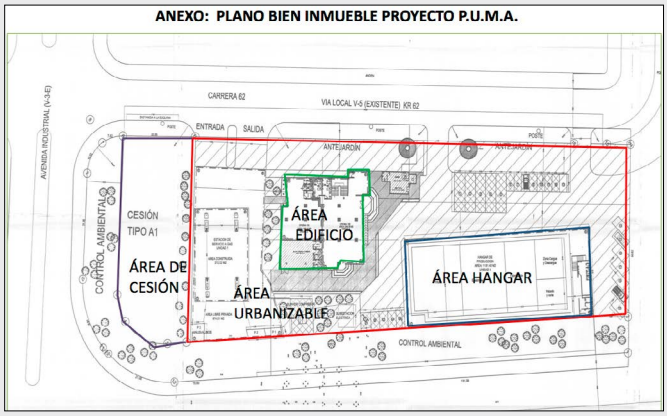
35 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Dirección Administrativa y Financiera, Policía Nacional de Colombia, miércoles, 31 de agosto de 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

36 "Contrato de Prestación de Servicios PN-DIRAF N°__06-7-10120- 11", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 31 de agosto de 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-598677

La Policía asignó la suma sin precedente de 50.000 millones de pesos (28 millones de dólares estadounidenses) al proyecto en enero de 2013.[37] Más de la mitad de esta cantidad se destinó a "fortalecimiento tecnológico", es decir, al software y hardware básicos necesarios para convertir PUMA en un sistema completo de interceptación legal, capaz de recopilar datos y contenido de llamadas de voz, VoIP, tráfico de Internet y redes sociales en 12 de los proveedores de servicios de telecomunicaciones de Colombia –cuatro redes de datos móviles y voz (Claro, Tigo, Avantel y Movistar) y ocho proveedores de servicios de Internet (Une, Telefónica, Emcali, Metrotel, ETB, Telebucaramanga, Telmex y EPM).



La sede de PUMA albergaba anteriormente una empresa de limpieza industrial. Izquierda: Un domingo de finales de septiembre de 2014, el hangar apareció abierto y sin apenas vigilancia. Créditos: Privacy International. Abajo: plano de la ampliación de PUMA



Sin embargo, en esta ocasión la Policía rompió con su proveedor habitual en materia de interceptación, Verint. Dio el contrato a otra empresa israelí, NICE Systems, en consorcio con la empresa colombiana Eagle Comercial SA.

Súper-PUMA, como se dio en llamar al sistema suministrado por NICE, iba a dar la Policía la capacidad de interceptar 20.000 "objetos", entre ellos líneas o dispositivos específicos, con la posibilidad expresa de llegar a los 100.000 objetos, aunque sin indicar claramente en qué plazo.

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

Súper-PUMA incluía también un módulo de monitoreo para tráfico de ISP y hasta 700 estaciones de trabajo por todo el país.[38] Los datos serían interceptados por medio de ocho sondas "NiceTrack IP", que filtran y extraen cantidades inmensas de datos enviados simultáneamente a través de sobrecargados enlaces IP. Por primera vez en la historia de los sistemas conocidos de interceptación de Colombia, el sistema sería capaz de interceptar datos 4G.

Se contrató también a NICE-Eagle para establecer un centro de datos móviles que "concentra toda la infraestructura tecnológica que soporta los procesos operativos y administrativos y se ha fijado como meta dar cobertura de comunicaciones de voz y datos." Durante esta fase, NICE-Eagle tenía que supervisar la migración de datos de Esperanza al nuevo sistema. Por último, la actualización de PUMA iba a incluir un sistema de administración de órdenes judiciales para datos móviles y voz con el que se pretendía reducir al mínimo el tiempo y la burocracia que mediaban desde la emisión de la orden hasta la recuperación de los datos.[39]

En 2014, durante la segunda fase de fortalecimiento de PUMA, NICE-Eagle tenía que centrarse en la instalación del sistema de interceptación para los ochos proveedores de servicios de Internet. El otro aspecto en que se centraría la segunda fase era el mantenimiento de los sistemas de interceptación de los cuatro proveedores de telecomunicación y del centro de datos.

Se suponía que, al final de 2014, PUMA habría reemplazado en gran medida al cada vez más desfasado sistema Esperanza. Sin embargo, su desarrollo se ha detenido por una falta de acuerdo entre la Fiscalía y la Policía, descrita en la conclusión del presente informe. PUMA está en condiciones de convertirse, no en el primero, pero sí en el más potente y avanzado sistema de monitoreo masivo de las comunicaciones de Colombia.

38 "Asunto: Respuesta proposición N.04 de 2013", Policía Nacional de Colombia, 12 de agosto de 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.

Más allá de la ley

El marco jurídico colombiano contiene varios mecanismos esenciales de protección del derecho a la privacidad, tanto en el texto de la Constitución de 1991 como en el bloque de constitucionalidad establecido de acuerdo con el artículo 93 de la Constitución. Este artículo incorpora a la legislación colombiana las obligaciones internacionales contraídas por Colombia en materia de derechos humanos y les otorga la condición de derecho constitucional por lo que tienen preferencia sobre las disposiciones legales.

Basándose en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), del que el Estado colombiano es signatario y que estipula que "[n]adie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación", el artículo 15 de la Constitución de 1991 dispone que toda persona tiene derecho al respeto de su intimidad personal y familiar. En concreto establece:

> "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."

La interceptación de las comunicaciones está regulada por la ley, a saber, por la Constitución y el Código de Procedimiento Penal. La Constitución faculta a la Fiscalía para "[a]delantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones" con control judicial (artículo 250). El Código de Procedimiento Penal lo establece de manera más específica. Comienza reiterando el derecho a la privacidad en su artículo 14, que dispone:

> "Toda persona tiene derecho al respeto de su intimidad. Nadie podrá ser molestado en su vida privada.
>
> No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este código. Se entienden excluidas las situaciones de flagrancia y demás contempladas por la ley.
>
> De la misma manera deberá procederse cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones.

> En estos casos, dentro de las treinta y seis (36) horas siguientes deberá adelantarse la respectiva audiencia ante el juez de control de garantías, con el fin de determinar la legalidad formal y material de la actuación."

El artículo 235 del Código estipula las condiciones en que la Fiscalía General de la Nación puede ordenar la interceptación de comunicaciones. Dispone:

> "El fiscal podrá ordenar, con el único objeto de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden.
>
> 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 tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron."

La disposición estipula que el fiscal sólo puede ordenar legalmente la interceptación de comunicaciones transmitidas por el espectro electromagnético (EMS)(teléfono, radio o cable de fibra óptica) y con el único fin de buscar elementos probatorios. La orden debe darse por escrito y tiene tres meses de vigencia.

En abril del 2013 se aprobó una nueva Ley de Inteligencia que estipulaba que las actividades de inteligencia y contrainteligencia" abarcan el "monitoreo del espectro electromagnético". El artículo 4 de la Ley dispone que sólo puede obtenerse información con fines legales, a saber: garantizar la seguridad nacional, la soberanía, la integridad territorial, la seguridad y la defensa de la nación, la protección de las instituciones democráticas y los derechos de las personas residentes en Colombia y de los ciudadanos colombianos y la protección de los recursos naturales y los intereses económicos de la nación. El artículo 17 de la Ley, relativo al "[m]onitoreo del espectro electromagnético e interceptaciones de comunicaciones privadas", dispone:

> "Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del monitoreo

> del espectro electromagnético en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones.
>
> La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales."

En segundo párrafo establece claramente que la interceptación de comunicaciones no está autorizada por la Ley de Inteligencia, sino que sólo debe realizarse en virtud de la autoridad legal del Código de Procedimiento Penal, de manera selectiva y de acuerdo con los procedimientos estipulados en el Código. No cabe afirmar, por tanto, que esta disposición autorice la interceptación de comunicaciones por los organismos de inteligencia o las autoridades policiales.[40]

La promulgación de la Ley recibió considerables críticas de la sociedad civil y de organismos públicos. Como la Ley de Inteligencia es una ley estatutaria –tipo especial de leyes superiores a las ordinarias y que deben ser aprobadas con un procedimiento especial y por mayoría absoluta en el Congreso– se sometió a la consideración de la Corte Constitucional para garantizar que cumplía el orden constitucional (incluidas las obligaciones internacionales contraídas por Colombia en materia de derechos humanos). La Ley de Inteligencia recibió la aprobación de la Corte Constitucional a principios de 2013.

En el curso de la revisión de la Corte Constitucional, la Ley de Inteligencia fue objeto de continuas críticas. La crítica de la Defensoría del Pueblo abordó el meollo de los problemas legales y técnicos de la disposición. En su exposición ante la Corte Constitucional, la Defensoría del Pueblo señaló:

> "la expresión 'El monitoreo no constituye interceptación de comunicaciones" [...] no se aviene a la Constitución, toda vez que entendido como 'vigilancia' o 'supervisión' del espectro, siempre recaerá sobre comunicaciones y, por ende, constituye una modalidad de intervención, interceptación o intromisión, que quedaría sustraída del control judicial (art. 15 superior)."[41]

40 Sin embargo, se ha sugerido que la Ley de Inteligencia podría de algún modo autorizar o abarcar los tipos de interceptación de comunicaciones que diversos sistemas con que cuentan los organismos colombianos –entre ellos PUMA y el SGID– pueden técnicamente efectuar.

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

La Defensoría del Pueblo sugirió que, para que la disposición fuera constitucional, habría que interpretar que tal monitoreo sólo "se realice sobre comunicaciones de personas indeterminadas, desde aparatos y números no especificados y por el tiempo razonable y estrictamente necesario para precisar los alcances de una investigación u operación en curso legalmente autorizada".

Los grupos de la sociedad civil Dejusticia y Fundación para la Libertad de Prensa fueron aún más allá en su crítica a la disposición. Sostuvieron que no había forma de limitar el "monitoreo" del espectro electromagnético como sugería la Defensoría del Pueblo. Explicaron que "el barrido al espectro electromagnético es una intervención directa sobre la intimidad de las personas. La falta de una orden judicial que ofrezca seguridad jurídica sobre estos hechos, deja al ciudadano particular en medio de una incertidumbre y completo desconocimiento sobre la posibilidad de estar siendo vigilado o de que sus asuntos personales están siendo escuchados por personas que él no autorizó para eso". Pidieron que la disposición se declarara inconstitucional.

El razonamiento por el que la Corte Constitucional determinó la constitucionalidad de la disposición es, en el mejor de los casos, un razonamiento viciado, y en el peor, objetiva y legalmente incorrecto.

La Corte comienza reiterando su anterior declaración de que el espectro electromagnético es "una franja de espacio alrededor de la tierra a través de la cual se desplazan las ondas radioeléctricas que portan diversos mensajes sonoros o visuales", explicación que contiene en sí misma datos inexactos (las imágenes no se desplazan por el espectro electromagnético). Determinó que el "monitoreo" del espectro electromagnético "consiste en llevar a cabo una labor de rastreo de forma aleatoria e indiscriminada". Explicó:

> "Ello implica la captación incidental de comunicaciones en las que se revelan circunstancias que permiten evitar atentados y controlar riesgos para la defensa y seguridad de la Nación. Técnicamente se estaría ante una especie de rastreo de sombras, imágenes y sonidos representados en frecuencias de radiación electromagnética y ondas radioeléctricas. La actividad de monitoreo del espectro electromagnético no podría involucrar un seguimiento individual. No envuelve un rastreo selectivo ni determinado sobre sujetos concretamente considerados. En esta medida, no puede confundirse el monitoreo del espectro electromagnético como actividad impersonal y abstracta con los actos propios de una investigación penal que es individual y concreta". [Énfasis añadido.]

La decisión de la Corte se basa en la idea de que hay una forma de "monitorear" el espectro electromagnético que no comporta interferencia en la privacidad de las comunicaciones. Es decir que los mensajes de correo electrónico y de texto y las llamadas de teléfono transmitidas por el espectro electromagnético pueden filtrarse, analizarse y monitorearse sin violar la integridad de la comunicación ni, por tanto, la privacidad de la persona que envía o recibe la comunicación.

Tal conclusión no es del todo incorrecta, pero se aplica a un conjunto sumamente limitado de actividades. Las únicas acciones en que posiblemente se podría "monitorear" el espectro electromagnético sin interferir de ningún modo en la privacidad de la comunicación serían las de los detectores térmicos y los instrumentos de orientación y antenas, por ejemplo. Todas las demás formas de "monitoreo" del espectro electromagnético hacen necesaria una interferencia (con una comunicación) de un tipo que sólo permite concluir que el monitoreo ha resultado en la intercepción de la comunicación.

El razonamiento de la Corte es, en última instancia, un razonamiento viciado. "[L]a actividad de monitoreo del espectro electromagnético –afirma–, no puede implicar interceptación o registro de las comunicaciones privadas, toda vez que para ello se requiere 'orden judicial, en los casos y con las formalidades que establezca la ley' [...] Por tanto, el monitoreo del espectro electromagnético es una actividad limitada por los derechos fundamentales y sujeta al sistema de control de poderes establecido en la Constitución (art. 113 superior), que no pueden ser vulnerados so pretexto del adelantamiento de tal actividad."

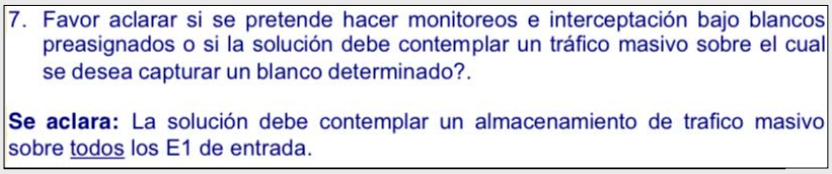
La función de la Corte consiste en evaluar la coherencia de las leyes con el orden constitucional de forma previa a su promulgación. Por tanto, decir que la actividad de monitoreo de los organismos de inteligencia no es interceptación porque estos organismos no están autorizados es una tautología. Sencillamente, cabe la posibilidad de que los legisladores elaboren leyes inconstitucionales.

En todo caso, incluso aceptando la validez constitucional de la disposición sobre el espectro electromagnético, es evidente que la Ley sólo autoriza un limitado conjunto de actividades de vigilancia que no constituyen interceptación de comunicaciones. Ese conjunto de actividades no incluyen el monitoreo masivo y pasivo del tipo que las tecnologías adquiridas por la DIPOL, el DAS y otros organismos posibilitan. Los contratos y otros documentos confidenciales que Privacy International ha conseguido muestran que las herramientas de vigilancia adquiridas por estos organismos dan acceso esencialmente a los mismos datos sobre las personas que otras plataformas de interceptación como Esperanza, si no a más.

Sistema en la sombra: la DIPOL y el Sistema Integral de Grabación Digital (SIGD)

Antes de PUMA, en 2005, la DIPOL estableció un sistema de interceptación masiva, el primero de Colombia. En febrero de ese año, la Policía convocó un concurso para el suministro del equipo necesario para monitorear la recién desarrollada tecnología de telefonía móvil de tercera generación (3G) en el marco de la "adquisición construcción y desarrollo tecnológico" de un Sistema Integral de Grabación Digital (SIGD).[42]

El SIGD se concibió para ir más allá de la interceptación de "blancos preasignados" y recopilar tráfico "masivo" de comunicaciones en 16 líneas troncales y generar nuevos blancos. Como explicó la DIPOL a las empresas que concursaron para suministrarla, la "solución debe contemplar un almacenamiento de tráfico masivo sobre todos los E1 de entrada". [Énfasis en el 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."

UN SISTEMA MASIVO

La DIPOL pretendía reunir información sobre las comunicaciones sin limitarse a objetivos conocidos.]

La DIPOL necesitaba que su Sistema Integral fuera completamente pasivo.[43] De este modo, tras la instalación inicial en la arquitectura de los proveedores de servicios, la DIPOL podía monitorear los flujos de información sin más asistencia técnica de los operadores.

DIPOL recurrió a Verint y a La Curacao para crear su sistema de interceptación. El primer componente, VANTAGE (adquirido en junio de 2005), lo comercializaba

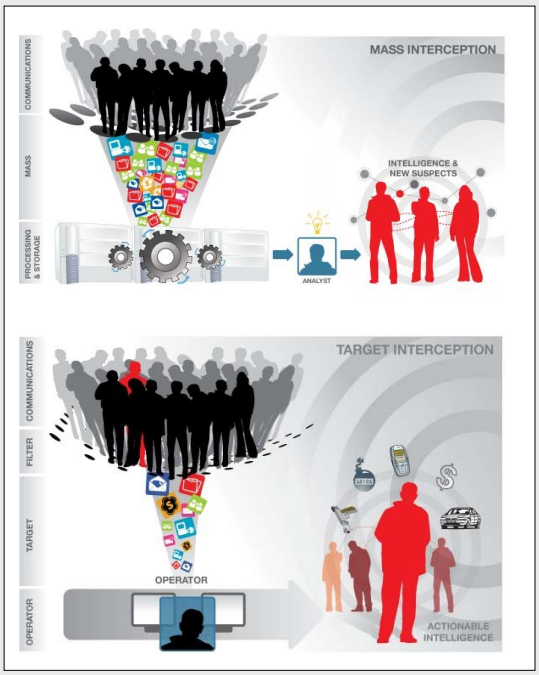
42 "Adquisición construcción y desarrollo tecnológico – Equipo de Monitoreo de Telefonía Móvil Celular Nueva Tecnología – Sistema Integral de Grabación Digital – con Destino a la Policía Nacional". En 2007, la Resolución 02049 había consolidado la autoridad de la DIPOL para realizar y coordinar actividades de recopilación de información monitoreando el espectro electromagnético por medio de su Grupo Producción de Inteligencia.

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", Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 25 de febrero de 2005.

Verint como herramienta que "ayuda a descubrir amenazas desconocidas, con independencia de cómo se comuniquen los responsables"[44] interceptando, filtrando y categorizando información de manera que un analista pueda registrarla en busca de patrones, así como de personas, números, servidores y otros datos de interés específicos. En Europa del Este se dio el caso de un organismo de inteligencia que utilizó VANTAGE para captar 3 millones de mensajes de correo electrónico y 12 millones de mensajes de correo web al día, almacenando las interceptaciones durante 90 días. El número de sondas utilizadas en este caso era el mismo que el adquirido por la Policía de Colombia (16 sondas),[45] si bien VANTAGE puede aumentarse o reducirse según los deseos y el presupuesto del gobierno comprador.

En septiembre de 2005, la DIPOL decidió adquirir un "módulo para monitoreo activo de Internet para ISP [proveedores de servicios de Internet". Optó por la solución RELIANT, de Verint, elegida posteriormente por la DIJIN en su sistema PUMA. Al igual que VANTAGE, viene con función de centro de monitoreo.

Los técnicos de Verint instalaron el equipo pertinente, con las sondas y todo, que la Policía importó directamente de Israel con exención de derechos de importación,[46] en



NUEVAS HERRAMIENTAS

La DIPOL compró VANTAGE por 575.000 dólares estadounidenses (alrededor de 1.600 millones de pesos), y RELIANT, por unos 160.400 dólares (372,5 millones de pesos). Ambas herramientas forman conjuntamente el núcleo de un sistema de monitoreo masivo que interceptaría y almacenaría sin orden judicial cantidades enormes de tráfico de comunicaciones en Colombia.

44 "Vantage", Verint, 2014, 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, noviembre de 2010, http://s3.documentcloud.org/documents/810401/1260-verint-product-description-security-and.pdf

46 "Ley 80 de 1993", Congreso de la República de Colombia, 28 de octubre de 1993, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=304

Sistema en la sombra: la DIPOL y el Sistema Integral de Grabación Digital (SIGD)

los centros de conmutación de los proveedores de servicios y lo conectaron a la sala de monitoreo de la DIPOL de su sede de la avenida Boyacá de Bogotá, dejando a cargo de La Curacao el mantenimiento y la solución de problemas del producto. Los analistas de sus 20 estaciones de trabajo eran capaces, al menos en teoría, de grabar conversaciones de un objetivo seleccionado,[47] captar 100 millones de registros de datos de llamadas al día e interceptar 20 millones de SMS diarios.[48] Además, una función de reconocimiento de voz generaría automáticamente datos de llamadas en formularios para procesador de texto, a los que los analistas podían añadir manualmente notas y transcripciones o resúmenes de las llamadas. Estas funciones masivas podían ampliarse o reducirse si era necesario, al precio correspondiente.

¿Pero funcionaba como se esperaba? La Policía niega públicamente tener en la actualidad[49] la capacidad de intervenir el tráfico de Internet. Personas con experiencia directa en contrataciones de defensa confirman que la presión para producir resultados –así como la promesa de que una "mejor" tecnología garantizará mejores resultados– llevó a la Policía a adquirir equipo cuyo funcionamiento no entendía. Varias personas describieron el sistema de Verint como una especie de trasto inútil. "En realidad no sabe lo que está comprando", recordó un ingeniero tras reunirse con el general Jairo Gordillo Rojas,[50] jefe de la oficina de telemática de la Policía, y con su equipo. "No sé [por qué lo compraron], pero desde luego fue una oportunidad que La Curacao aprovechó. Pero sé que no funciona tan bien como esperaban".

"Cada organismo creaba su propio sistema de inteligencia", afirma un experto en telemática de la Policía. "Los sistemas de inteligencia se investigan a sí mismos también y tienen mucha presión para producir resultados positivos. Naturalmente, hay competencia". Cada organismo tiene un presupuesto, y no hay integración de los presupuestos, explicó. Así que, ante esta situación, sumada a la presión para producir información de inteligencia, los organismos compran equipos que se les proponen sin apenas examinar lo que están comprando.

El sistema de la DIPOL estaba separado de Esperanza. En 2005, en el momento del desarrollo del sistema, las empresas interesadas en licitar para el contrato formularon preguntas a la autoridad contratante. "¿El sistema se va a conectar al switch Esperanza? Si es así ¿ya han hecho las gestiones de alto nivel para hacer la conexión a la Fiscalía?" La DIPOL respondió con claridad: "En ninguna parte se habla de la aplicación de esta herramienta al sistema Esperanza. Los oferentes se deben limitar a las especificaciones exigidas". Preguntaron de nuevo: "En los 16 E1 solicitados, ¿cuántos son para telefonía fija y cuantos para telefonía móvil celular? ¿Estos últimos provienen de switch Esperanza?". Una vez más, la DIPOL explicó claramente que el sistema sería independiente: "No, no

47 "Respuesta observaciones: Contratación Directa No. 006 de 2005", Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 25 de febrero de 2005.

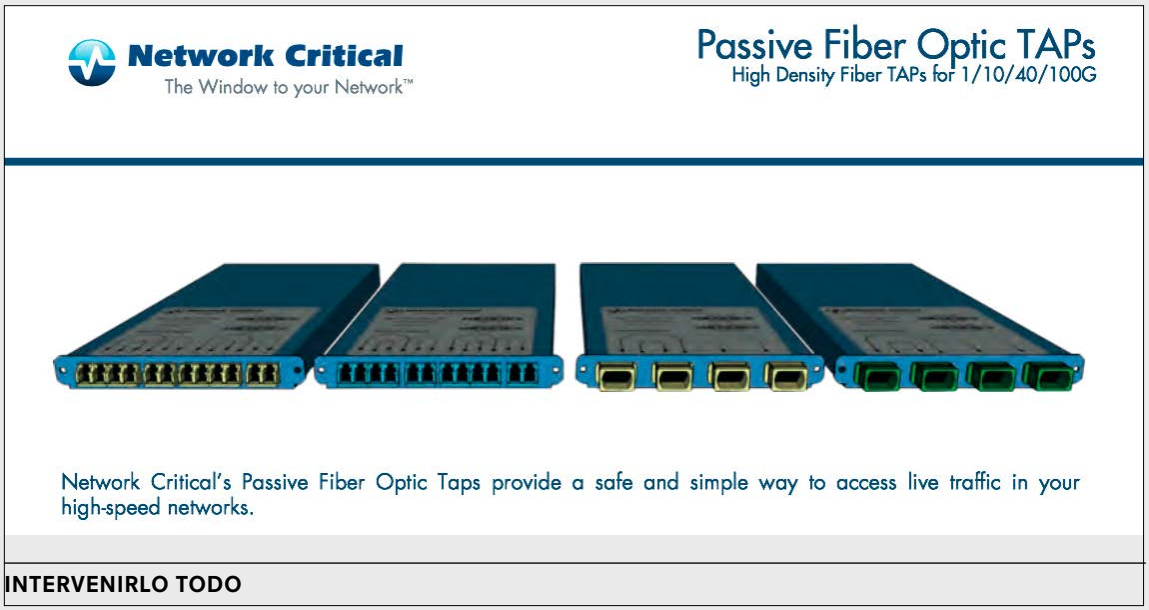
48 "Contrato de Compraventa No. 034 de 2005, celebrado entre el Fondo Rotatorio de la Policia y la Firma Compañía Comercial Curacao de Colombia", Police Revolving Fund, Ministry of Defence, 17 June 2005.

49 A fecha de septiembre de 2014.

50 El general Gordillo fue citado en mayo de 2014 para interrogarlo acerca de presuntas escuchas y vigilancia de dos periodistas. "Fiscalía realiza interrogatorios por supuestas 'chuzadas'", Noticias RCN, 9 de mayo de 2014, http://www.noticiasrcn.com/nacional-pais/fiscalia-realiza-interrogatorios-supuestas-chuzadas

provienen del switch Esperanza".[51]

La relación entre la DIPOL y la Fiscalía en este sistema no está clara. Las especificaciones técnicas para el Sistema Integral de Grabación Digital (SIGD) establecen que no recibiría información de Esperanza, y el sistema parece recibir pasivamente todos los datos que pasan por los respectivos E1. Sin embargo en 2006, el entonces director del sistema Esperanza, Vladimir Flórez Beltrán, autenticó los "certificados de conectividad" a Esperanza".[52] En ese momento, la Policía estaba ampliando las funciones del sistema, utilizando una vez más tecnología de Verint suministrada por su representante colombiano, La Curacao.



INTERVENIRLO TODO

La DIPOL también compró interceptores para cables de fibra óptica en 2009. El cable de fibra óptica es un manojo de hebras que puede transmitir señales moduladas en ondas de luz, a diferencia del cable de cobre tradicional, en el que la señal se transmite por voltaje eléctrico. Mientras que Esperanza necesitaba la conformidad del operador de telecomunicaciones para manipular su centro de conmutación móvil cada vez que se solicitaba un registro o una llamada de teléfono (garantizando así, al menos en teoría, que se presentara una solicitud formal y una justificación), el sistema de vigilancia la DIPOL está configurado para conectarse al centro de monitoreo de la DIPOL y transmitirle cantidades masivas de tráfico. Puede encontrarse mayor información en el informe de Privacy International "Oferta y demanda: al descrubeirto la industria de la vigilancia en Colombia".

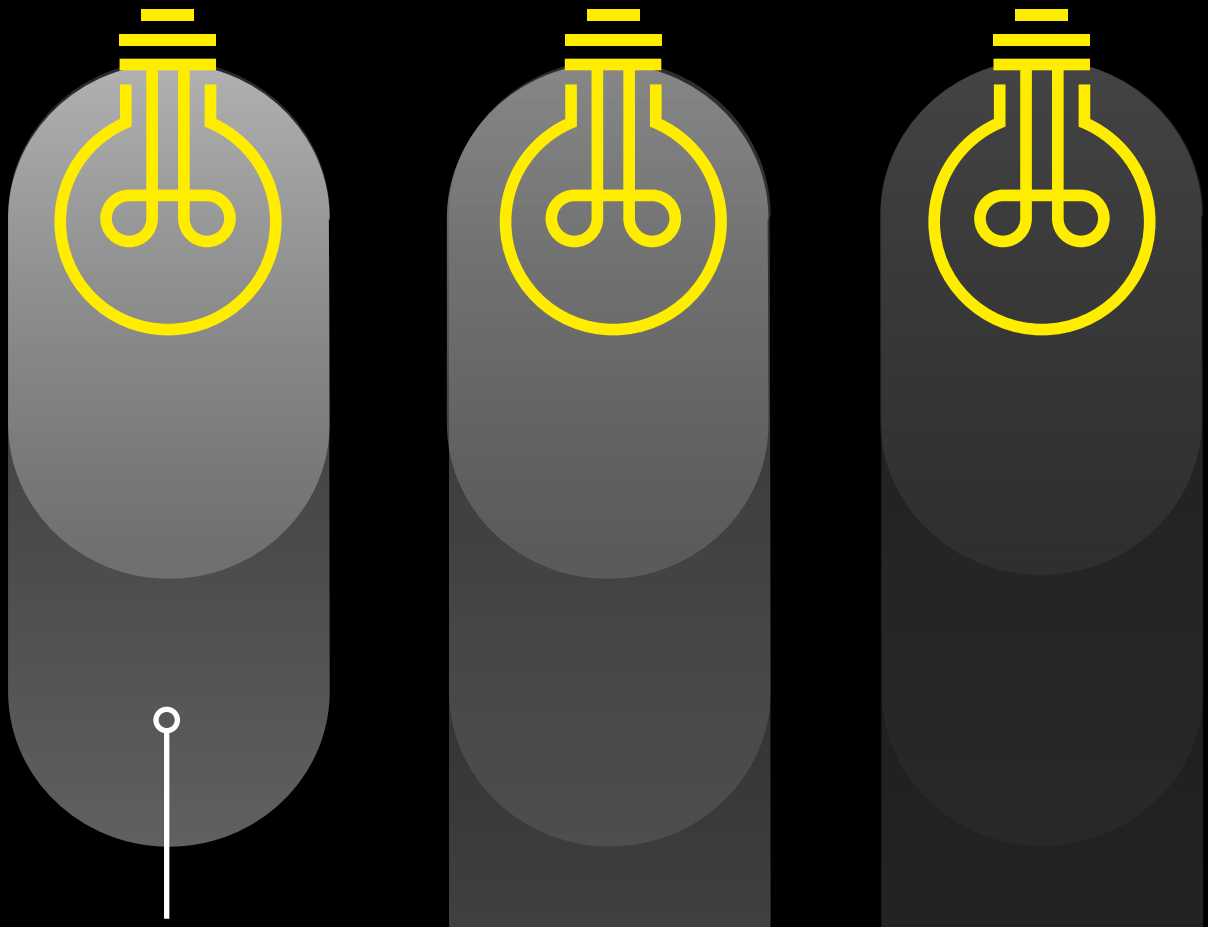
La DIPOL obtuvo tres dispositivos "Slimline Fiber Optic Passive TAP" de varias dimensiones. Slimline es una marca registrada de NetworkCritical, empresa radicada en Reino Unido que suministra tecnología de monitoreo de red.[54]

51 "Adenda 02: Adquisición Sistema Integral de Grabación Digital", Dirección Administrativa y Financiera, Policía Nacional de Colombia, 2007.

52 "Adjudicación de la Contratación Directa No. 055 de 2006", Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 29 de noviembre de 2006, https://www.contratos.gov.co/archivospuc1/ADA/115001003/06-2-16355/ADA_PROCESO_06-2-16355_115001003_31717.pdf (archivado)

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

Sistemas de vigilancia de las comunicaciones



Sistema Esperanza

Datos interceptados en líneas específicas previa solicitud a la Fiscalía y con la colaboración activa del TSP. Accesible para la DIJIN (cumplimiento de la ley) y, anteriormente, el DAS con orden judicial.

PUMA

Datos Interceptados en masa en la troncal de telecomunicaciones sin la colaboración de los TSP, aparte de la instalación. Tecnología gestionada por la DIJIN (cumplimiento de la ley) con supervisión administrativa de la Fiscalía.

SIGD

Datos interceptados en masa de la troncal de telecomunicaciones sin colaboración de los proveedores de servicios, aparte de la instalación. Gestionado técnicamente por la DIPOL (inteligencia). Sin supervisión clara.

Herramientas tácticas

Las tecnologías tácticas[54] de interceptación están presentes en los arsenales de vigilancia de varios organismos colombianos distintos.

Al crear su sistema de interceptación, la DIPOL adquirió equipo de monitoreo móvil para la identificación o interceptación de objetivos en ubicaciones conocidas. Esta tecnología se conoce coloquialmente como IMSI catcher o stingray.

El IMSI catcher transmite una intensa señal inalámbrica que hace que los teléfonos de los alrededores se conecten a él, y puede actualizarse con tecnologías de monitoreo de ubicación que determinan la ubicación de un objetivo con una precisión de un metro. Estos dispositivos pueden orientarse selectivamente al dispositivo de una persona en particular, dirigiéndolos, por ejemplo, a su lugar de trabajo. Pueden utilizarse también para identificar a personas desconocidas que asistan a manifestaciones y otras reuniones, porque muchos teléfonos móviles se conectaran a IMSI catcher y transmitirán información de identificación.

La DIPOL compró un IMSI catcher "Laguna", fabricado por la empresa neozelandesa de tecnología Spectra Group. En septiembre de 2005 pagó 474.000 dólares estadounidenses (970,8 millones de pesos) a la empresa colombiana Maicrotel Ltd.

El interceptor Laguna puede dirigirse a una cantidad relativamente pequeña de tráfico a una distancia fija de hasta 500 metros. Entre los datos que el equipo de Spectra puede grabar figuran los registros de identificación exclusivos de un teléfono. Para ello no es necesario que un analista elija activamente qué números captar: "La identificación de la presencia del Objetivo en una zona bajo control y la revelación de sus identificadores desconocidos es hecha de un modo automático con la ayuda de los teléfonos móviles especiales, incluidos en el Sistema".[55] El equipo almacena la información interceptada en formato digital en discos duros que pueden luego llevarse al centro de monitoreo de la DIPOL para conectarlos a los ordenadores y analizarlos. Por consiguiente, al activar un

54 Empleamos el término "tácticas" para denotar las tecnologías de interceptación en que los datos y el contenido de las comunicaciones se toman directamente del dispositivo o por señales emitidas por éste, no de la arquitectura de red del proveedor de servicios.

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", Fondo Rotatorio de la Policía, Ministerio de Defensa Nacional, 30 de septiembre de 2005.

IMSI catcher pueden ser potencialmente interceptados todos los datos de los números de teléfono de una determinada zona, aun cuando la DIPOL no pretenda centrarse más que en una determinada persona o edificio.[56]

Además, la policía colombiana adquirió tecnología de la empresa italiana Hacking Team. La suite Remote Control System (RCS) de la empresa permite interceptar ordenadores y dispositivos móviles sin que los usuarios lo detecten. Infectando el dispositivo del objetivo, a menudo utilizando "vulnerabilidades", la suite RCS puede recopilar sus datos, activar y desactivar a distancia la webcam y el micrófono y copiar archivos y contraseñas tecleadas. En 2014, Hacking Team tenía un técnico externo en Colombia y un contrato activo con la policía colombiana. Se sospecha del uso por parte el gobierno colombiano de productos de malware ofensivo de Hacking Team desde que los investigadores de The Citizen Lab identificaron un servidor de comando y control para la suite RCS en el país.[57]

56 Maicrotel y Star ganaron en noviembre de 2006 un contrato, de 466.666 dólares estadounidenses (1.196 millones de pesos), para equipo de monitoreo de telefonía móvil, y tuvieron el mantenimiento de este equipo a lo largo de 2009. En principio consiguió el contrato Maicrotel Ltda en asociación temporal con Star Colombia. Tras una revisión del comité de licitaciones, la parte del proyecto relativa al Equipo de Monitoreo de Telefonía Celular para Protocolo GSM se declaró nula. Eagle ganó el contrato en apelación, al retirar algunos de sus competidores sus ofertas y no aparecer ninguno en la audiencia. Su rival Eagle ganó también un contrato de 1.228 millones de pesos, alrededor de 610.700 dólares estadounidenses, en diciembre de 2006 y 329 millones de pesos en diciembre 2007. Técnicamente, este contrato se ganó en otro proceso de licitación, pero básicamente para el mismo tipo de producto, equipo de monitoreo GSM. Eagle ganaría más tarde un importante contrato para la renovación de la plataforma PUMA de la DIJIN.

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

La DIPOL y la empresa de vigilancia de Silicon Valley

Palantir

Pilot Proposal to DIPOL

THE PALANTIR PLATFORM

Prepared for:

[redacted]

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

Prepared by:

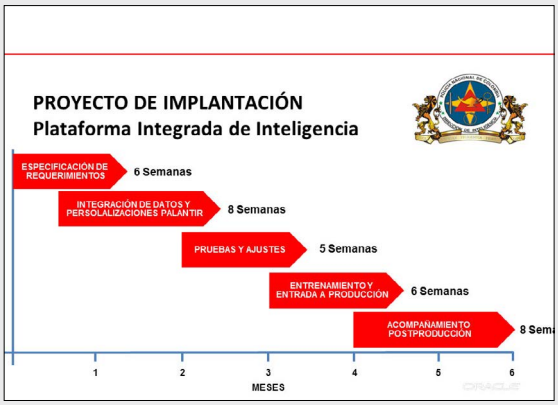
Palantir Technologies Inc.
http://www.palantir.com
+1 650-815-0200

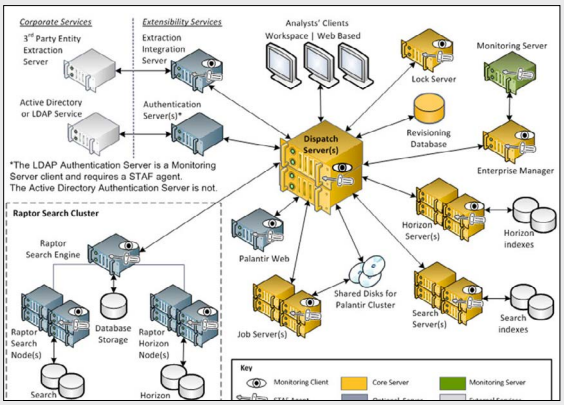
PALANTIR POC: [redacted] Tel. +1 571 419 4226

100 Hamilton Ave.
Suite 300
Palo Alto, CA 94301

1660 International Dr.
Suite 800
McLean, VA 21022

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 propuso instalar una plataforma de inteligencia integrada para la DIPOL durante seis meses en 2012. El nuevo sistema ampliaría la plataforma de inteligencia basada en Oracle ya existente e integraría 10 bases de datos policiales. Palantir está concebido para el análisis de información de código abierto que puede sacarse de Internet, así como de datos recibidos de servidores de centros de monitoreo.

En 2012, la DIPOL reconoció que necesitaba una plataforma o sistema con que procesar de manera más eficaz las enormes cantidades de información que estaba recibiendo. Ese año, la Policía sacó a concurso un contrato para suministrar tal plataforma. Una de las empresas que se presentaron fue el gigante estadounidense de la visualización y el análisis de datos Palantir. Palantir propuso a la DIPOL una Plataforma de Inteligencia Integrada "SI3". Oracle había intentado lanzar por su cuenta su propia solución de análisis en noviembre de 2011, antes de unirse a Palantir y STAR para proponer una solución que utilizaba tecnología tanto de Palantir como de Oracle, según una presentación en PowerPoint incluida en los anexos.

Palantir se introdujo en el mercado de la visualización y el análisis datos con una inversión de In-Q-Tel, empresa de capital de riesgo sin ánimo de lucro, establecida por el Organismo Central de Información (CIA) de Estados Unidos.[58] El ejército estadounidense utiliza una versión del software de Palantir que combina imágenes de dron con sensores terrestres y escáneres biométricos en operaciones militares.[59]

A un costo 1,5 millones de dólares, Palantir propuso un sistema que permitiría a la DIPOL incorporar, categorizar, etiquetar, filtrar y dar coherencia a los datos, en su mayoría de fuentes internas, con la posibilidad de incluir datos de determinado número de fuentes externas –por ejemplo, de fuentes de inteligencia de código abierto como Facebook y Twitter–. Entre las fuentes internas que Palantir propuso integrar con los datos obtenidos de fuentes de información de inteligencia de código abierto figuraban 10 bases de datos de la Policía.

En su oferta, Palantir propuso entrenar 30 analistas e integrar las diversas bases de datos policiales de Colombia, incluida la "S12" basada en Oracle, que alberga gran parte de la información que la DIPOL recibe. Según la oferta, también se añadirían a todo archivo imágenes, vídeo y datos biométricos obtenidos, por ejemplo, mediante vigilancia física u otros medios más habituales. Palantir explicó claramente que con su plataforma se podían determinar las conexiones entre los conjuntos de datos y las personas, con la posibilidad de categorizar y analizar tanto la información como a las personas.

"Palantir es una suite completa de productos, concebida para aprovechar los repositorios de información existentes de la DIPOL y analizar los datos a nivel estratégico, operativo y táctico".

Aunque los productos del estilo de los de Palantir son potentes herramientas para combatir la delincuencia y el terrorismo, su uso puede poner en peligro el derecho a la privacidad garantizado constitucionalmente a la ciudadanía colombiana. El motor de búsqueda algorítmico de Palantir está concebido para funcionar con una "escala de datos enorme", lo que supone que puede buscar en los datos de millones de colombianos y colombianas,

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 de julio de 2013, http://defensetech.org/2013/07/01/special-forces-marines-embrace-palantir-software/

incluidos los datos de las comunicaciones, para aislar a personas de interés basándose en términos de búsqueda determinados por las autoridades. El sistema de Palantir no tiene función de auditoría interna, por lo que pueden concederse a los analistas privilegios de acceso distintos. Esta función de auditoría depende, en cambio, del empeño de las mismas autoridades que solicitan la información (en este caso, la DIPOL) en administrar bien la plataforma y, cuando proceda, en controlarla y en controlar sus propios poderes.

Palantir dijo, en respuesta a Privacy International, que aunque la empresa fue parte de una propuesta en el año 2012, no avanzó más allá de dicha fase.

El DAS: sondas de red e interceptación táctica

A la vez que la DIPOL desarrollaba sistemas de "monitoreo" que interceptaban enormes cantidades de datos aparentemente sin orden judicial, el DAS mantenía también, calladamente, su propio sistema de escuchas en la infraestructura de las telecomunicaciones. Se plantea por ello la cuestión de si las interceptaciones que reveló Semana a principios de 2009 suponían en realidad uso indebido de Esperanza, como se denunciaba, o si el DAS estaba llevando a cabo sus interceptaciones por separado, sirviéndose de tecnología de interceptación masiva y automatizada.

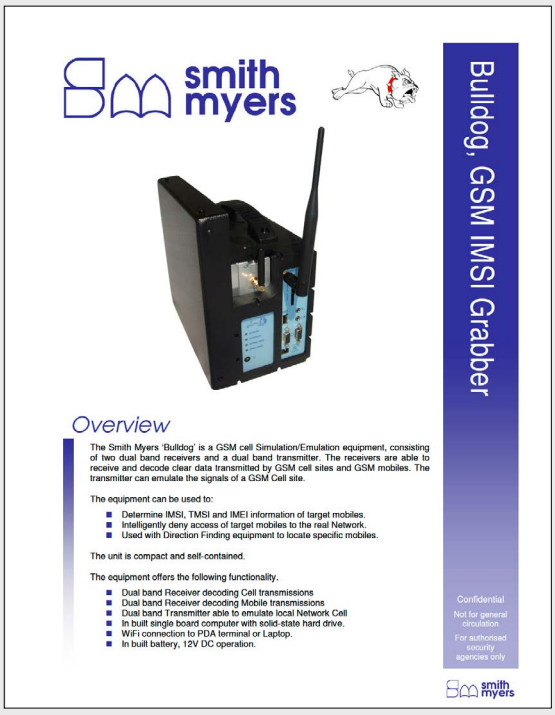
El DAS tenía el menos un centro de monitoreo y una sonda de Internet. Incluso en agosto de 2011, cuando estaba siendo ya investigado por interceptaciones ilegales y faltaban dos meses para que fuera disuelto oficialmente, el DAS pagó para que La Curacao garantizara "el pleno funcionamiento e integridad de la solución sistema de la sala de análisis de información registrada al navegar por Internet RELIANT de Verint System".[60] Este servicio incluía mantener la "sonda táctica en cualquier lugar del país donde se encuentre operando", lo que indica que era una sonda que podía quitarse y volverse a insertar para intervenir cables cuando fuera necesario.

¿Estaban esta sonda y este centro de monitoreo separados de Esperanza? El DAS tenía una sala de monitoreo enlazada a Esperanza, la famosa Sala Vino, donde los analistas recibían llamadas interceptadas. Pero en ninguna parte del anexo técnico del contrato de mantenimiento entre el DAS y STAR para la Sala Vino, reproducido aqui, se hace mención alguna de la sonda de Verint. Tampoco se menciona a Verint ni su tecnología en las decenas de documentos relativos a Esperanza que Privacy International ha recopilado. Mientras STAR era responsable del mantenimiento y la solución de diversos problemas técnicos de las plataformas del sistema Esperanza gestionado por la Fiscalía, La Curacao mantenía las sondas y las salas de monitoreo de la DIPOL y el DAS que utilizaban tecnología de Verint.

STAR y La Curacao forman parte de un saturado mercado de tecnología de vigilancia y tienen que competir a menudo entre sí por los contratos. Las tecnologías de estos proveedores habrían sido en general incompatibles o, en el mejor de los casos, compatibles en grado mínimo, a fin de que sus clientes tuvieran menos motivos para recurrir a otros proveedores. La incompatibilidad de la solución de Verint con la suministrada por Esperanza se presentaría posteriormente, en 2014, como una de las principales razones para detener la implementación del sistema PUMA.

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.", Fondo Rotario del Departamento Administrativo de Seguridad, 22 de agosto de 2011, http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=11-12-620217

El DAS acudió también al mercado de herramientas de intervención selectiva y análisis forense. Entre ellas figura el monitoreo de llamadas basado en la ubicación, los IMSI catchers anteriormente descritos. En mayo de 2010, el DAS examinó presupuestos para los productos Nesie y Bulldog de la empresa británica Smith Meyers. Nesie es un IMSI catcher , similar al producto "Laguna" de Spectra vendido a la DIPOL. Un analista podía también operar a distancia el dispositivo Nesie a través de un enlace IP.



NESIE Y BULLDOG

Estos dispositivos móviles de vigilancia pueden localizar y captar tráfico telefónico activo a una distancia fija; el DAS quiso comprar estos productos en 2010.

El DAS adquirió también "unidades móviles forenses" en algún momento antes de 2010. Eran estaciones de trabajo que podían utilizarse para copiar ordenadores, teléfonos y otros dispositivos de los objetivos en busca de material sospechoso para hacerle copias con calidad probatoria. Los agentes del DAS habrían conseguido estos dispositivos, que introducían en los ordenadores para hacer una copia y llevarla a una estación fija,[61] posiblemente incluso a su propio centro de monitoreo.

61 El DAS estuvo al principio dispuesto a pagar más de 641 millones de pesos por esto. En diciembre de 2007, el DAS celebró una audiencia sobre la oferta, que finalmente se anuló en diciembre 2006 al no poder suministrar ningún postor todos los componentes necesarios para el sistema.

Un contrato de mantenimiento de este equipo de diciembre 2010[62] muestra que el DAS se lo compró a La Curacao. El sistema utilizaba Forensic Toolkit (FTK), software informático forense de AccessData, empresa radicada en Estados Unidos. Ese software permite a un analista "prever la máquina de un objetivo desde el otro lado de la red para determinar la pertinencia antes de la adquisición, pero [...] también adquirir y analizar completamente los datos contenidos en el sistema, incluida la RAM".[63] Los analistas podían analizar con fines forenses los datos activos (memoria del sistema, volúmenes lógicos, dispositivos físicos) en un dispositivo remoto desde su propio sistema. Utilizando este equipo, un mínimo de 15 agentes, radicados principalmente en Bogotá, podían conseguir las contraseñas de los dispositivos y analizar todos los mensajes de correo electrónico y las comunicaciones contenidas en el dispositivo secuestrado.[64]

En septiembre de 2009, el DAS manifestó que las interceptaciones que había publicado Semana "no se hicieron desde ningún equipo móvil de monitoreo del Departamento Administrativo de Seguridad [...] Además, estos equipos están controlados desde el pasado 22 de febrero como usna medida preventiva".[65] El Congreso de Estados Unidos también prohibió que el DAS recibiera fondos de diversos programas del Departamento de Estado en 2010.[66] Los técnicos de STAR mantuvieron los equipos técnicos de la Sala Vino y otras salas de monitoreo enlazadas con Esperanza a lo largo de 2010, y el DAS estuvo haciendo contratos de compra de más unidades móviles de vigilancia. Incluso si los dispositivos concretos a que se refirió el director del DAS, Felipe Muñoz Gómez, estaban "bajo control", es evidente que las interceptaciones del DAS no cesaron, a pesar de las investigaciones y los escándalos.[67]

62 Una interesante indicación de cooperación en toda la Policía y el DAS es que el supervisor del proyecto sería el coordinador del grupo de controles técnicos de la DIJIN.

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

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

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

66 "Consolidated Appropriations Act, 2010", Congreso de Estados Unidos, 30 de septiembre de 2010, http://www.gpo.gov/fdsys/pkg/BILLS-111hr3288enr/pdf/BILLS-111hr3288enr.pdf

67 Desde su disolución se ha creado un nuevo organismo de inteligencia, la DNI, del se sabe muy poco públicamente. "Consulta de archivos de inteligencia del DAS, bajo control de la DNI", El Tiempo, 16 de julio de 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.

LA SALA VINO.

Los técnicos de STAR mantuvieron los equipos técnicos de la famosa sala de interceptación del DAS durante todo el escándalo de las interceptaciones y hasta la disolución del organismo.

Controles legales y técnicos

La reciente preocupación por la ampliación de PUMA no es más que uno de los capítulos de una larga historia de vigilancia ilegal llevada a cabo en Colombia. Diversos organismos del Estado que compiten por tener facultades de interceptación independientes han desarrollado potentes programas de vigilancia masiva solapados entre sí, sin salvaguardias legales suficientes.

La rivalidad institucional es culpable en parte de la falta de articulación entre los sistemas, pero las razones que se ofrecen para explicar esta rivalidad difieren. Un ex investigador de la DIJIN informó a Privacy International de que los investigadores de la Fiscalía tienen prioridad para aprovechar los cupos de interceptación de cada proveedor de servicios conectado al sistema Esperanza, por lo que los investigadores del DAS y de la DIJIN sólo pueden solicitar un número limitado de intervenciones.

Sin embargo, cada organismo está sometido a la misma presión para que consiga cada vez más información a fin de producir resultados en la investigación. Al preguntarle si, a pesar del marco legal, era posible técnicamente que la Policía llevara a cabo sus propias investigaciones, el investigador dijo: "Todas las interceptaciones de la DIJIN pasan por Esperanza; si no, sería ilegal".

"PUMA es un sistema que se adapta a estaciones remotas interconectadas con el sistema Esperanza", explicó un funcionario de la DIJIN al preguntarle Privacy International. Añadió: "Esperanza está detrás. Tenemos que actualizarnos, pero la Fiscalía no tiene la información bien ni la tecnología correcta. No podemos [la DIJIN] actualizarnos porque la comunicación [entre la Fiscalía y la Policía] se ha roto". Lo frustrante es, dijo el policía, que aunque que la Policía controla los cables y las escuchas, la Fiscalía tiene que programarlas. "Estamos supeditados al control administrativo de la Fiscalía [...] PUMA está supeditado y controlado por Esperanza. No se activa nada si no está autorizado técnicamente por Esperanza".

Los datos expuestos en este informe muestran que todavía pueden efectuarse intervenciones fuera del sistema Esperanza. Aunque la DIJIN debe aún presentar solicitudes de intervención para que la Fiscalía las autorice a fin de que sus actuaciones sean legales,[68] el control de la Fiscalía es fundamentalmente de naturaleza administrativa y jurídica. La DIJIN tiene todavía autonomía técnica para

68 "Asunto: Respuesta proposición N.04 de 2013", Policía Nacional de Colombia, 12 de agosto de 2013

recibir y almacenar datos de comunicaciones interceptadas de la redes de los proveedores de servicios, pues las tecnologías de Verint y, ahora, NICE están concebidas para ello.

En respuesta a las preguntas de un comité parlamentario sobre la futura relación entre PUMA y el sistema Esperanza, el director general de la Policía, José Roberto León Riaño, manifestó 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" [Énfasis añadido].[69]

Con tan potente sistema de vigilancia pasiva, el riesgo de que vuelvan a producirse interceptaciones ilegales es grande mientras no se establezcan fuertes salvaguardias técnicas y legales. En 2010, la Fiscalía comunicó que se interceptaban las comunicaciones telefónicas de sus propios investigadores, debido a falsos informes presentados por dos agentes de la Policía Nacional y por otros del Cuerpo Técnico de Investigación de la Fiscalía (CTI).[70] En 2013, el ex investigador del CTI y varios agentes de policía fueron declarados culpables de interceptar ilegalmente las comunicaciones del ex magistrado de la Corte Suprema Iván Velásquez. Y este año han desaparecido de los servidores del Archivo General de la Nación archivos clave relacionados con las interceptaciones del DAS.[71]

Es dudoso que pueda regularse de manera efectiva la vigilancia de las comunicaciones en el marco actual. Privacy International contactó con algunas de las empresas que venden la tecnología de vigilancia mencionada en este informe para informarse sobre su función en estos sistemas.[72]

69 "Asunto: Respuesta proposición N.04 de 2013", Policía Nacional de Colombia, 12 de agosto de 2013

70 Micrófonos ocultos, seguimientos e interceptaciones ilegales", Huellas, Fiscalía General de la Nación, agosto de 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 de julio de 2014, http://colombiareports.co/evidence-colombias-intelligence-agency-wiretapping-scandal-disappeared/

72 El representante legal de la asociación NICE-Eagle negó saber algo en concreto sobre el contrato de ampliación de PUMA al preguntarle por él incluso después de que se hiciera público en 2013. Preguntado específicamente por las escuchas telefónicas en 2011, el director de Eagle, Archimedes Bonilla Vega, manifestó: "Suministro equipo, pero no tengo obligación ni competencia para determinar si lo utilizan mal; es responsabilidad de cada agente, si es que seguían." "Contratos por más de US 35 millones para renovar salas de interceptación", Radio Caracol, 25 de abril de 2014, http://www.caracol.com.co/noticias/judiciales/contratos-por-mas-de-us-35-millones-para-renovar-salas-de-interceptacion/20140425/nota/2194095.aspx

Una nueva fase de “chuzadas”

¿Cuál es el futuro de PUMA? El proyecto se detuvo en agosto de 2014, al advertir el fiscal general, Eduardo Montealegre, que no podía continuar si no se ponía aún más bajo el control de la Fiscalía. Advirtió públicamente contra el “uso indiscriminado de la interceptación como herramienta de investigación en casos en los que esa invasión de derechos fundamentales ni siquiera es necesaria en la lucha contra la criminalidad”.[73] A este respecto, Montealegre es inflexible: “Ningún otro organismo del Estado [diferente de la Fiscalía] está facultado para ordenar la interceptación de comunicaciones o administrar los equipos que sirven para esto”. [Énfasis añadido.] Se ha informado de que el equipo de PUMA está en cajas de cartón en el lugar que Privacy International vio,[74] mientras una comisión de funcionarios de la Policía y la Fiscalía determinan su futuro. Sin embargo, se han firmado varios contratos nuevos para la instalación de salas para PUMA en oficinas regionales de la Policía, incluidas las de Bucaramanga[75] y Villavicencio y según el Director de la Policía Rodolfo Palomino, PUMA será operativo en otoño de 2015.[76]

No está claro que la Fiscalía conozca cuán amplias son las capacidades de “monitoreo” de la Policía en actualidad, dado el escaso éxito del despliegue de Súper-PUMA, lo cual resulta preocupante para el derecho a la privacidad de la ciudadanía colombiana.

Privacy International habló del sistema PUMA con ex objetivos confirmados de la vigilancia del DAS y con personas que están convencidas de que siguen siendo objeto de vigilancia electrónica estatal.

“Aparte de lo que esta públicamente disponible, no tengo más información sobre PUMA. Mi opinión es que PUMA afecta derechos fundamentales. El uso de este sistema no respeta los derechos humanos”, afirma Reinaldo Villalba, del Colectivo de Abogados José Alvear Restrepo (CAJAR). CAJAR fue objetivo específico del DAS en el marco de una campaña de deslegitimización con el nombre en clave de

73 “Fiscalía le dice ‘no’ a sistema de interceptación ‘Puma’ de la Policía”, El Tiempo, sábado, 30 de agosto de 2014, http://www.eltiempo.com/politica/justicia/sistema-de-interceptacion-de-la-policia-puma/2092

74 En septiembre de 2014.

75 “Mantenimiento, Adecuación 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”, Policía Metropolitana de Bucaramanga, octubre de 2014, https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-1-127391

76 “Mantenimiento, Adecuación y Dotación de la Instalaciones para el Fortalecimiento e Implementación de la Plataforma Única de Monitoreo y Análisis de la Regional No. 7 ‘SALA PUMA’”, Policía Meta, octubre de 2014, https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-11-3000746

“Transmilenio”. Los documentos del DAS recuperados durante el escándalo de 2009 contienen detalladas descripciones de los movimientos de empleados de CAJAR y de sus familias, listas de sus contactos telefónicos y registros de los intentos del DAS de vincular números de teléfono con miembros de CAJAR. Reinaldo Villalba explica: “Estábamos seguros de que nos espiaban […] desde el inicio. De lo que no teníamos [conocimiento] en concreto era de las dimensiones de la persecución. En 2009 fuimos muy sorprendidos al conocer los miles de folios incautados en el DAS, agencia de inteligencia que depende directamente del presidente de la República, que revelaban la detallada persecución de la que éramos víctimas. Tenían información sobre cada reunión que habíamos mantenido y cada persona con la que nos habíamos visto en el extranjero. La persecución se extendía a nuestras familias, incluso a nuestros hijos menores de edad”.

Reinaldo afirma que CAJAR recibió avisos sobre la vigilancia de las comunicaciones en varios momentos.

“Una persona a quien yo conocía vino y me dijo: ‘Reynaldo, tengo información de la que tienes que confiar plenamente en su veracidad. No me cites como testigo porque negaré haber hablado alguna vez contigo. En el DAS han creado un grupo para monitorear las actividades de la CCAJAR y demás ONG de derechos humanos. Esta agencia de inteligencia tiene el encargo de aniquilarles’. No quisieron decirme cuál era la fuente [de la información]”. CAJAR sigue enfrentándose a acusaciones y ataques públicos de altas autoridades del Estado, así como a amenazas flagrantes de grupos paramilitares o presuntamente paramilitares: “Las labores ilegales de las agencias estatales de inteligencia no han cesado. Tenemos varios casos probados que muestran la continuidad de esta persecución”.

> **“Estábamos seguros de que nos espiaban […] desde el inicio. De lo que no teníamos [conocimiento] en concreto era de las dimensiones de la persecución.**
>
> **– Reinaldo Villalba. CCAJAR**

¿Está PUMA sujeto a salvaguardias suficientes para garantizar que no volverán a producirse las interceptaciones del DAS y de otros organismos a través de Esperanza o de sus propios sistemas independientes? El padre Alberto Franco, de la Comisión Intereclesial Justicia y Paz (CIJP) es escéptico: “Como decimos en Colombia, es pedir al gato que te guarde la carne o al diablo que haga las hostias (para la comunión”). La CIJP trabaja en la agitada región de Urabá para representar a comunidades campesinas. Documenta y denuncia ante los tribunales los vínculos entre los grupos paramilitares, las empresas privadas y el ejército colombiano. La acusan constantemente de simpatizar con las FARC.

“Damos siempre por hecho que estamos siendo vigilados. Es parte de nuestro modo de vida y trabajo” , explicó el padre Alberto. “Creemos que es una táctica para desgastarnos. Nos enteramos porque nos han dicho personas desde dentro del mismo Estado: los están escuchando’. Nos contaron cosas de discusiones

y conflictos internos de nuestra organización que nadie externo sabía.” Es difícil probar que se han vigilado las comunicaciones de una determinada persona. Pero que, a juzgar simplemente por la muestra de contratos que Privacy International ha analizado, el Estado colombiano haya gastado en el último decenio centenares de miles de millones de pesos en la creación de una extensa arquitectura de vigilancia indica que no es mero escaparate. Desde 2008, la CIJP viene recibiendo amenazas por teléfono, de las que informa a la Policía sin que se haya procesado a nadie por ello hasta ahora.

“Puede que haya gente dentro que quiera utilizarlo [PUMA] con buena intención. Pero la gente que quiere seguir la ley tiene dificultades”.

Padre Alberto Franco (CIJP)

El padre Alberto es escéptico con respeto al valor de PUMA como instrumento para hacer cumplir la ley sin un realineamiento fundamental de las prioridades de inteligencia. “Puede que haya gente dentro que quiera utilizarlo [PUMA] con buena intención. Pero la gente que quiere seguir la ley tiene dificultades. Porque no ha habido depuración del [personal del] DAS implicado en interceptaciones. Cuando cambiaron las instituciones, se reasignó sin más a la gente a otro lugar. La inteligencia militar no ha cambiado”.

“No conozco el sistema PUMA”, afirma Franklin Castañeda, presidente del Comité de Solidaridad con los Presos Políticos (CSPP). “En derechos humanos, nadie es un experto. Hemos recibido sólo asesoramiento básico: Lo único que decimos es que el Estado debería poner límites claros al efecto que tiene sobre la vida privada”. El CSPP hace trabajo de promoción acerca de la información de inteligencia. Propugna que se desclasifiquen y se eliminen los archivos del DAS, pues se utilizaban para identificar y asesinar a objetivos. Castañeda señala dos formas en las que el CSPP supo que estaban siendo espiados: informes de inteligencia posteriores al escándalo del DAS de 2009 en los que se mencionaba al CSPP y avisos de agentes estatales que advirtieron al CSPP de acciones judiciales que se pensaban entablar contra él sobre la base de comunicaciones y estrategias internas. Después de un ataque a los servidores informáticos del CSPP en el que sus archivos estaban siendo copiados y los reenviados a un destino desconocido, un grupo de seguridad digital ayudó al CSPP a establecer nuevos cortafuegos y barreras de intrusión Con todo, el personal del CSPP, como el de muchas organizaciones de derechos humanos, se esfuerza por utilizar sistemas de cifrado y herramientas que ayuden a proteger su trabajo. “Todos trabajamos bajo la premisa de que siempre estamos monitoreados”. ¿Habrá alguna vez razón para cambiar esta presunción?

Conclusión

Los sistemas de interceptación y monitoreo de Colombia operan en un marco jurídico que no protege debidamente el derecho constitucional de la ciudadanía colombiana a la privacidad. Las distinción que se establece en las leyes que regulan la vigilancia de las comunicaciones entre el monitoreo del espectro electromagnético y otras formas de interceptación da vía libre a la recopilación de cantidades masivas de datos personales sobre las comunicaciones privadas de la ciudadanía.

Las revelaciones sobre la magnitud del uso indebido que han hecho los agentes del gobierno colombiano de las tecnologías de vigilancia a lo largo del último decenio han conmocionado a la sociedad colombiana y al mundo. Las medidas adoptadas por la Fiscalía para investigar estos delitos y la buena disposición de los tribunales para garantizar la rendición de cuentas representan un positivo avance.

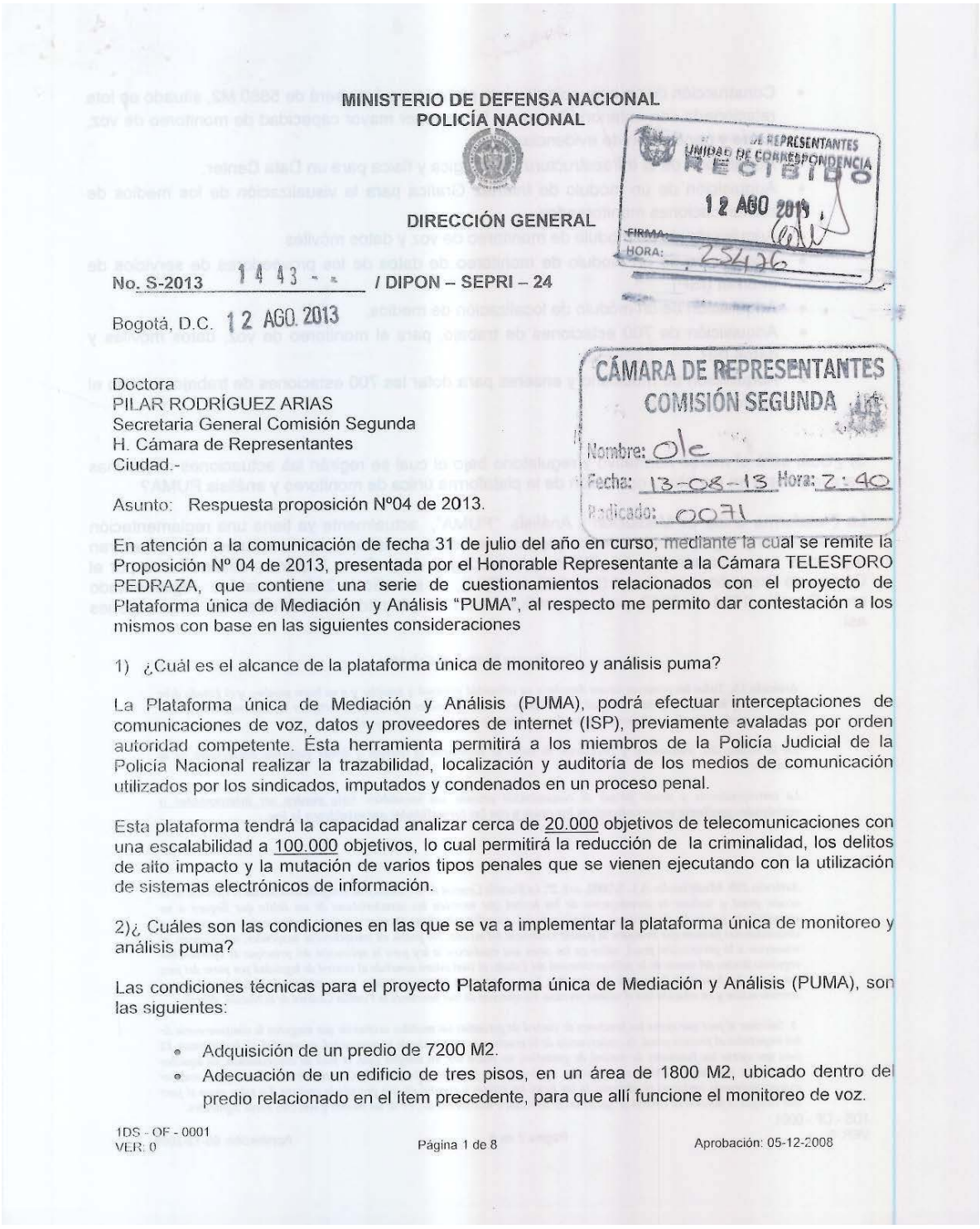
No obstante, no serán las tecnologías en sí las que brinden protección efectiva contra la extralimitación en la vigilancia de las comunicaciones. La mayoría de las herramientas de vigilancia no llevan incorporados mecanismos de control con que impedir el acceso ilegal, arbitrario o discriminatorio a los datos de las comunicaciones privadas. La protección efectiva del derecho a la privacidad ha de provenir en cierta medida de la existencia de mejores leyes, que no concedan a las autoridades policiales facultades de vigilancia masiva en virtud de una interpretación deficiente del proceso técnico de vigilancia.

La disparidad técnica y legal entre los sistemas de vigilancia, como el SIGD, PUMA y Esperanza, más las herramientas tácticas utilizadas por diversos organismos de manera independiente, genera estándares distintos de supervisión y el riesgo de que éstos no se respeten.

Es preciso abordar estas lagunas jurídicas para crear un sistema que garantice la seguridad de los colombianos y colombianas a la vez que respeta su derecho a la privacidad, especialmente la de quienes trabajan por una sociedad mejor y más democrática.

Anexos

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 14 43 - - / DIPON – SEPRI – 24

Bogotá, D.C. 12 AGO. 2013

CÁMARA DE REPRESENTANTES
COMISIÓN SEGUNDA
Nombre: Ole
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

Anexos

Página 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.***

(…)

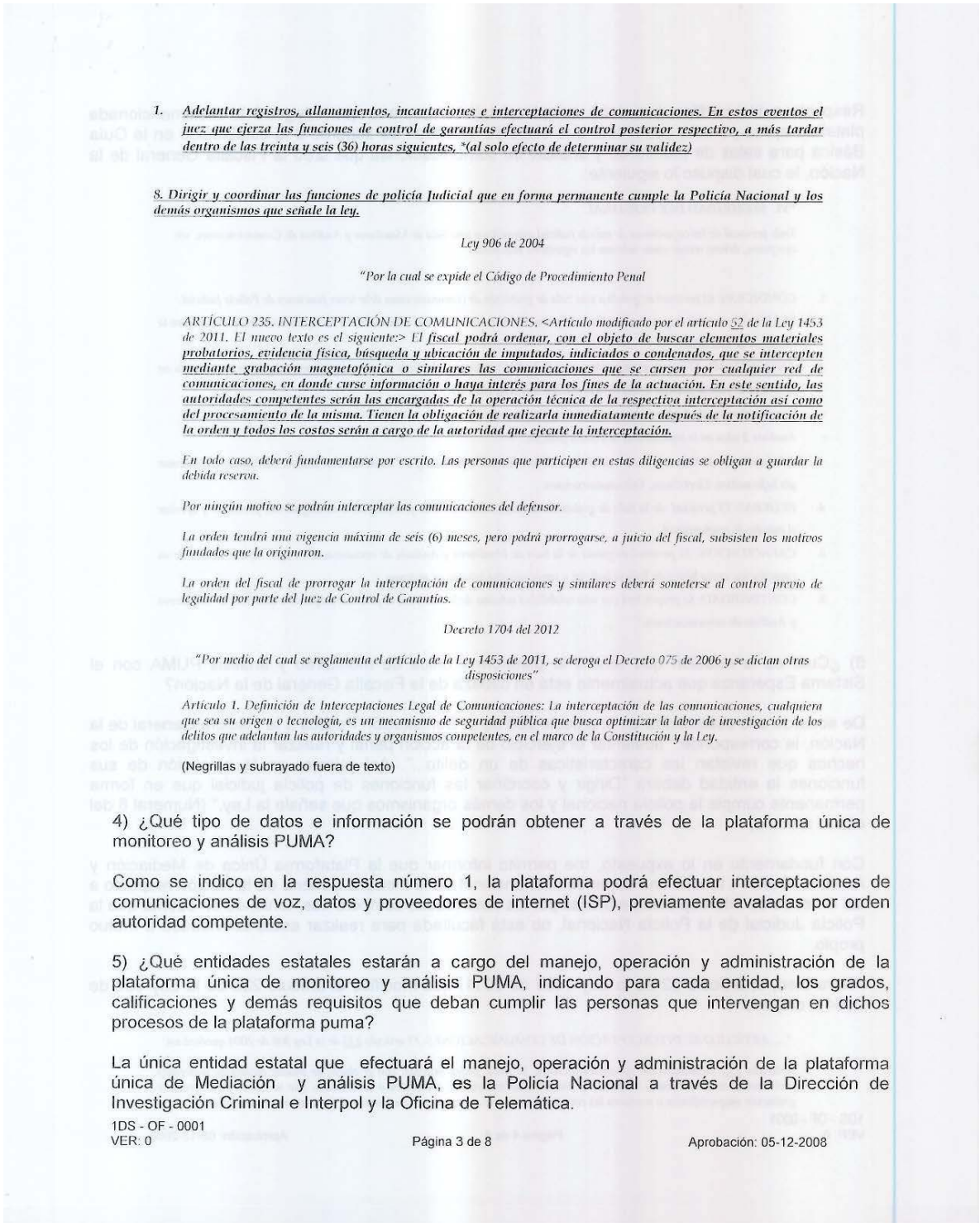
Artículo 250 Modificado. A.L. 3/2002, art. 2º. *La Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella 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

Anexos

Página 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

Anexos

Página 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

Anexos

Página 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.

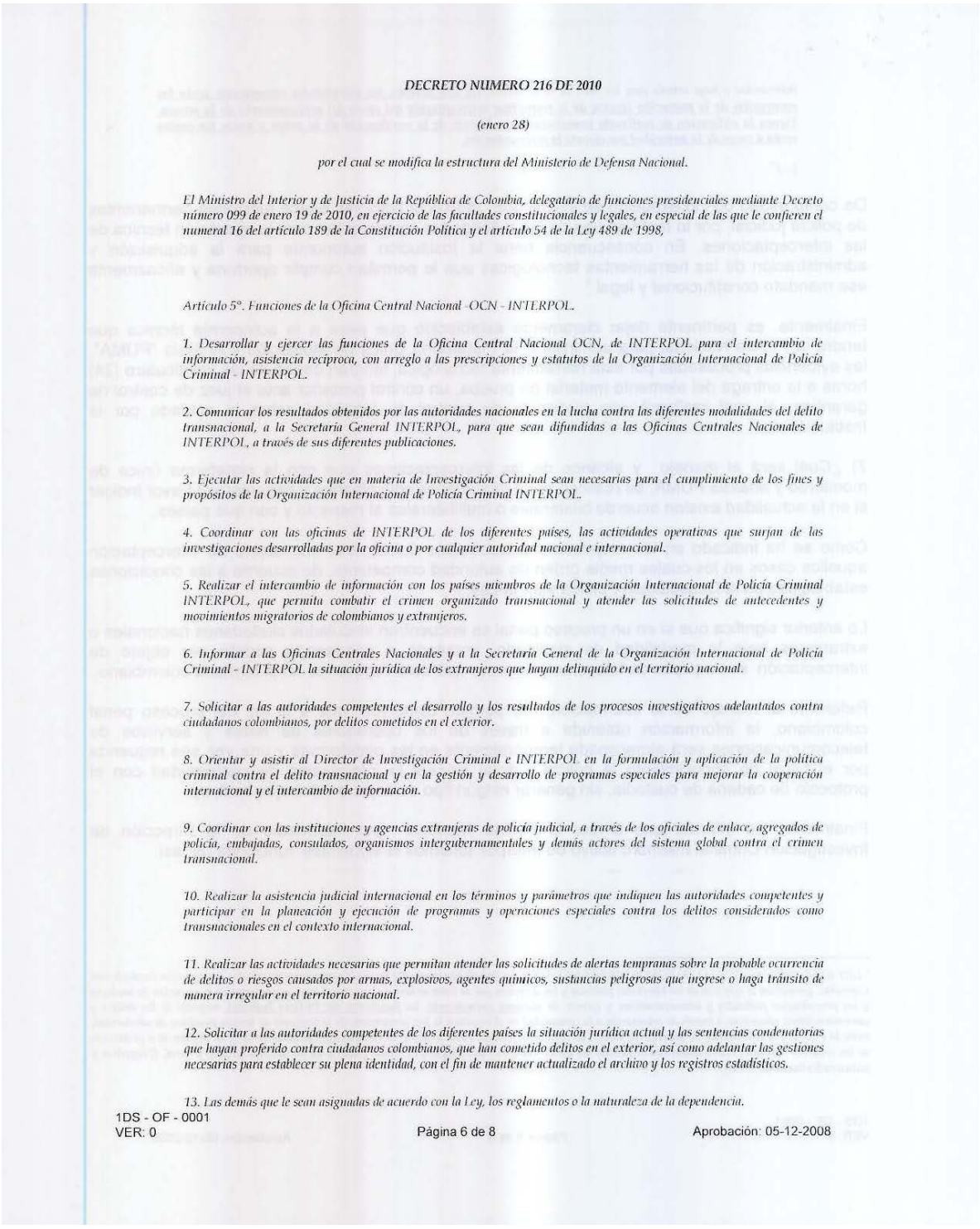
Referente al manejo de la información, me permito comunicar que a la luz del proceso penal colombiano, la información obtenida a través de los operadores de redes y servicios de telecomunicaciones será almacenada temporalmente en las plataformas y una vez sea requerida por el fiscal de conocimiento la 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 administrativas, 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)

Anexos

Página 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

Anexos

Página 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

Anexos

Página 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

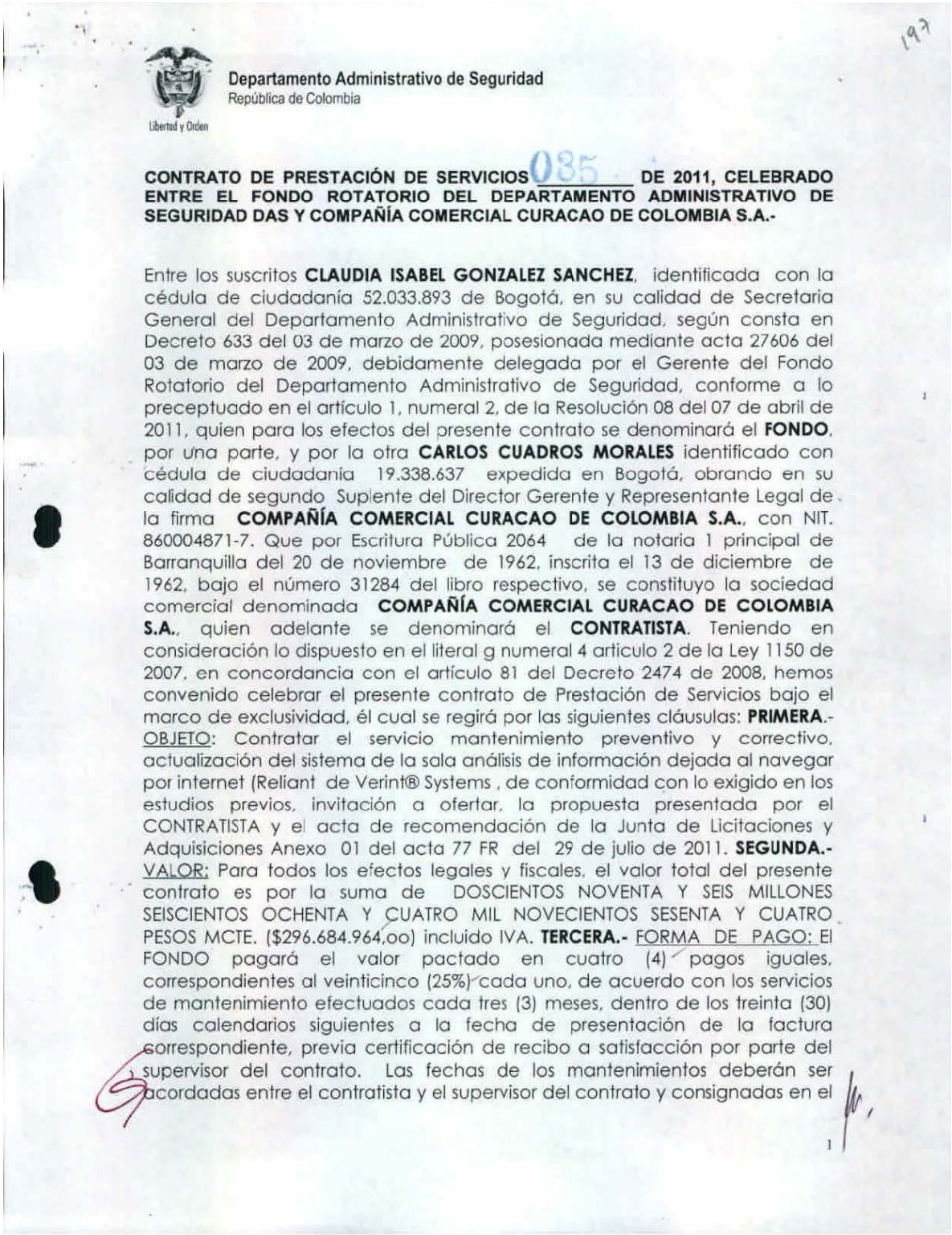
Elaborado por: MY. Néstor Flórez DIJIN
TE. Tatiana Ortega OFITE
Ase 08 Luisa Fernanda Aguirre Cardona SEGEN
Revisado por: TC Pablo Antonio Criollo Rey SEGEN
Revisado por: CT Óscar Andrés Rivera Rojas SEGEN

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

PROSPERIDAD PARA TODOS

Anexos

Página 1: 2011-8/22 DAS Contrato Verint



197

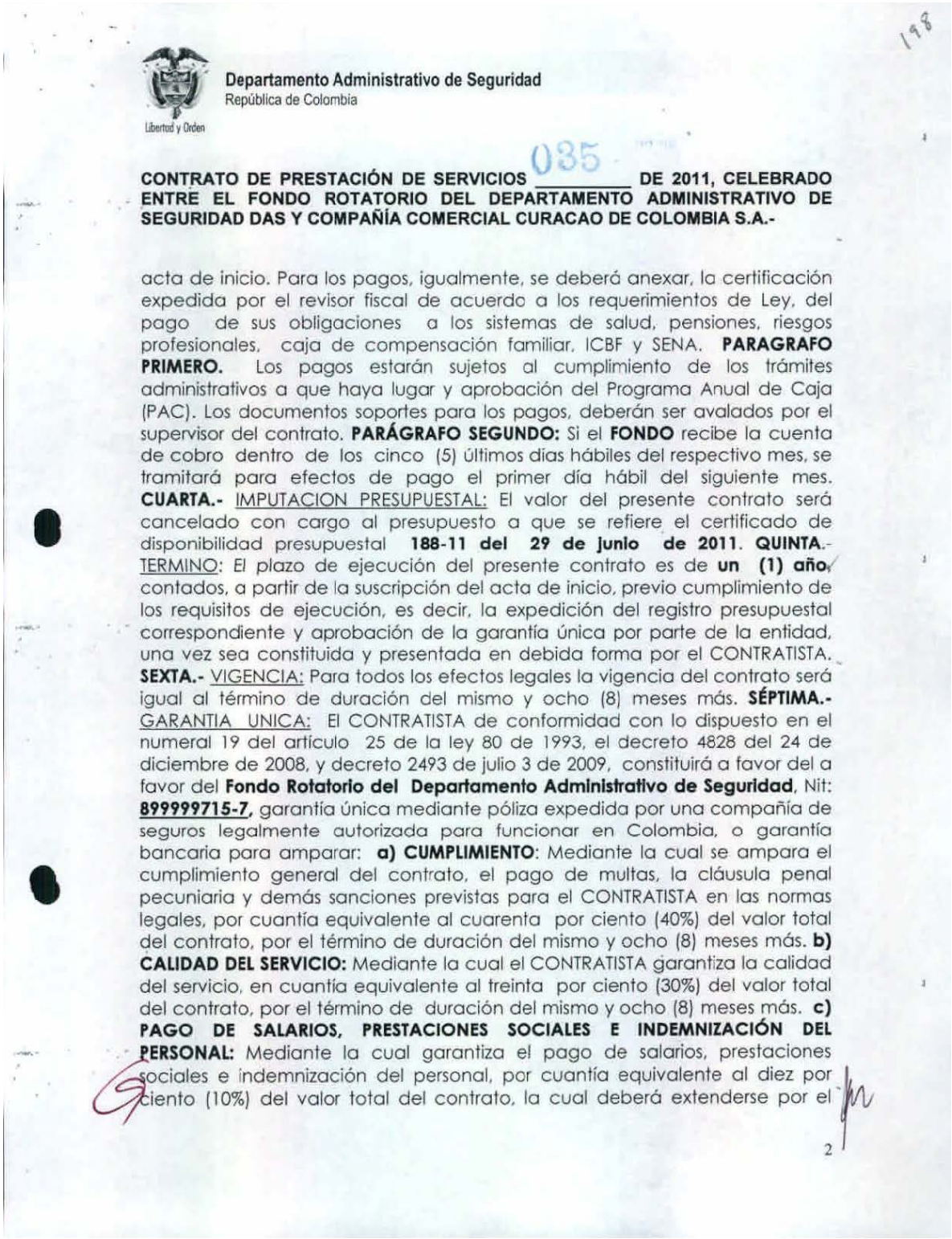
Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

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.-

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

Anexos

Página 2: 2011-8/22 DAS Contrato Verint



198

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

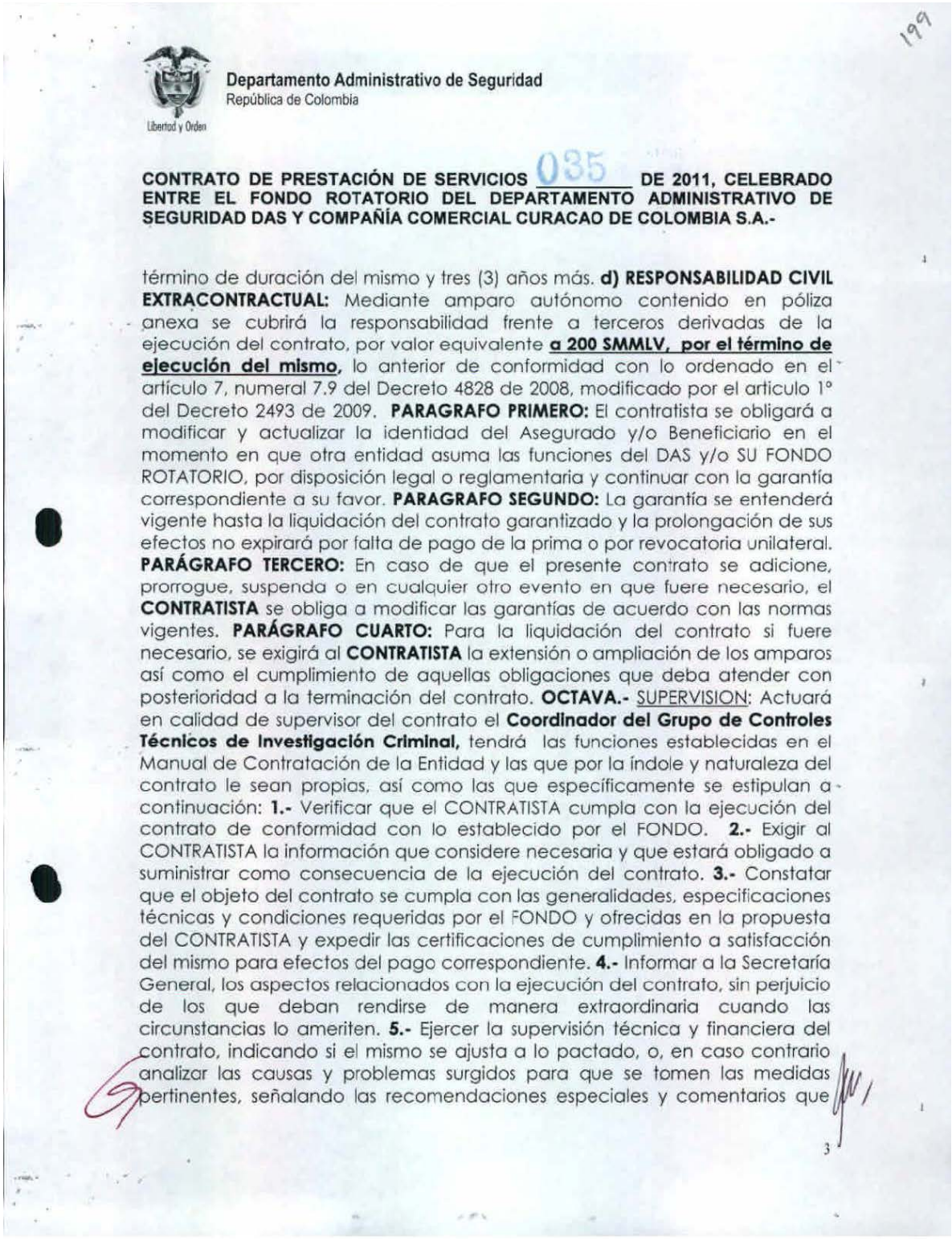
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 3: 2011-8/22 DAS Contrato Verint



199

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

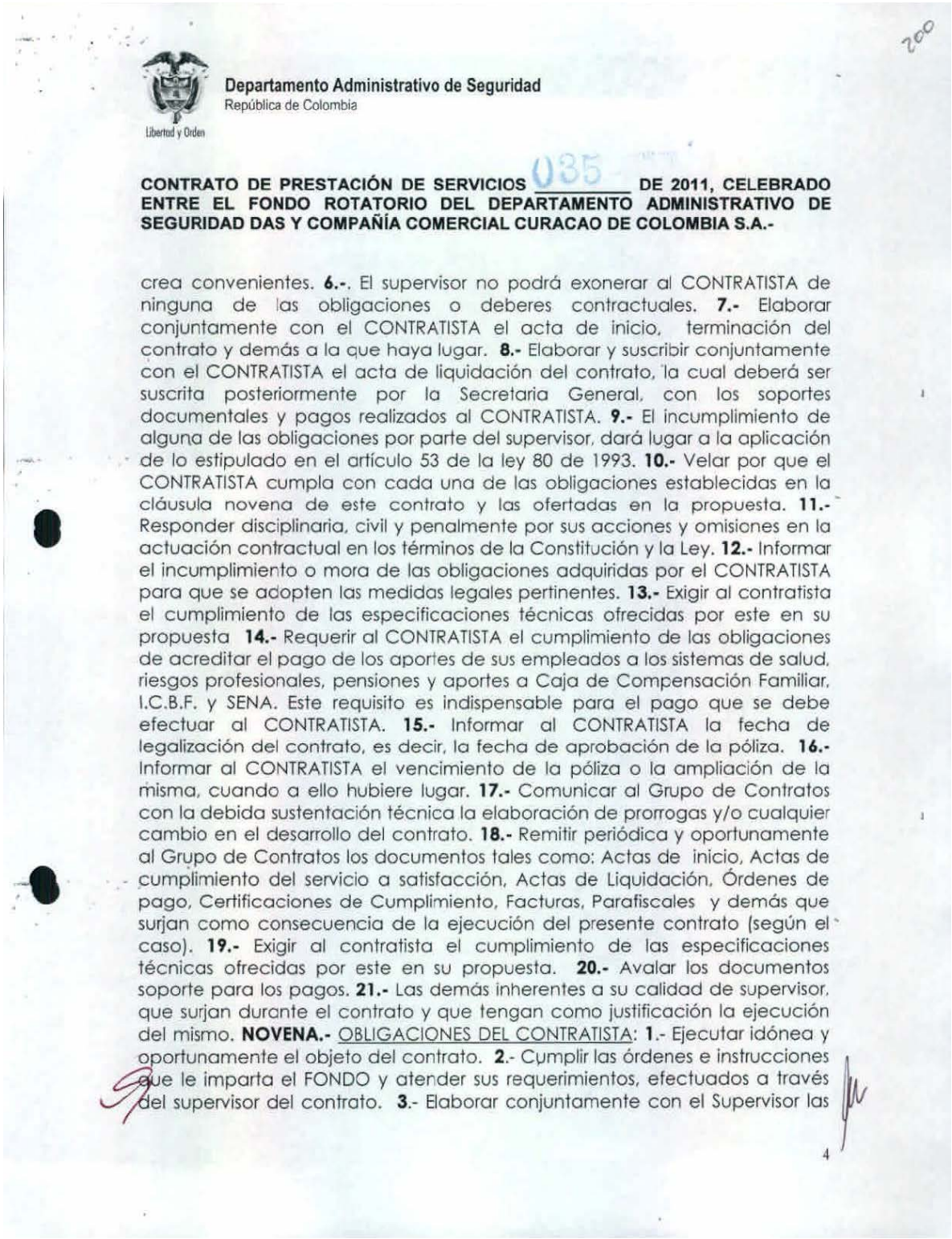
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 4: 2011-8/22 DAS Contrato Verint



Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

200

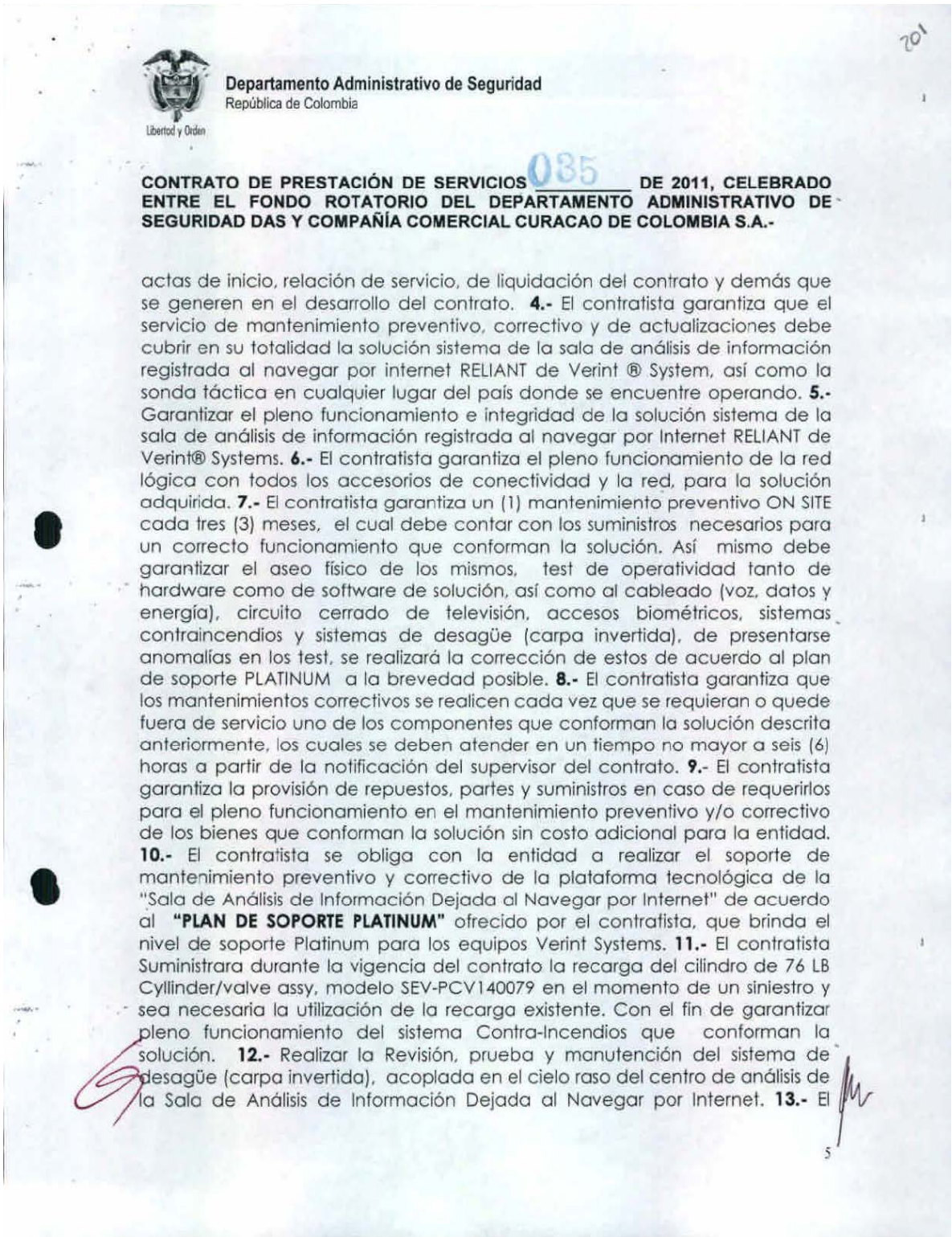
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 5: 2011-8/22 DAS Contrato Verint



Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

201

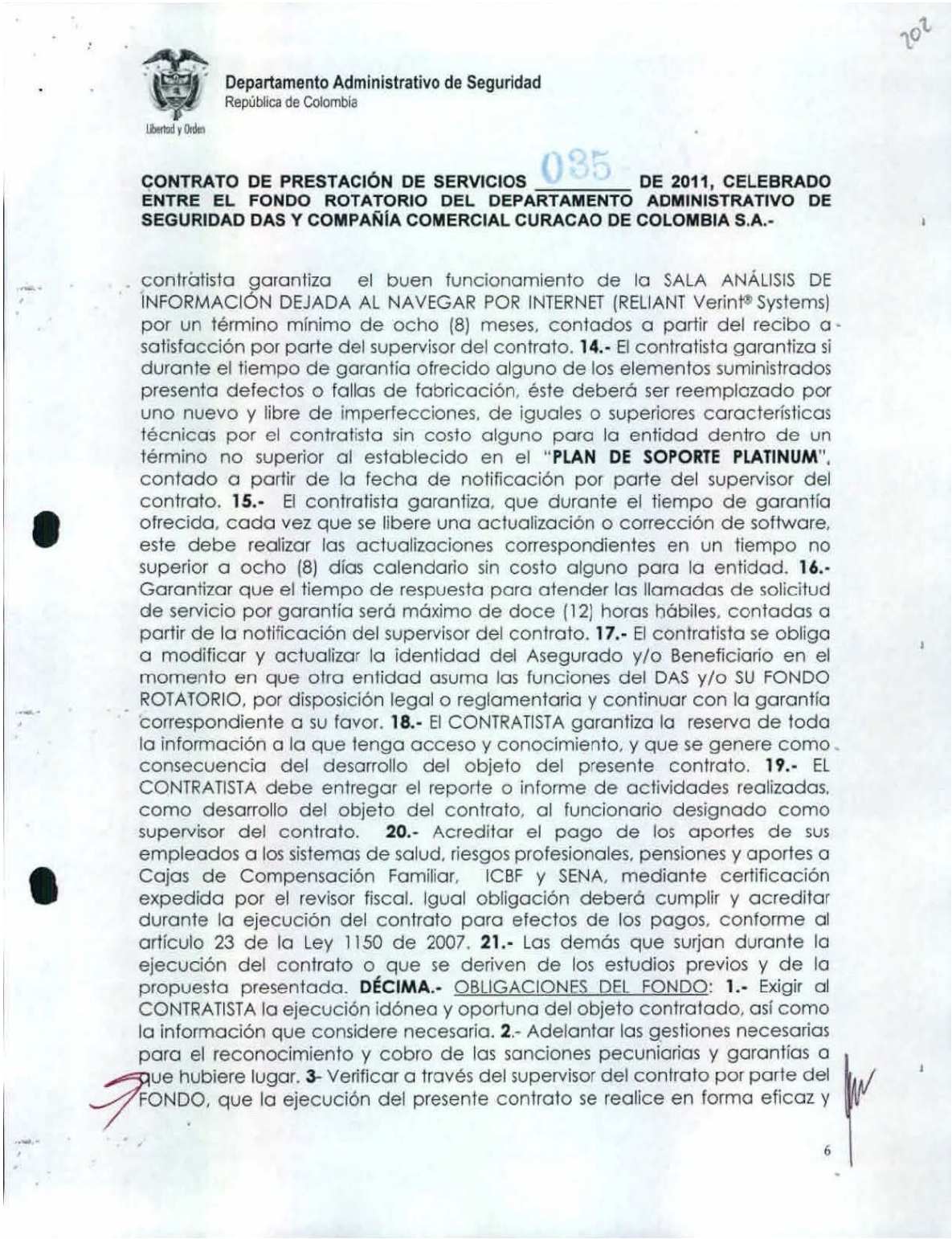
CONTRATO DE PRESTACIÓN DE SERVICIOS 085 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 6: 2011-8/22 DAS Contrato Verint



202

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

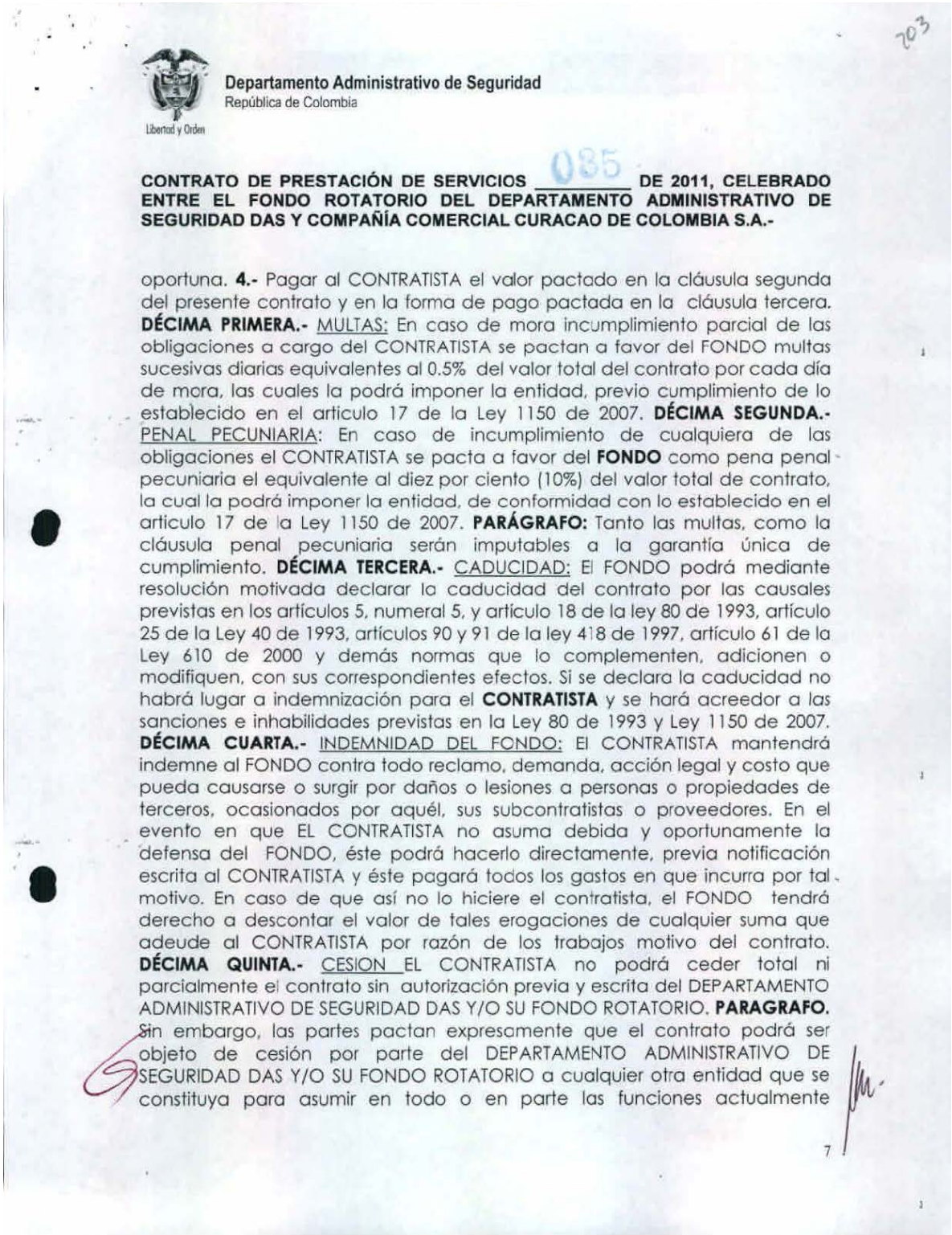
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 7: 2011-8/22 DAS Contrato Verint



203

Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

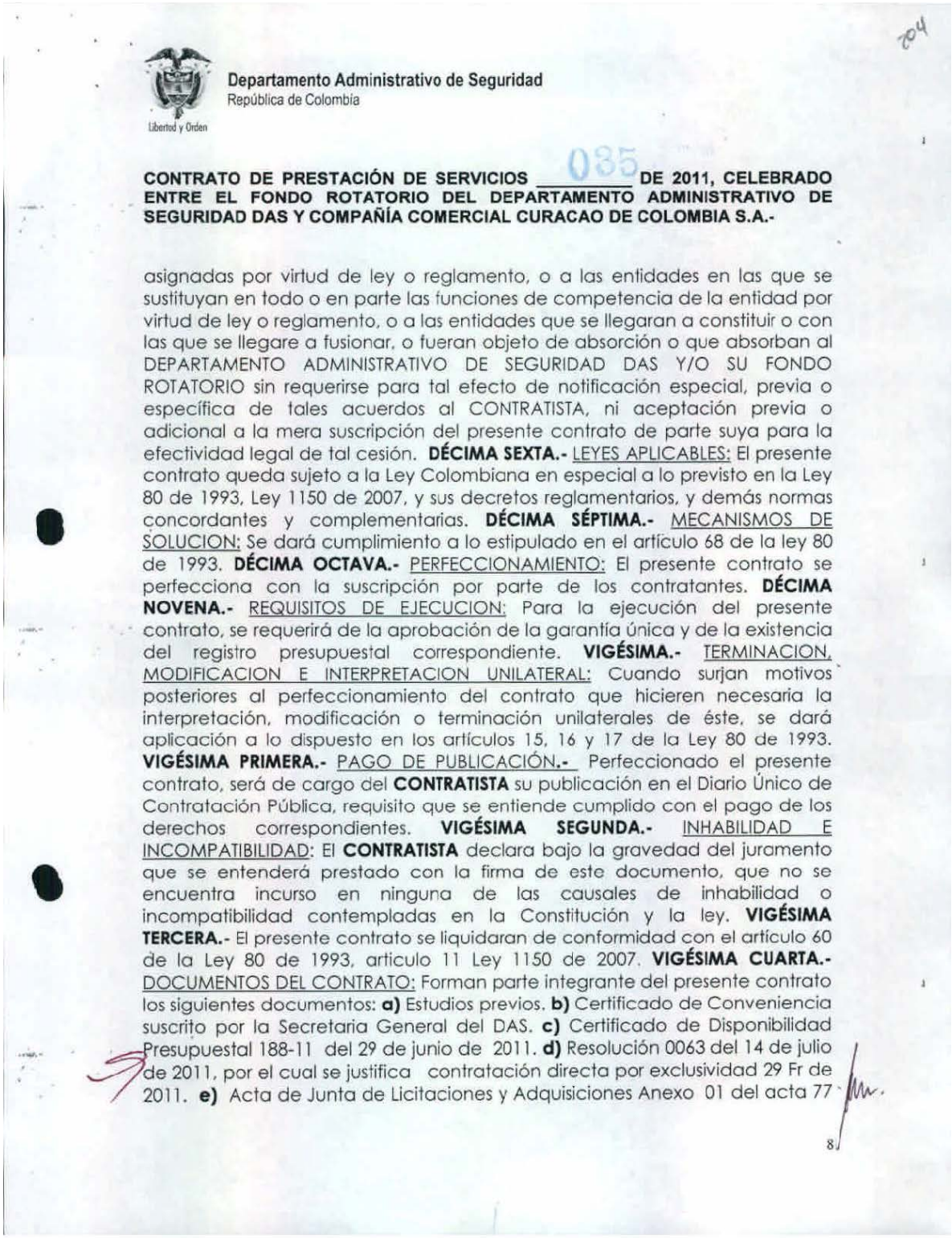
CONTRATO DE PRESTACIÓN DE SERVICIOS 085 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 8: 2011-8/22 DAS Contrato Verint



Departamento Administrativo de Seguridad
República de Colombia
Libertad y Orden

204

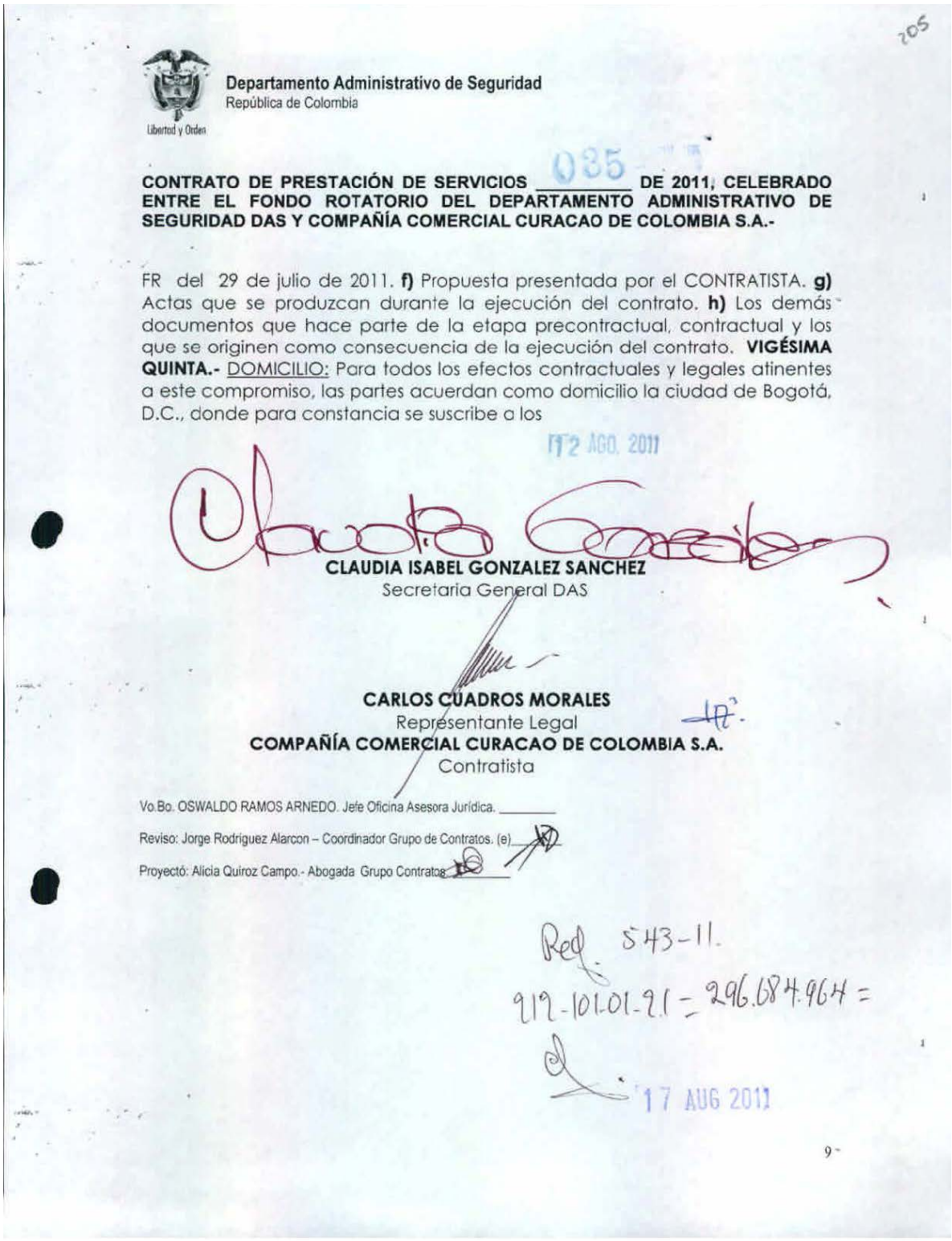
CONTRATO DE PRESTACIÓN DE SERVICIOS 035 DE 2011, CELEBRADO ENTRE EL FONDO ROTATORIO DEL DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD DAS Y COMPAÑÍA COMERCIAL CURACAO DE COLOMBIA S.A.-

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

Anexos

Página 9: 2011-8/22 DAS Contrato Verint



205

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 _____

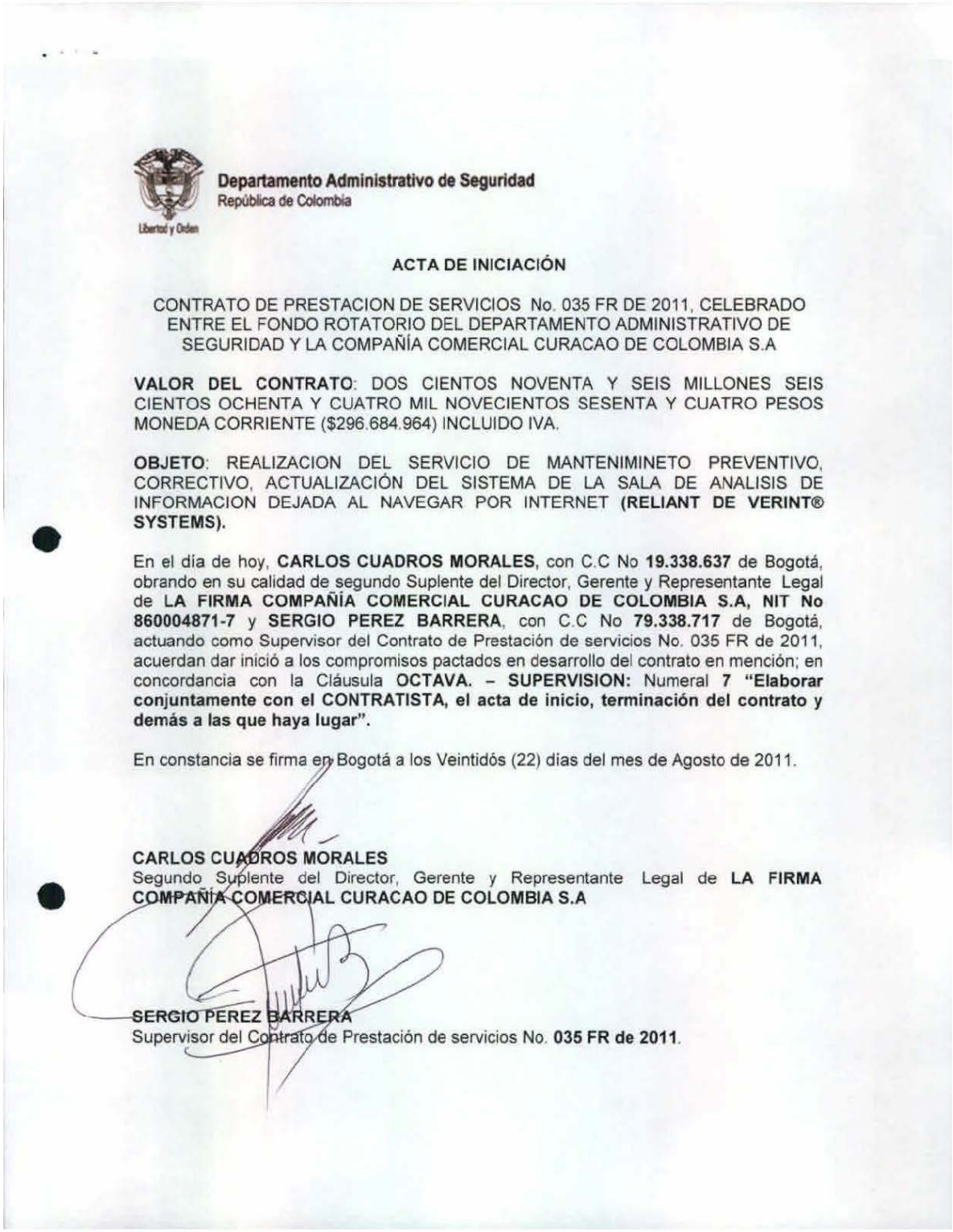
Red 543-11.
919-101.01-21 = 296.684.964 =

17 AUG 2011

9

Anexos

Página 10: 2011-8/22 DAS Contrato 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".**

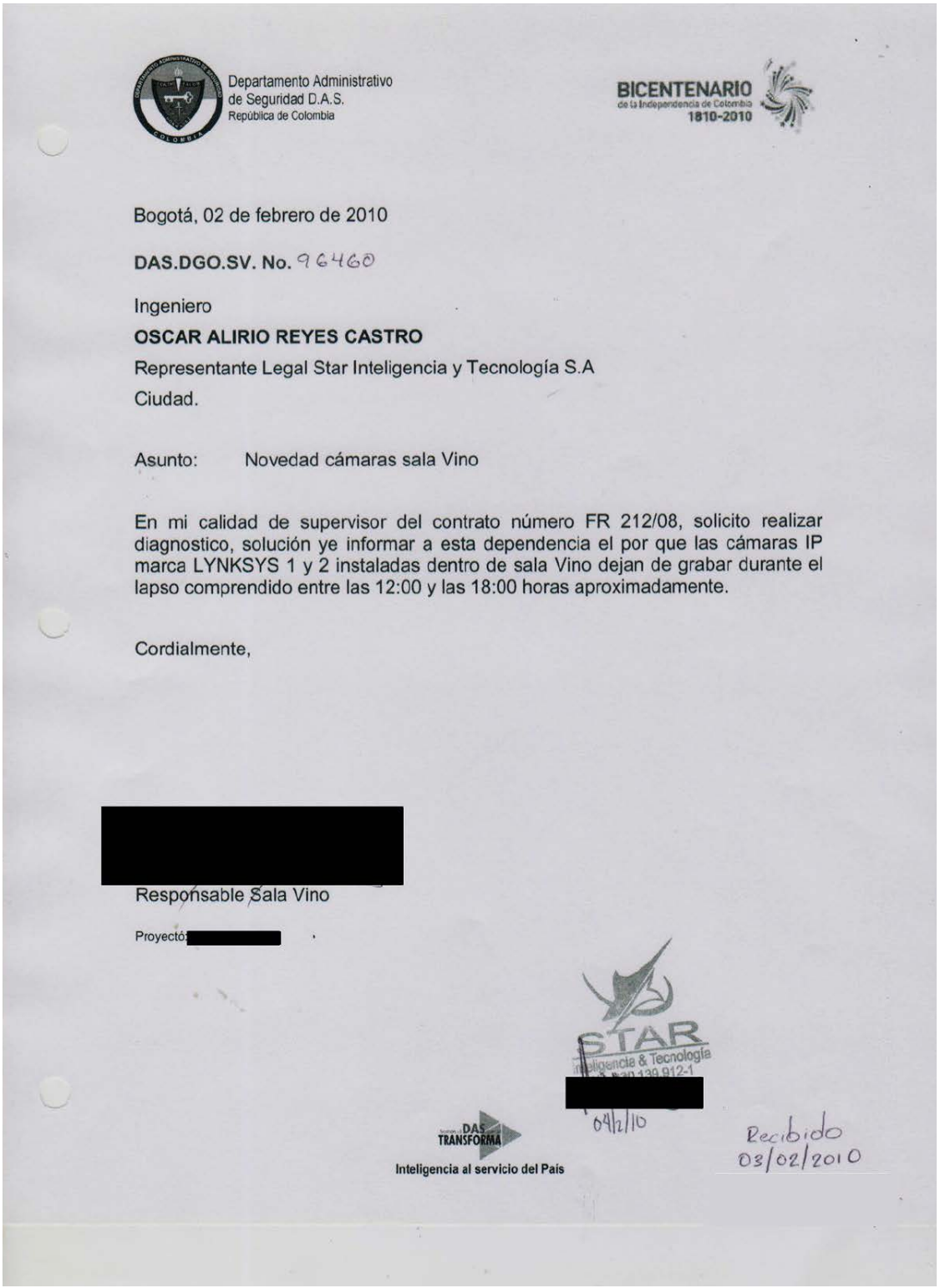
En constancia se firma en Bogotá a los Veintidós (22) dias del mes de Agosto de 2011.

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**.

Anexos

Anexo - Mensajes de error



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]

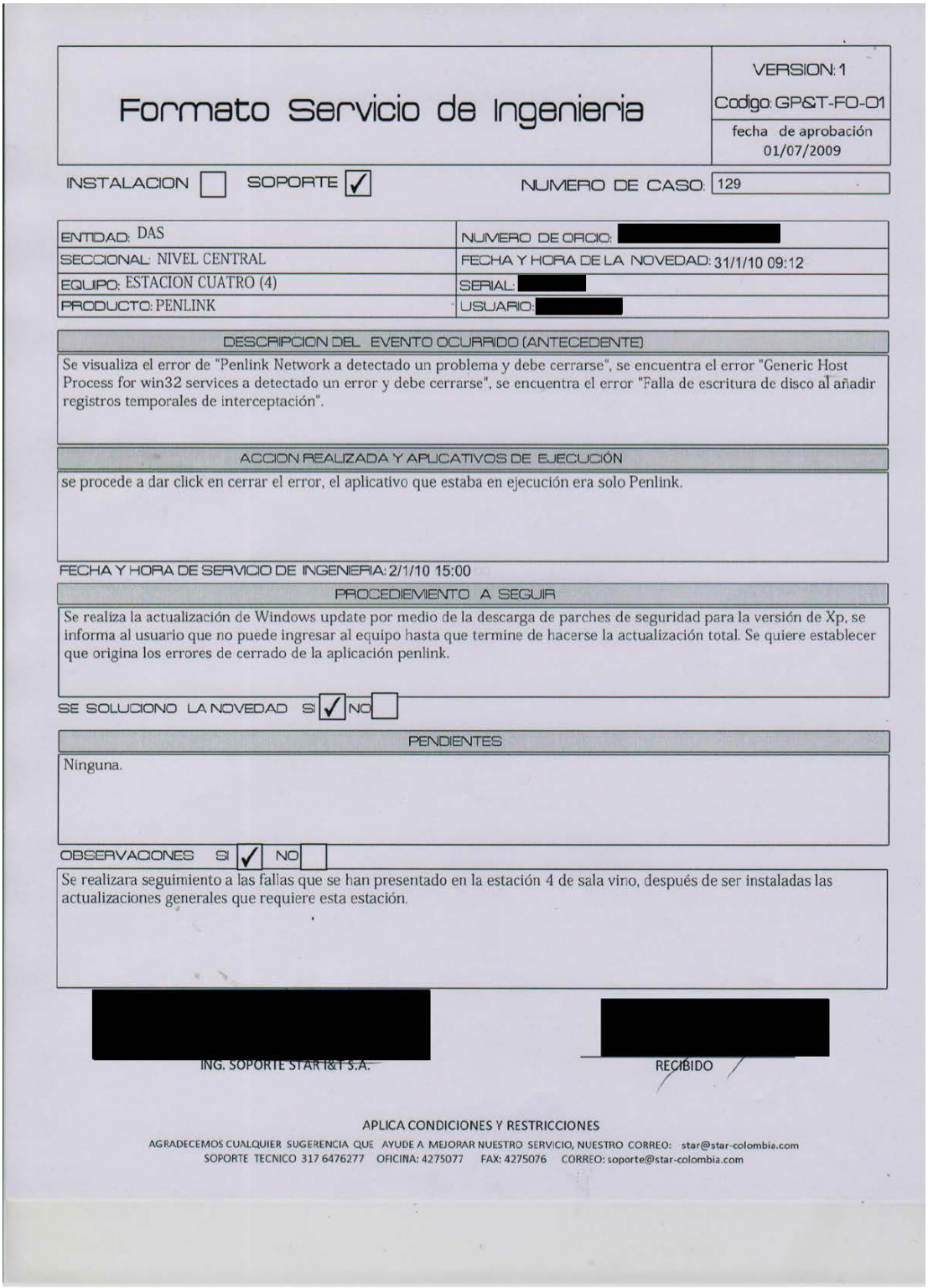
STAR
Inteligencia & Tecnología
[redacted]
04/2/10

DAS TRANSFORMA
Inteligencia al servicio del País

Recibido
03/02/2010

Anexos

Anexo - Mensajes de error



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.

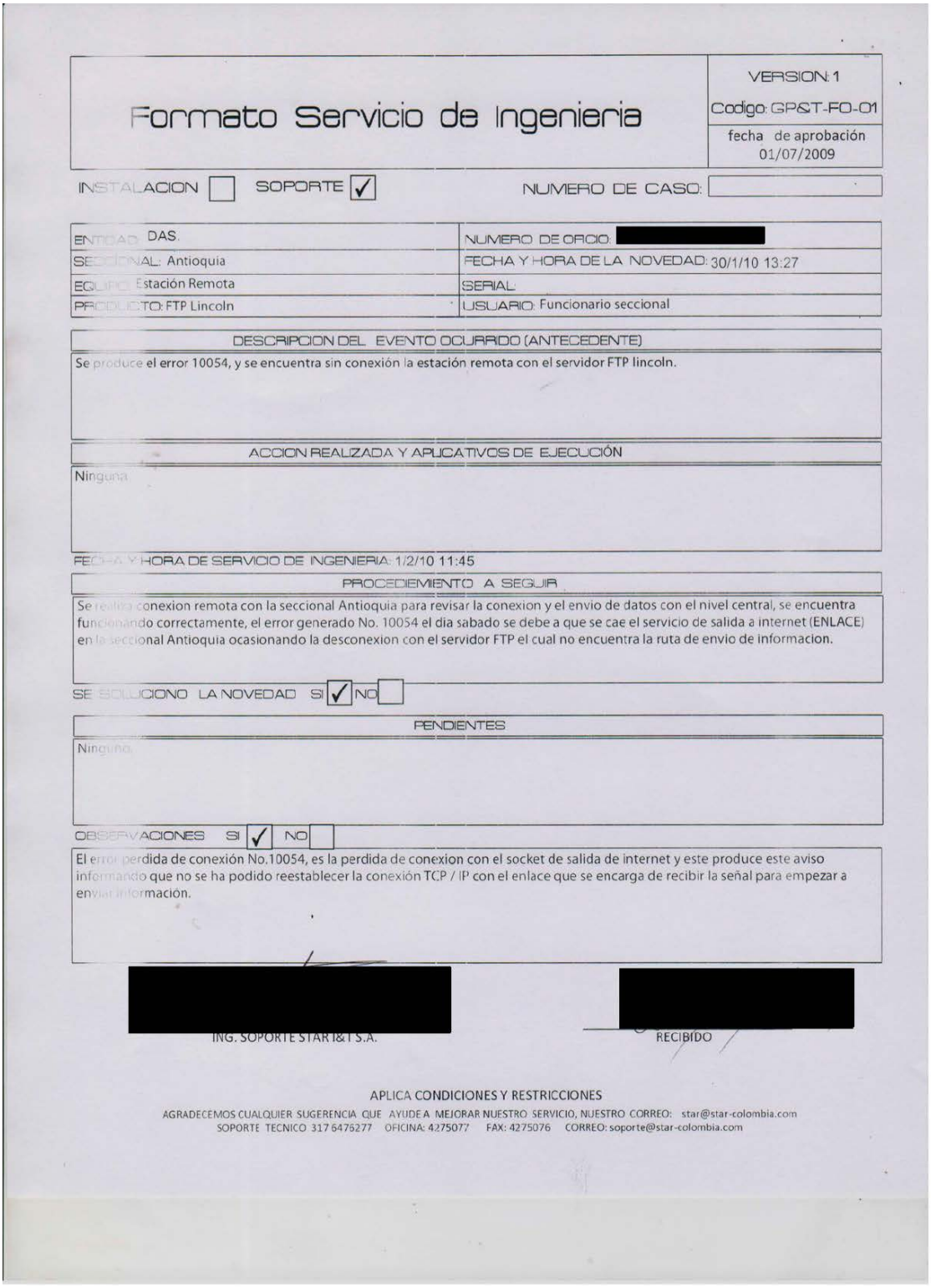
[redacted]
RECIBIDO

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

Anexos

Anexo - Mensajes de error



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.

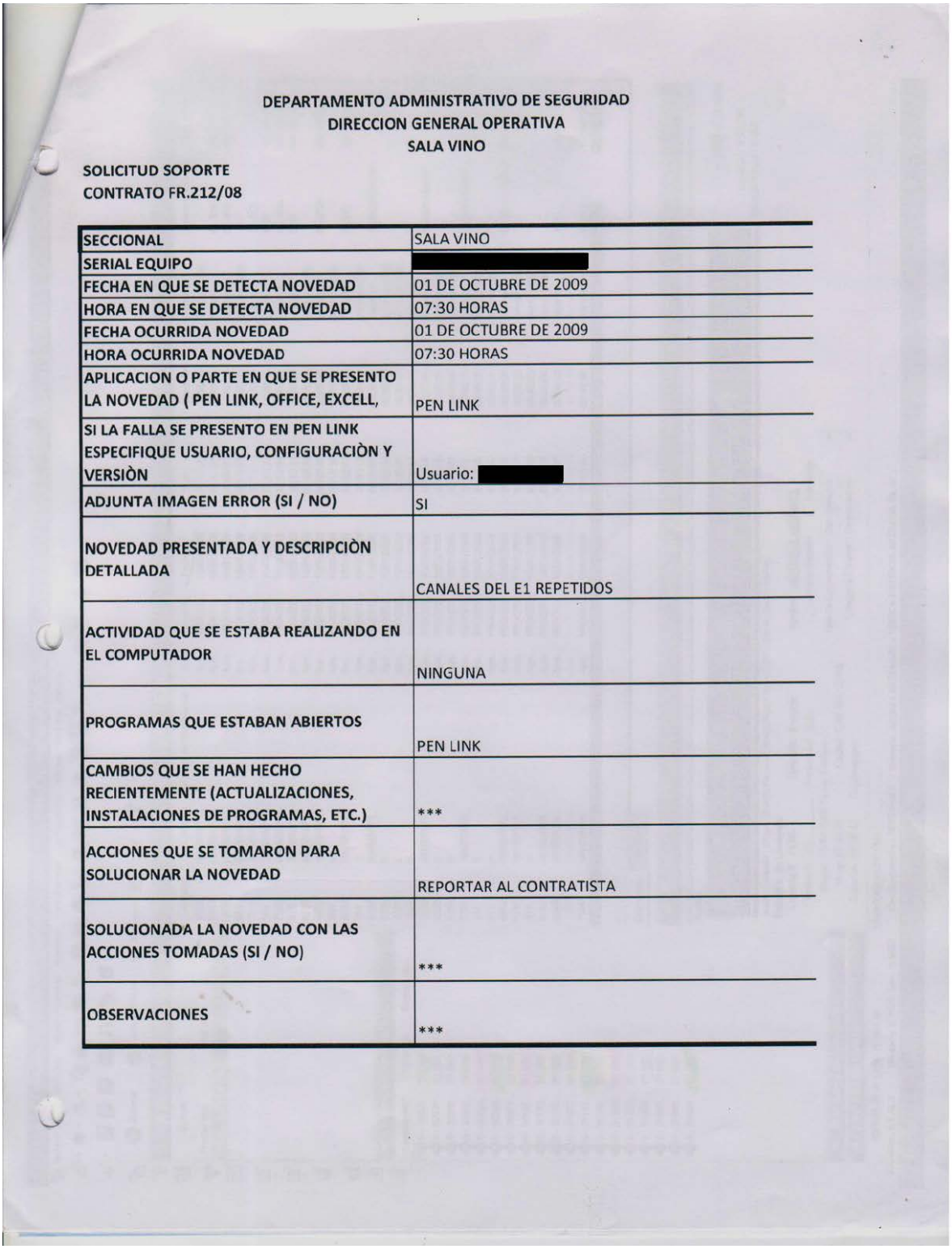
[redacted]
RECIBIDO

APLICA CONDICIONES Y RESTRICCIONES

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

Anexos

Anexo - Mensajes de error



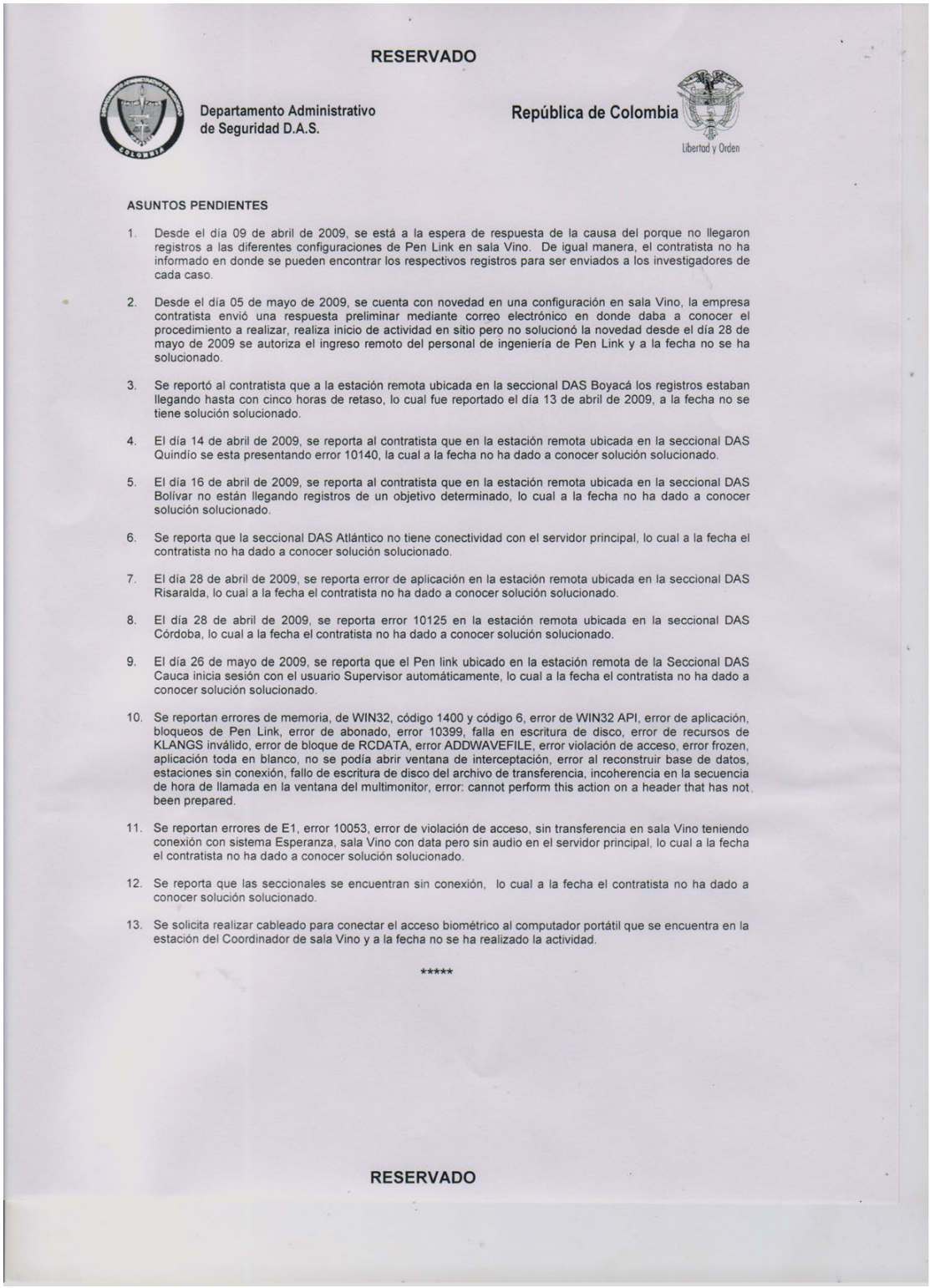
DEPARTAMENTO ADMINISTRATIVO DE SEGURIDAD
DIRECCION GENERAL OPERATIVA
SALA VINO

SOLICITUD SOPORTE
CONTRATO FR.212/08

SECCIONAL	SALA VINO
SERIAL EQUIPO	[redacted]
FECHA EN QUE SE DETECTA NOVEDAD	01 DE OCTUBRE DE 2009
HORA EN QUE SE DETECTA NOVEDAD	07:30 HORAS
FECHA OCURRIDA NOVEDAD	01 DE OCTUBRE DE 2009
HORA OCURRIDA NOVEDAD	07:30 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, CONFIGURACIÒN Y VERSIÒN	Usuario: [redacted]
ADJUNTA IMAGEN ERROR (SI / NO)	SI
NOVEDAD PRESENTADA Y DESCRIPCIÒN DETALLADA	CANALES DEL E1 REPETIDOS
ACTIVIDAD QUE SE ESTABA REALIZANDO EN EL COMPUTADOR	NINGUNA
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	***

Anexos

Anexo - Mensajes de error



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

Anexos

Anexo - La presentación de Palantir con Star Inteligencia

Palantir

Presentación Palantir – Star I&T S.A

[redacted]

Palantir

¿Quién es Palantir?

- Ingenieros destacados de “Silicon Valley”.
- Solucionan problemas complejos para gobiernos y entidades privadas.
- Reuso de la plaforma a través de verticales.
- ~550 empleados, 75% ingenieros.
- Palo Alto HQ; NY, DC, LON, AU…