



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Llamamiento Décimo Octavo fracción II y V, incisos a) y d) y Vigésimo Cuarta fracción II de los Estatutos Generales para la Clasificación y Descalificación de la Información de sus dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece los Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Rubrica del Titular de la Unidad Administrativa	

ANEXO TÉCNICO

ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS"

DESCRIPCIÓN DE "EL BIEN".

La descripción de "EL BIEN" se encuentra precisada en la cotización expedida por "EL PROVEEDOR" en fecha 24 de octubre de 2014, misma que se agrega para formar parte del presente acuerdo de voluntades.

Arquitectura de Alto Nivel

El sistema "Pegasus" está diseñado en capas. Cada capa tiene la responsabilidad de formar juntos una solución de análisis y recolección de inteligencia cibernética integral.

Las capas principales y bloques de construcción de los sistemas son:

- **Instalaciones:** Capa de la instalación está a cargo de la emisión de las nuevas instalaciones de agente, actualizar y desinstalar agentes existentes.
- **Recolección de datos:** Capa de la recopilación de datos está a cargo de recoger los datos desde el dispositivo instalado. "Pegasus" ofrece inteligencia integral y completa mediante el empleo de métodos de recolección de cuatro
- **Extracción de datos:** Extracción de los datos todo que existe en el dispositivo sobre la instalación del agente
- **Vigilancia pasiva:** Nuevos datos de llegada al dispositivo
- **Colección Monitor Activo:** Activar la cámara, micrófono, GPS y otros elementos para recopilar datos en tiempo real
- **Colección basada en eventos:** Definir escenarios que activa automáticamente datos específicos colección
- **Transmisión de datos:** La capa de transmisión de datos es la encargada de transmitir los datos a los servidores de comando y control, utilizando la forma más eficiente y segura.
- **Análisis de la presentación:** El componente de presentación análisis es una interfaz de usuario que se encarga de presentar los datos recogidos a los operadores y analistas, convirtiendo los datos de inteligencia. Esto se hace mediante los siguientes módulos:

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales:	Totalmente
Fundamento Legal	15 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, artículos 41 y 42 y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXII de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años* (sic)
Roberto del Tiller de la Unidad Administrativa	

- **Monitoreo en tiempo real:** Presenta los datos recogidos en tiempo real de específico o varios objetivos. Este módulo es muy importante cuando se trata de objetivos sensibles o durante las actividades operacionales, donde cada pieza de información que llega es crucial para la toma de decisiones.
- **Análisis offline:** Avanzado mecanismo de consultas que permite a los analistas consultar y recuperar cualquier pieza de información que se recopila. El mecanismo avanzado proporciona herramientas para encontrar información y conexiones ocultas.
- **Análisis basado en geolocalización:** presenta los datos recogidos en un mapa y conducta consultas basadas en geo.
- **Administración:** es el componente de administración encargado de gestionar el permiso de todo el sistema, seguridad y salud: contactos de extractos mensajes, correos electrónicos, fotos, archivos, ubicaciones, contraseñas, lista de procesos y más
- **Permiso:** el mecanismo de permisos permite al administrador del sistema gestionar los distintos usuarios del sistema. Proporcionar cada uno de ellos el nivel correcto acceso sólo a los datos que se les permite. Esto permite para definir los grupos de la organización que manejan sólo uno o más temas y otros grupos que maneja diferentes temas.
- **Seguridad:** El módulo de seguridad monitorea el nivel de seguridad del sistema, asegurándose de que los datos recogidos se insertan a la base de datos de sistema limpio y seguro para su futura revisión.
- **Salud:** El componente de salud de la solución de "Pegasus" monitorea el estado de todos los componentes asegurándose de que todo está funcionando sin problemas. Monitorea la comunicación entre las diferentes partes, el rendimiento del sistema, la disponibilidad de almacenamiento de información y alertas si algo falla.

Solución de Hardware

Las especificaciones de hardware para el funcionamiento del sistema Pegasus depende del número de agentes instalados concurrentes, el número de estaciones de trabajo, la cantidad de datos almacenados y por cuánto tiempo deben guardarse.

Todo el hardware necesario es suministrado con el sistema al despliegue y requerir personalización local que tiene que ser manejado por el cliente en función de que las direcciones. Si es necesario, hardware puede adquirirse por el cliente en función de las especificaciones proporcionadas por nosotros.

Operadores de Terminales

Los operadores de las terminales son unidades estándar de escritorio, con las siguientes especificaciones:

- Procesador: Core i5
- Memoria: 3 GB de RAM





*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, fracciones c) y d) y Vigésimo Cuarta fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años* (sic)
Reserva del Titular de la Unidad Administrativa	

- Disco Duro: 320 GB
- Sistema operativo: Windows 7

Sistema de Hardware

Para apoyar plenamente la infraestructura del sistema, el siguiente hardware se requiere:

- Dos unidades de 42U gabinete
- Redes hardware
- 10TB de almacenamiento
- 5 servidores estándar
- UPS
- Celular módems y tarjetas SIM

GARANTÍA, MANTENIMIENTO Y ACTUALIZACIONES DE "EL BIEN"

La garantía de "EL BIEN" será de 12 meses a partir de la fecha de recepción del mismo. "EL PROVEEDOR" se compromete a proporcionar mantenimiento a "EL BIEN" y brindar soporte, sin costo para "LAPROCURADURÍA" de conformidad a lo siguiente:

Mantenimiento y Soporte

"EL PROVEEDOR" proporcionará servicios de mantenimiento y soporte de nivel tres niveles que incluye:

- **Nivel 1:** Sistema estándar operaciones problemas de correo electrónico y soporte telefónico
- **Nivel 2:** Resolución proactiva de ingenieros dedicados problemas o técnica inspeccionará, examinar y resolver problemas técnicos comunes, poniendo sus mejores esfuerzos, asistencia remota usando software de escritorio remoto y una red privada Virtual (VPN) cuando así lo solicite
- **Nivel 3:** Fallo sistema de fijación y las actualizaciones de sistema importantes desperfectos

Soporte telefónico: además de lo anteriormente mencionado, "EL PROVEEDOR" proporciona el teléfono y correo electrónico para cualquier pregunta y solución de algún el problema.

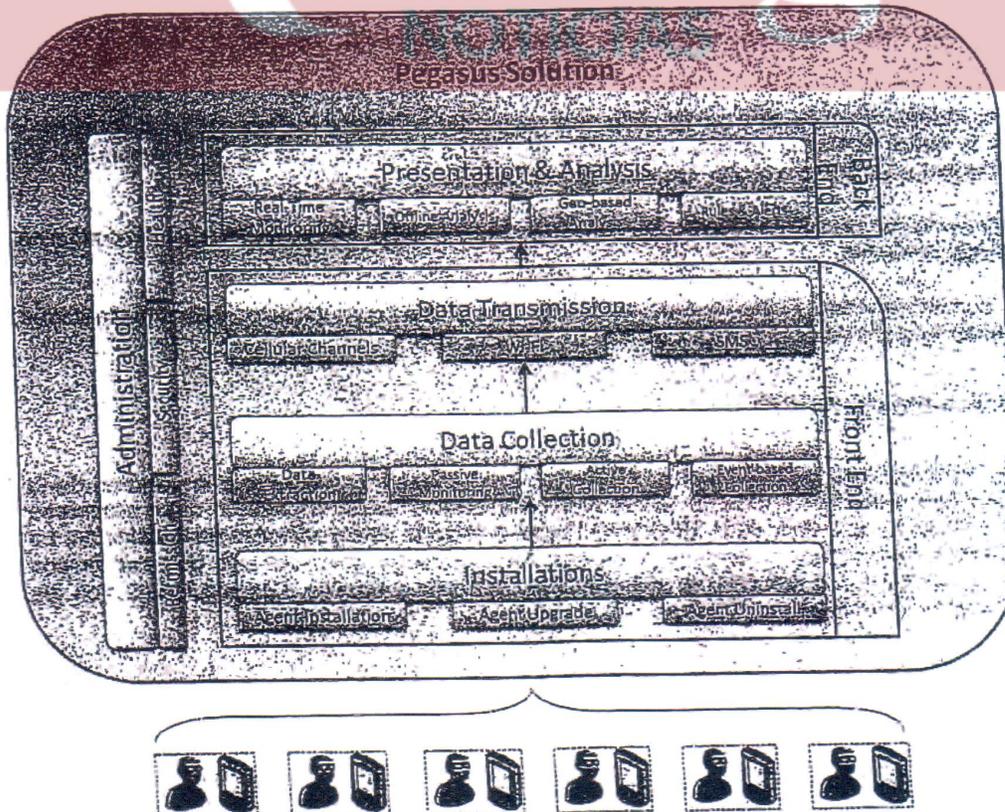
Además, "EL PROVEEDOR" será capaz de añadir la siguiente asistencia

- Asistencia en el sitio planeado o de emergencia
- Sistema de monitoreo de salud

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Informativa para el Combate a la Delincuencia
Clasificación	Reservada
Partes e Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Didáctico Códice fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años* (sic)
Ámbito del "Fidei" de la Unidad Administrativa	

Las capas del sistema y los componentes se muestran en la figura 1.

Figura 1: Arquitectura de nivel alto de Pegasus



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Período o Situaciones reservadas o condicionales	Totalmente
Fundamento Legal	13 Fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Gubernamental Pública y Vigésimo Cuarto Fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXII de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años* (sic)
Rubrica del Titular de la Unidad Administrativa	

Instalación del Agente

Para empezar a recolectar datos desde smartphone su blanco, un componente de software de base ("agente") debe de forma remota y secretamente instalarse en su dispositivo.

Propósito del Agente

El "agente", un componente de software base, reside en los dispositivos de punto final de las metas monitoreadas y su propósito es reunir los datos para que se configuró. El agente es compatible con los sistemas operativos más populares: dispositivos basados en Symbian, BlackBerry, Android y iOS (iPhone).

Cada agente es independiente y está configurado para recolectar información diferente del dispositivo y para transmitir la señal mediante canales específicos en plazos definidos. Los datos se envían a los servidores de Pegasus de manera oculta, comprimida y encriptada.

El agente continuamente recopila la información del dispositivo y lo transmitirá una vez que disponga de conexión a internet confiable.

Cifrado de las comunicaciones, el uso de muchas aplicaciones y otras comunicaciones ocultar métodos ya no es relevantes cuando un agente está instalado en el dispositivo.

Vector de Instalación del Agente

Inyectables y la instalación de un agente en el dispositivo son la fase más sensible e importante de la operación de inteligencia llevada a cabo en el dispositivo de destino. Cada instalación debe planearse con cuidado para asegurar que tiene éxito. El sistema Pegasus soporta varios métodos de instalación. La variedad de métodos de instalación responde a los distintos escenarios operacionales que son únicos para cada cliente, dando como resultado la solución más completa y flexible. Los siguientes son los vectores de instalación admitidos:

Instalación Remota (Rango):

- **Por aire (OTA):** empuje se envía un mensaje de forma remota y secretamente en el dispositivo móvil. Este mensaje activa el dispositivo para descargar e instalar al agente en el dispositivo durante toda la instalación proceso de cooperación o compromiso del objetivo se requiere (por ejemplo, hacer clic en un vínculo, un mensaje de apertura) y ninguna indicación aparece en el dispositivo. La instalación es totalmente silencioso e invisible y no puede ser prevenida por el objetivo. Esta es la singularidad NSO, que distingue significativamente la solución Pegasus de cualquier otra solución disponible en el mercado.

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones Reservadas o Confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años (12)
Autorevisión del Estado de la Unidad Administrativa	

PLAZO DE CUMPLIMIENTO.

PLAN DE DESPLIEGUE DE "PEGASUS"	NOVIEMBRE					DICIEMBRE				
	DÍAS/SEMANA	1 AL 2	3 AL 9	10 AL 16	17 AL 23	24 AL 30	1 AL 7	8 AL 14	15 AL 21	22 AL 31
FASE 1 PREOPERATIVOS		Adquisición de equipamiento	Integración de sistemas							
FASE 2 IMPLEMENTACIÓN										
FASE 3 ENTRENAMIENTO Y FINALIZACIÓN							Proceso de transición de dispositivo			

Fase 1 – Preparaciones:

- Se definen los requisitos para un procedimiento de prueba de aceptación (ATP) junto con el cliente. **(ATP req)**
- Adquisición de hardware y software y personalización para responder a las necesidades y requerimientos del cliente. **(Adquisición de equipamiento)**
- Cuando sea necesario, el sistema Pegasus está integrado con los sistemas e infraestructuras locales. **(Integración de sistemas)**
- Adaptaciones del sistema a las redes móviles locales. **(Ajuste de LAN)**

Fase 2- Implementación

- Pruebas de Sistema
- Instalación de hardware **(Entrega de Centro de Control y Comando)**
- Adaptaciones del sistema para versiones de firmware del dispositivo local **(Proceso de transferencia de dispositivo)**



Fecha de la clasificación	México, D.F. a 16 de octubre de 2024
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o parafiscalizadas	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Poderes de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, Incisos a) y c) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 fracción JOO de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Desde 22 años (20)
Ámbito del Titular de la Unidad Administrativa	

Fase 3 – Formación y Terminación

- Simulación y detallado sistema de entrenamiento, situaciones de la vida real practicando (Entrenamiento del sistema)
- Cliente ATP como se define en fase 1 (puesta en marcha ATP)

“LA PROCURADURÍA” proporcionará a “EL PROVEEDOR” a la firma del presente contrato un espacio en sus instalaciones el contara contará con las siguientes características:

- 2 sistemas de aire acondicionado (18° C) regulados de manera independiente.
- 6 tomas eléctricas (20A) por rack.
- 2 enlaces de ATM simétrico de ISP diferente. Cada enlace con 10 direcciones IP estáticas (deben ser dos diferentes proveedores):
- ISP #1: Fibra óptica basada en red (20 MB dedicado)
- ISP #2: Ethernet categoría-7 basado en cable. (20 MB dedicado)
- 1 enlace simétrico.
- ISP #3: Fibra óptica basada en red (200 MB no dedicados)
- 2 conexiones E1 PRI, cada una conteniendo 10 extensiones (deben ser dos diferentes proveedores)
- Corriente regulada con tierra física para la sala y site.
- 1 UPS de 30 KVA para el site.
- Lámparas de emergencia para sala y site.
- Alarma contra incendios.
- Salida de emergencia con señalización.

Una vez hecho lo anterior, “EL PROVEEDOR” proporcionará todo el equipo y mobiliario necesario para óptimo funcionamiento del “EL BIEN” sin costo alguno para “LA PROCURADURÍA”, así como en caso de requerir algún tipo de adecuación en el espacio que le sea proporcionado deberá de contar con la autorización del “ADMINISTRADOR DEL CONTRATO” y en caso de ser procedente todos los gastos serán cubiertos por “EL PROVEEDOR”.

22



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservado
Partes o Secciones reservadas o no clasificadas	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Didáctico Octavo Fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años* (sic)
Órgano del Poder de la Unidad Administrativa	

ANTICIPO Y SU AMORTIZACIÓN.

La amortización del anticipo se aplicará de conformidad a la tabla siguiente:

DESCRIPCIÓN	PRECIO UNITARIO	PORCENTAJE DEL ANCIPO	AMORTIZACIÓN DEL ANCIPO 100%
SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS 500"	\$ 32'016,000.00 USD	35% DEL PRECIO UNITARIO EQUIVALENTE A LA CANTIDAD DE \$11'205,600.00 USD	\$11'205,600.00 USD

*NOTA: LAS CANTIDADES INCLUYEN EL IMPUESTO AL VALOR AGREGADO

FORMA DE PAGO.

"LA PROCURADURÍA" efectuará los pagos de conformidad a lo siguiente:

PAGOS	PORCENTAJE DEL PAGO
PAGO 1	35% DEL PRECIO UNITARIO EQUIVALENTE A LA CANTIDAD DE \$11'205,600.00 USD UNA VEZ CONCLUIDA LA FASE 2
PAGO 2	30% DEL PRECIO UNITARIO EQUIVALENTE A LA CANTIDAD DE \$9'604,800.00 USD UNA VEZ CONCLUIDA LA FASE 3

Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Prevención del Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental; Artículo Octavo Fracción II y V, fracciones c) y d) y Vigésimo Cuarto Fracción II de los Libros del Código Federal de Procedimientos y Justicia Administrativa; Artículo 149 de la Constitución Política de los Estados Unidos Mexicanos; y el Artículo 149 de la Constitución Política de los Estados Unidos Mexicanos para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Órgano del Titular de la Unidad Administrativa	

COTIZACIÓN EXPEDIDA POR “EL PROVEEDOR” DE FECHA 24 DE OCTUBRE DE 2014.

Introducción

Pegasus es una solución de inteligencia líder en el mundo cibernético que permite la aplicación de la ley y las agencias de inteligencia que remotamente y secretamente extraen inteligencia valiosa desde prácticamente cualquier dispositivo móvil. Esta solución innovadora fue desarrollada por los veteranos de las agencias de inteligencia de élite para proporcionar a los gobiernos con una forma de abordar los nuevos desafíos de interceptación de comunicaciones en batalla cibernética altamente dinámica de hoy. Mediante la captura de nuevos tipos de información desde dispositivos móviles, Pegasus es un desfase tecnológico sustancial que ofrece la más completa y precisa inteligencia para sus operaciones de seguridad.

Desafío de Interceptación de Smartphone

El mercado de las comunicaciones móviles altamente dinámico y creciente - caracterizado por la introducción de nuevos dispositivos, sistemas operativos y aplicaciones prácticamente a diario – exige un replanteamiento del paradigma tradicional de la inteligencia. Estos cambios en el paisaje de comunicaciones plantean verdaderos desafíos y obstáculos que deben ser superados por las organizaciones de inteligencia y policiales en todo el mundo:

- Cifrado: Amplia utilización de dispositivos encriptados y aplicaciones para transmitir mensajes
- Abundancia de aplicaciones de comunicación: caótico mercado de aplicaciones sofisticadas, más de las cuales son basadas en IP y usar protocolos propietarios.
- Objetivo fuera interceptación dominio: Comunicaciones objetivos son a menudo fuera del dominio de interceptación de la organización u otra manera inaccesibles (por ejemplo, los objetivos son itinerantes, cara a cara reuniones, uso de redes privadas, etc.)
- Enmascaramiento: Uso de diferentes identidades virtuales que son casi imposibles de reemplazo de SIM.
- Seguimiento y Rastreo: Reemplazo de tarjetas SIM para evitar cualquier tipo de extracción de datos.
- Interceptación Frecuente: La mayoría de la información no se envían a través de la red o compartida con otros partidos y sólo está disponible para el usuario final dispositivo.
- Compleja y Costosa Implementación: Como las comunicaciones se convierten cada vez más complejas, son necesarios más interfaces de red. Configurar estas interfaces con los proveedores de servicio es un proceso largo y costoso y requiere de regulación y normalización.



*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 Fracciones I, IV y V y 14 Fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental; Llave de Seguridad Octavo Sección II y V, Incisos c) y d) y Vigésimo Cuarto Artículo II de los Lineamientos Generales para la clasificación y desclasificación de la Información de las dependencias y entidades de la Administración Pública Federal.
Ley específicas	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (12a)
Rúbrica del Titular de la Unidad Administrativa	

Soluciones estándar de interceptación no son suficientes

Hasta que se abordan los desafíos mencionados y objetivos resueltos, criminales y terroristas son probablemente es "seguro" de sistemas estándar y el legado de interceptación, lo que significa que se está perdiendo valiosa inteligencia. Estas soluciones estándar (descritas en las secciones a continuación) entregan sólo parcial inteligencia, dejando a las organizaciones con boquetes de inteligencia substancial.

Intercepción Pasiva

Intercepción pasiva requiere muy profundas y estrecha relaciones con proveedores de servicios locales (celulares, proveedores de Internet y PSTN) y tradicionalmente ha permitido para un seguimiento adecuado de los mensajes de texto y llamadas de voz. Sin embargo, la comunicación más contemporánea se compone de tráfico basadas en IP, que es extremadamente difícil de controlar con interceptación pasiva debido a su uso de cifrado y protocolos propietarios.

Aun cuando este tráfico es interceptado, típicamente lleva cantidades masivas de datos técnicos que no están relacionados con el contenido real y los metadatos se comunican. No sólo tiene este resultado en analistas frustrados y tiempo perdido en circular a través de datos irrelevantes, también proporciona una reproducción parcial (la mejor) de las comunicaciones del objetivo. Además, el número de interfaces requeridas para cubrir los prestadores de servicios pertinentes amplía el círculo de entidades expuestas a información sensible y aumenta la posibilidad de fuga.

Intercepción Táctica GSM

Soluciones tácticas de interceptación GSM monitorizan de manera efectiva las llamadas de voz y mensajes de texto en las redes GSM. Cuando avanzadas tecnologías celulares son desplegados (Redes 3G y LTE), estas soluciones se vuelven menos eficientes. En tales casos, es necesario rebajar violentamente el objetivo de una red basada en GSM, que afecta notablemente la experiencia del usuario y la funcionalidad

Estas soluciones también requieren de un equipo táctico bien entrenado y un campo situado cerca del objetivo monitoreado. Así, en la mayoría de los casos donde se desconoce la ubicación de destino, estas soluciones convertidas en irrelevantes. En otros casos, colocando un equipo táctico cerca del objetivo puede plantear grave riesgo al equipo y a la operación de inteligencia entera.





PGR
PROCURADURÍA GENERAL
DE LA REPÚBLICA

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Artículo Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la Información de las dependencias y entes de la Administración Pública Federal.
Ley especial	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 72 años* (sic)
Política del Titular de la Unidad Administrativa	

Software Malicioso (Malware)

Malware presumiblemente proporciona acceso al dispositivo móvil del objetivo. Sin embargo, no es completamente transparente y requiere la implicación del objetivo para ser instalado en sus dispositivos. Este tipo de compromiso generalmente toma la forma de múltiples confirmaciones y aprobaciones antes de que el malware sea funcional. La mayoría de los blancos es poco probable que se deje engañar para que coopere con malware debido a su alto nivel de sensibilidad para la privacidad en sus comunicaciones.

Además, tal malware es probable ser vulnerable a la mayoría de software anti-spyware y antivirus disponible comercialmente. Como tal, dejan rastros y son fácilmente detectados en el dispositivo.

Inteligencia Cibernética para el Mundo Móvil

Pegasus es una solución de inteligencia líder en el mundo cibernético que permite la aplicación de la ley y las agencias de inteligencia que remotamente y secretamente extraer inteligencia valiosa desde prácticamente cualquier dispositivo móvil. Esta solución innovadora fue desarrollada por los expertos de las agencias de inteligencia de élite para proporcionar a los gobiernos con una forma de abordar los nuevos desafíos de interceptación de comunicaciones en batalla cibernética altamente dinámica de hoy.

Mediante la captura de nuevos tipos de información desde dispositivos móviles, Pegasus puentes un desfase tecnológico sustancial para ofrecer la más completa y precisa inteligencia para sus operaciones de seguridad. Esta solución es capaz de penetrar los smartphones más populares del mercado basados en sistemas operativos BlackBerry, Android, iOS y Symbian.

Pegasus silenciosamente implementa software invisible ("agente") en el dispositivo de destino. Este agente luego extrae y transmite correctamente los datos recogidos para su análisis. Instalación se realiza de forma remota (OTA), no requiere ninguna acción de o compromiso con el objetivo y no deja ningún rastro alguno en el dispositivo.

Beneficios de Pegasus

Organizaciones que desplegar Pegasus son capaces de superar los retos mencionados para lograr la recolección de inteligencia móvil incomparable:

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Adscripción del Titular de la Unidad Administrativa	

Acceso ilimitado a los dispositivos móviles del objetivo: Remotamente y secretamente recopilar información sobre de su objetivo relaciones, ubicación, llamadas telefónicas, planes y actividades – cuando y donde son.

Interceptar llamadas: Seguimiento transparente de voz y llamadas VoIP en lagunas de inteligencia en tiempo real.

- **Puente:** Recoger únicos y nuevos tipos de información (ej. Contactos, archivos, vigilancia ambiental, contraseñas, etc...) para ofrecer la más completo y preciso inteligencia.
- **Mango codificado contenido y dispositivos:** Superar la encriptación, SSL, protocolos propietarios y cualquier obstáculo presentado por el monitoreo de aplicaciones complejas comunicaciones mundial.
- **Monitorear una multitud de aplicaciones:** Incluyendo objetivos como: Skype, WhatsApp, Viber, Facebook y BlackBerry Messenger (BBM).
- **Seguimiento de objetivos:** Obtener información utilizando independencia GPS
- **Servicio proveedor de posicionamiento preciso:** No cooperación con la red móvil local los operadores (MNO) es necesario.
- **Descubrir identidades virtuales:** Monitorear constantemente el dispositivo sin preocuparse de conmutación frecuente de identidades virtuales y reemplazo de tarjetas SIM.
- **Evite riesgos innecesarios:** Eliminar la necesidad de proximidad física con el objetivo o el dispositivo en cualquier fase.

Tecnología Destacada

La solución de Pegasus utiliza tecnología de punta especialmente desarrollada por veteranos de inteligencia y policiales. Ofrece un rico conjunto de características avanzadas y las capacidades de inteligencia sofisticada colección no están disponibles en las soluciones estándar de interceptación:

- Penetra en Android, BlackBerry, iOS y dispositivos basados en Symbian
- Acceso a dispositivos protegidos por contraseña
- Totalmente transparente para el objetivo
- No deja huella en el dispositivo
- Mínima batería, memoria y datos consumo
- Autodestrucción en caso de exposición riesgo
- Recupera cualquier archivo desde el dispositivo para análisis más profundo

Arquitectura de Alto Nivel

El sistema Pegasus está diseñado en capas. Cada capa tiene la responsabilidad de formar juntos una solución de análisis y recolección de inteligencia cibernética integral.

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 54 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Deciso Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entes de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (12)
Rubros del Título de la Unidad Administrativa	

Las capas principales y bloques de construcción de los sistemas son:

- Instalaciones: Capa de la instalación está a cargo de la emisión de las nuevas instalaciones de agente, actualizar y desinstalar agentes existentes.
- Recolección de datos: Capa de la recopilación de datos está a cargo de recoger los datos desde el dispositivo instalado. Pegasus ofrece inteligencia integral y completa mediante el empleo de métodos de recolección de cuatro
- Extracción de datos: Extracción de los datos todo que existe en el dispositivo sobre la instalación del agente
- Vigilancia pasiva: Nuevos datos de llegada al dispositivo
- Colección Monitor Activo: Activar la cámara, micrófono, GPS y otros elementos para recopilar datos en tiempo real
- Colección basada en eventos: Definir escenarios que activa automáticamente datos específicos colección
- Transmisión de datos: La capa de transmisión de datos es la encargada de transmitir los datos a los servidores de comando y control, utilizando la forma más eficiente y segura.
- Análisis de la presentación: El componente de presentación análisis es una interfaz de usuario que se encarga de presentar los datos recogidos a los operadores y analistas, convirtiendo los datos de inteligencia. Esto se hace mediante los siguientes módulos:
- Monitoreo en tiempo real: Presenta los datos recogidos en tiempo real de específico o varios objetivos. Este módulo es muy importante cuando se trata de objetivos sensibles o durante las actividades operacionales, donde cada pieza de información que llega es crucial para la toma de decisiones.
- Análisis offline: Avanzado mecanismo de consultas que permite a los analistas consultar y recuperar cualquier pieza de información que se recopila. El mecanismo avanzado proporciona herramientas para encontrar información y conexiones ocultas.
- Análisis basado en geolocalización: presenta los datos recogidos en un mapa y conducta consultas basadas en geo.
- Administración: es el componente de administración encargado de gestionar el permiso de todo el sistema, seguridad y salud: contactos de extractos mensajes, correos electrónicos, fotos, archivos, ubicaciones, contraseñas, lista de procesos y más
- Permiso: el mecanismo de permisos permite al administrador del sistema gestionar los distintos usuarios del sistema. Proporcionar cada uno de ellos el nivel correcto acceso sólo a los datos que se les permite. Esto permite para definir los grupos de la organización que manejan sólo uno o más temas y otros grupos que maneja diferentes temas.
- Seguridad: El módulo de seguridad monitorea el nivel de seguridad del sistema, asegurándose de que los datos recogidos se insertan a la base de datos de sistema limpio y seguro para su futura revisión.
- Salud: El componente de salud de la solución de Pegasus monitorear el estado de todos los componentes asegurándose de que todo está funcionando sin problemas. Monitorea la comunicación entre las diferentes partes, el rendimiento del sistema, la disponibilidad de almacenamiento de información y alertas si algo falla.

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamientos Generales Fracción II y V, Incisos c) y d) y Vigésimo Cuarto Artículo II de los Lineamientos Generales para la clasificación y desclasificación de la Información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXII de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Rúbrica del Titular de la Unidad Administrativa	

- **Mensaje de ingeniería Social mejorado (ESEM):** En casos donde el método de instalación OTA es inaplicable¹, el operador del sistema puede elegir enviar un mensaje de texto normal (SMS) o un correo electrónico, atrayendo el objetivo para abrirlo. Solo clic, planificada o no intencional, en el enlace se traducirá en instalación del agente oculto. La instalación está totalmente oculta y aunque el objetivo hacer clic en el enlace no serán conscientes de que software está siendo instalado en su dispositivo.

Las posibilidades de que el objetivo se haga clic en el enlace son totalmente dependientes en el nivel de contenido credibilidad. La solución de Pegasus ofrece una amplia gama de herramientas para componer un mensaje inocente y diseñado para atraer la meta para abrir el mensaje.

Nota: Ambos métodos OTA y ESEM requieren solamente un número de teléfono o una dirección de correo electrónico que se utiliza por el objetivo. Nada más se necesita para lograr una instalación exitosa del agente Pegasus en el dispositivo

Cerca del objetivo (Rango limitado):

- **Elemento táctico de red:** agente de la Pegasus puede ser inyectado en silencio una vez que el número se adquiere mediante el elemento de red táctica como **Base estación transmisora (BTS)**. El Pegasus la solución aprovecha las capacidades de estas herramientas tácticas para llevar a cabo una inyección remota e instalación del agente. Tomando una posición en el área de la blanco es, en la mayoría de los casos, suficientes para llevar a cabo la adquisición de número de teléfono. Una vez que el número está disponible, la instalación se realiza remotamente.
- **Física:** cuando el acceso físico al dispositivo es una opción, el agente de Pegasus puede ser manualmente inyectado e instalado en menos de cinco minutos. Después de la instalación del agente, extracción de datos y monitoreo de datos futuros se realiza remotamente, ofreciendo las mismas características de cualquier otro método de instalación.

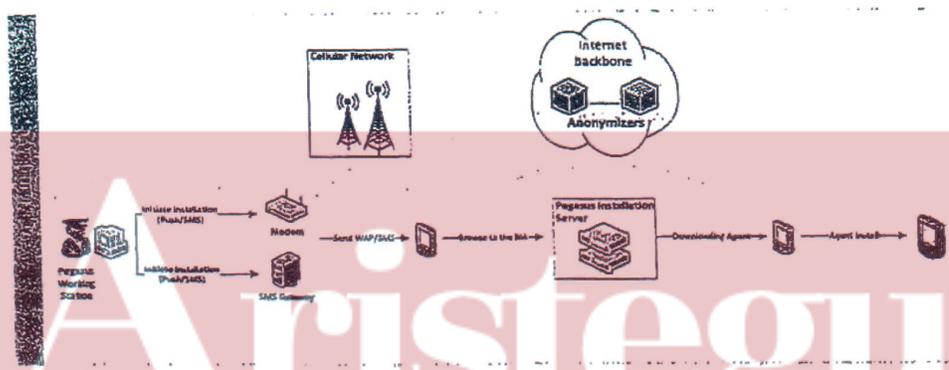
Nota: Generalmente se utilizan instalaciones Tácticas y físicas donde ningún número de teléfono de destino o dirección de correo electrónico están disponibles.

Fecha de la clasificación	México, D.F. a 18 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	53 fracciones I, IV y V y 14 fracción I de la Ley de Fomento de Transparencia y Acceso a la Información Pública Gubernamental, Livramento Dóctro Octava fracción II y V, incisos a) y d) y Vigésima Cuarta fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción I de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Reserva "2 años" (sic)
Alcance del Titulo de la Unidad Administrativa	

Flujo de instalación del agente

Flujo de instalación del agente remoto se muestra en la Figura 2.

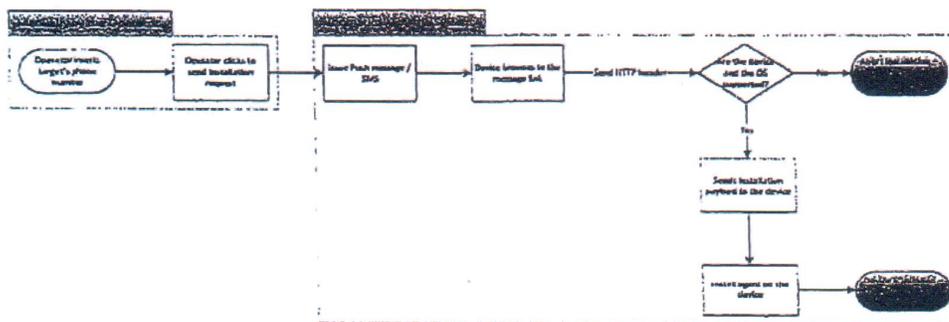
Figura 2: Flujo de instalación del agente



Para iniciar una nueva instalación, el operador del sistema Pegasus sólo debe introducir el número de teléfono de destino. El resto se realiza automáticamente por el sistema, resultando en la mayoría de los casos con un agente instalado en el dispositivo de destino.

Iniciación de configuración del agente se muestra en la Figura 3.

Figura 3: El Agente de inicio de instalación



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Acceso a la Información Pública Gubernamental, Lineamiento Decimo Octavo fracción I y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años* (sic)
Ámbito del Titular de la Unidad Administrativa	

Sistemas y Dispositivos Operativos Compatibles

Sistema Operativo (SO)	Versión OS	Dispositivo	Comentarios
Android	2.1 - 4.2	Samsung Galaxy series Sony Ericsson Xperia series Otros	El apoyo se basa en las versiones locales de firmware, cosa que se debe definir con el cliente.
iOS	4.x - 6.1.4	iPhone 4 iPhone 4S iPhone 5	
BlackBerry	5.0 - 7.1	Curve (8520, 9300, 9350, 9360) Bold (9000, 9700, 9780, 9790, 9900, 9930) Torch (9800, 9810, 9850, 9860) Pearl (9100)	
Symbian	Versión S60 OS9 3rd edition FP1, FP2, 5th edition and Symbian^3	Variedad de dispositivos	El apoyo se basa en las versiones locales de firmware, cosa que se debe definir con el cliente.

Nota: Los dispositivos basados en Android a menudo se añaden a la lista de admitidos. Una lista actualizada puede ser enviada a petición del cliente.

Falló la instalación la instalación:

A veces puede fallar debido a las razones siguientes:

1. **Dispositivo no compatible:** el dispositivo de destino no es compatible con el sistema (que aparece más arriba).
2. **Sin soporte OS:** el sistema operativo del dispositivo de destino no es compatible con el sistema
3. **Sin soporte de navegador:** el navegador por defecto del dispositivo previamente fue reemplazado por el objetivo. Instalación de los navegadores distinta de la predeterminada del dispositivo (y también dispositivos basados en Chrome para Android) no es compatible con el sistema.

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	12 fracciones I, IV y V y 14 fracción I de la Ley de Fideicomiso de Transparencia y Acceso a la Información Pública Gubernamental, Artículo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública
Periodo de reserva	Hasta 12 años (sic)
Órgano del Titular de la Unidad Administrativa	

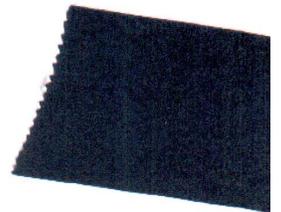
En cualquiera de los casos antes mencionados, si el operador inicia una instalación remota a un dispositivo no compatible, sistema operativo o navegador, la inyección se producirá un error y se aborta la instalación. En estos casos el proceso haya terminado con un navegador abierto en el dispositivo de destino apuntando y mostrando la página URL que fue definida por el operador antes de la instalación. El dispositivo, el sistema operativo y el navegador se identifican mediante el sistema mediante su agente de usuario HTTP. Si por algún motivo que el agente de usuario fue manipulado por el blanco, el sistema podría no identificar correctamente el dispositivo y el sistema operativo y proporcionan la carga instalación incorrecta. En tal caso, la inyección se producirá un error y se aborta la instalación, mostrando nuevamente la página URL antes mencionada.

Recolección de Datos

Tras la instalación del agente exitoso, una amplia gama de datos se controla y recopilada desde el dispositivo:

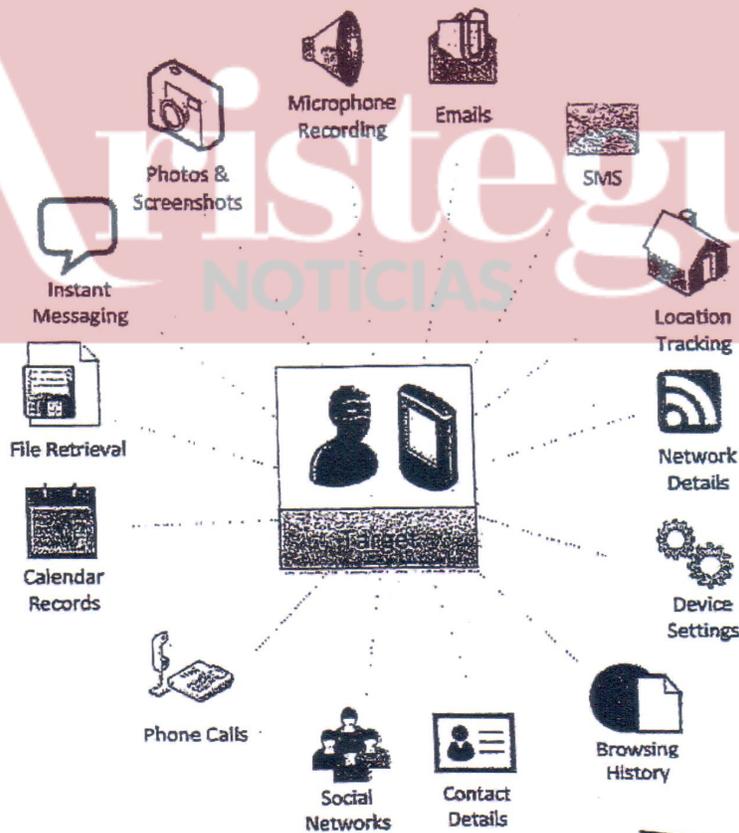
- **Textual:** Información Textual incluye mensajes de texto (SMS), correos electrónicos, registros de calendario, llamado historia, mensajería instantánea, lista de contactos, viendo la historia y mucho más. Información textual suele ser estructurado y pequeño de tamaño, por lo tanto más fácil de transmitir y analizar.
- **Audio:** Audio información incluye llamadas interceptadas, sonidos ambientales (grabación de micrófono) y otros archivos de audio grabados.
- **Visual:** información Visual incluye cámaras instantáneas, recuperación de fotos y capturas de pantalla.
- **Archivos:** cada dispositivo móvil contiene cientos de archivos, algunos osos inteligencia invaluable, tales como bases de datos, documentos, videos y más.
- **Ubicación:** seguimiento de la ubicación del dispositivo (Cell-ID y GPS) continúa

La variedad de los datos que son recogidos por el sistema Pegasus se muestra en la Figura 4.



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I en la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, incisos e) y f) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entes de la Administración Pública Federal.
Ley específica	Artículo 48 Fracción ICG de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años (sic)
Rollos del Titular de la Unidad Administrativa	

Figura 4: Los datos Recopilados.



La recolección de datos se divide en tres niveles:

- Extracción Inicial
- Monitoreo Pasivo
- Recolección de Datos Activa



*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, incisos a) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública, Federal.
Ley específica	Artículo 40 Fracción III de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (12)
Ritmos del Titular de la Unidad Administrativa	

Extracción Inicial de Datos

Una vez que el agente es inyectado con éxito e instalado en el dispositivo, los siguientes datos que residen y que existen en el dispositivo pueden extraerse y enviados al centro de mando y control

- Registro de SMS
- Detalle de Contactos
- Historial de Llamadas (registro)
- Calendario de registros
- Mensaje de Correo Electrónico
- Mensajería instantánea
- Historial de Navegación

A diferencia de otras soluciones de colección de inteligencia que proporcionan sólo futuro monitoreo de comunicaciones parciales, Pegasus permite la extracción de todos los datos existentes en el dispositivo. Como resultado la organización goza de acceso a datos históricos sobre el objetivo, que asiste en la construcción de una imagen completa y precisa de la inteligencia.

Nota: La extracción de datos inicial es una opción y no una necesidad. Si la organización no está permitida acceder a los datos históricos del blanco, esta opción puede desactivarse y sólo nuevos datos de llegada serán monitorizados por el agente

Monitoreo Pasivo

Desde el punto del que agente fue instalado con éxito mantiene el dispositivo de monitoreo y recupera cualquier nuevo registro que esté disponible en tiempo real (o en condición específica si configura diferentemente). Debajo está la lista completa de datos que es supervisado por el agente:

- Registros de SMS
- Detalles de Contactos
- Historial de llamadas (Registro)
- Calendario de Registros
- Mensajes de correo electrónico
- Mensajería instantánea
- Historial de navegación
- Ubicación de Seguimiento (Cell-ID basada)

*Fecha de la clasificación	México D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Céfiro Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entes de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rolario del Titular de la Unidad Administrativa	

Recopilación activa

Además de la vigilancia pasiva, Al exitoso agente de instalar el amplio conjunto de colección esté disponible. Colección activa se refiere a activar las solicitudes enviadas por los operadores para recoger información específica del unscrew instalado. Este conjunto de características son llamada activa, llevan su cum colección implícita A solicitud del explotador. Activo colección permite al operador realizar las acciones en tiempo real sobre la recuperación de dispositivos de destino información única del dispositivo y de los alrededores de la meta, que incluye:

- Rastreo de ubicación (basado en el GPS)
- Las llamadas de voz interceptación
- Recuperación de archivos
- Grabación de sonido ambiental (Grabación de micrófono)
- Seguimiento de fotos
- Captura de Pantalla

Colección activa distingue a Pegasus de cualquier otra solución de colección de inteligencia, como el operador controla la información que se recopila. En lugar de sólo esperando información llegar, esperando que esta es la información que buscas, el operador activamente recupera información importante desde el dispositivo, recibiendo la información exacta que estaba buscando.

Descripción de los datos recogidos.

Los diferentes tipos de datos disponibles para la extracción, vigilancia pasiva y activa colección con sus respectivas características se enumeran en la tabla 1.

Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley de Protección de Datos Personales y Vigilancia Ciudadana fracción II y V, incisos d) y e) y Vigilancia Ciudadana fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción IXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Política del Titular de la Unidad Administrativa	

Tipo de Aplicación	Descripción de Características	Extracción de Datos	Colección Pasivo /Activo
Grabación de sonido ambiental (grabación del micrófono)	<p>El usuario puede solicitar para encender el micrófono del dispositivo y escuchar en tiempo real a los sonidos del entorno. Los sonidos del entorno se registran y pueden ser analizados y reproducidos en una etapa posterior.</p> <p>Al encender el micrófono se basa en una llamada silenciosa en el dispositivo desde el servidor (PBX). Se autorizará dicha llamada sólo después de que el agente de seguridad de que el dispositivo está en modo de reposo (el dispositivo no está en uso activo y la pantalla está apagada).</p> <p>Ninguna acción de la meta que se enciende la pantalla dará lugar a la llamada inmediata de colgar y de cese de la captura de los sonidos del entorno. No hay indicación de la grabación o la llamada silenciosa entrante aparece en el dispositivo, en cualquier punto.</p> <p>La calidad de la grabación depende de la sensibilidad del micrófono del dispositivo, el ruido circundante y el modelo del dispositivo. Esta sensibilidad varía entre los diferentes modelos de teléfonos móviles y es fijado por el fabricante del teléfono. Por lo general, el contenido de una conversación celebrada a pocos metros al lado del dispositivo puede ser escuchado.</p>	N/A	*
SMS	El agente extrae y monitorea todos los mensajes de texto entrantes y salientes (SMS).	*	*
Intercepción de Llamada (Grabación de llamada) - Solo Android	<p>El usuario puede pedir grabar llamadas entrantes y salientes del dispositivo del objetivo.</p> <p>Las llamadas son grabadas localmente en el dispositivo y después enviadas al servidor hasta que se complete.</p>	N/A	*
Email: 1. Aplicación de Email en todas las plataformas. 2. Aplicaciones Gmail en Android	Agente extrae y supervisa todos los correos electrónicos que se encuentran en el dispositivo. La aplicación de correo electrónico principal (acción) en el dispositivo se controla, por lo tanto, todas las cuentas que se definen no son monitoreados (por ejemplo, el intercambio, gmail, etc.) Para dispositivos basados en Android tanto en la aplicación de correo electrónico principal y la aplicación gmail son monitoreadas.	*	*
Recuperación de archivos	A petición del usuario una lista completa de los archivos y carpetas se extrae del dispositivo (memoria interna y la tarjeta SD). Cuando el operador ve un archivo de interés que puede solicitar de inmediato para recuperarlo.	N/A	*



PGR

PROCURADURÍA GENERAL
DE LA REPÚBLICA

Fecha de la clasificación	México, D.F., a 10 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Libramiento Decimo Octavo fracción II y VI, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción JOO de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Órgano del Titular de la Unidad Administrativa	

Toma de la foto	Al usuario de petición instantánea utilizando la cámara frontal y trasera se toman desde el dispositivo y se envían a los servidores. Se toman las instantáneas después de que el agente de seguridad de que el dispositivo está en modo inactivo. Durante la foto teniendo la indicación aparece en el dispositivo y el flash no se utiliza nunca. La calidad de la foto puede ser elegida por el operador para reducir el uso de los datos y la transmisión rápida de fotos. Dado que el flash no se utiliza y el teléfono podría estar en movimiento o las habitaciones interiores con poca luz, las fotos son a veces fuera de foco.	N/A	*
Captura de Pantalla	A petición del usuario se toma una captura de pantalla y se envía a los servidores de Pegasus. Las capturas de pantalla de dispositivos pueden proporcionar información sobre las aplicaciones utilizadas por el objetivo, imagen de fondo utilizada y la información más íntima sobre el objetivo.	N/A	*
Historial de navegación	El agente extrae y monitorea el historial de los sitios web explorados desde el navegador predeterminado del dispositivo.	*	*
Favoritos de navegación	Los agentes extraen y monitorean los sitios web favoritos guardados en el navegador predeterminado del dispositivo.	*	*
Historial de llamadas	El agente extrae el historial de todas las llamadas entrantes / salientes realizadas desde / hacia el dispositivo. Los datos incluyen la persona que llama y los números llamados y la duración de la llamada. Intentos que no resultaron con una conversación de llamada mostrará la duración de 0 (cero) segundos.	*	*
Historial de llamadas	El agente extrae el historial de todas las llamadas entrantes / salientes realizadas desde / hacia el dispositivo. Los datos incluyen la persona que llama y los números llamados y la duración de la llamada. Intentos que no resultaron con una conversación de llamada mostrará la duración de 0 (cero) segundos.	*	*



PGR

PROCURADURÍA GENERAL
DE LA REPÚBLICA

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Intervención para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Registro del Titular de la Unidad Administrativa	

Los datos antes mencionados son los datos posibles que pueden ser recolectados por un agente. El agente recopilará los datos que están disponibles en el dispositivo y aplicables. Si no existe uno o más de las aplicaciones mencionadas o quitado el dispositivo, el agente funcionará de la misma manera. Recolectarán los datos del resto de los servicios y aplicaciones que están en uso en el dispositivo. Además, todos los datos recogidos desde la aplicación quitado todavía se guardarán en los servidores o en el agente, si no era todavía transmiten a los servidores.

Además, los datos antes mencionados que son recogidos por el agente cubren las aplicaciones más populares utilizadas en el mundo. Puesto que la popularidad de las aplicaciones varía de país a país, que entiende la extracción de datos y monitoreo de aplicaciones será necesarios tiempo evoluciona y nuevas aplicaciones son adoptadas por objetivos. Cuando tal requisito se levanta, podemos fácilmente extraer datos importantes de prácticamente cualquier aplicación basada en la demanda del cliente y lanzarlo como una nueva versión que estará disponible para el cliente.

Colección de Buffer

El agente instalado monitorea los datos desde el dispositivo y la transmite a los servidores. Si la transmisión no es posible³ el agente recogerá la nueva información disponible y la transmite cuando se disponga de conexión. Los datos recogidos se almacenan en un búfer oculto y cifrado. Este buffer está listo para llegar a no más del 5% del espacio libre disponible en el dispositivo. Por ejemplo, si el dispositivo monitoreado tiene 1GB de espacio libre, el buffer puede almacenar hasta 50MB. En caso de que el buffer ha llegado a su límite, los datos más antiguos se borran y se almacenan los datos nuevos (FIFO). Una vez que se ha transmitido los datos, el contenido del búfer es totalmente eliminado.

Transmisión de Datos

De forma predeterminada, los datos recogidos (extracción de los datos iniciales, vigilancia pasiva y activa colección) son enviados hacia el centro de comando y control en tiempo real. Los datos se envían a través de canales de datos, donde Wi-Fi es la conexión preferida para utilizar cuando está disponible. En otros casos se transmiten datos mediante canales de datos móviles (GPRS, 3G y LTE). Extra pensaba poner en métodos de compresión y centrarse en la transmisión de contenido textual siempre que sea posible. Las huellas de datos son muy pequeñas y suelen tener sólo unos cientos de bytes. Esto es para asegurarse de que los datos recogidos se transmiten fácilmente, asegurando un impacto mínimo en el dispositivo y en el plan de datos móviles de blanco.

Si no existen canales de datos, el agente de recopilar la información del dispositivo y guárdela en un búfer dedicado, como se explica en la sección de recopilación de datos.

Transmisión de datos es cesada automáticamente en los siguientes escenarios:



*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservado
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 Sección I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la Información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rebaja del Nivel de la Unidad Administrativa	

Seguridad de la Transmisión de Datos

Todas las conexiones entre los agentes y los servidores están cifradas con algoritmos fuertes y mutuamente se autentican. Cifrado de datos es probablemente el tema más instando a, cuidado adicional fue dado para asegurar la memoria, pila y datos mínimos son consumidos dentro de los requerimientos de los agentes. Esto es para asegurarse de que no se crían preocupación por el destino. Es casi imposible detectar a un agente operativo por el objetivo. El agente Pegasus está instalado a nivel del núcleo del dispositivo, bien ocultado y es imposible de encontrar por el software antivirus y anti-espía.

Los datos transmitidos están encriptados con cifrado simétrico AES de 128 bits.

Red de Transmisión Anónima de Pegasus

Agente transparencia y seguridad de la fuente son los principios rectores de la solución de Pegasus. Para asegurar que se remontan a la entidad explotadora es imposible, el Pegasus anonimizar transmisión Network (red), una red de Anonimizadores se despliega para servir a cada cliente. Los nodos de la red se distribuyen en diferentes lugares alrededor del mundo, permitiendo a agente conexiones ser redirigido a través de diferentes caminos antes de llegar a los servidores de Pegasus. Esto asegura que las identidades de ambas partes comunicantes son altamente oscurecidas.

Presentación de Datos y Análisis.

Recopilación de datos exitoso de cientos de objetivos y dispositivos genera enormes cantidades de datos para análisis, presentación y visualización. El sistema proporciona un conjunto de herramientas operativas para ayudar a la organización a transformar datos de inteligencia. Esto es para ver, ordenar, filtrar, consultar y analizar los datos recogidos. Las herramientas incluyen:

- **Análisis Geográfico:** seguimiento de localización en tiempo real e históricos del objetivo, varios objetivos en el mapa
- **Reglas y alertas:** definir reglas para generar alertas a la llegada de los datos importantes
- **Favoritos:** marcar eventos importantes y favoritos para revisión posterior y más profundo análisis
- **Inteligencia de tablero de instrumentos:** Ver destacados y estadísticas de gestión de destino actividades.
- **Entidad de Gestión:** Gestionar objetivos por grupos de interés (por ejemplo, medicamentos, terrorismo, delitos graves, ubicación, etc...)
- **Análisis de la Línea de Tiempo:** revisión y analizar los datos recogidos de una búsqueda avanzada determinado plazo
- **Búsqueda Avanzada:** de conducta de términos, nombres, palabras clave y números para recuperar información específica



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	15 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Decreto Octavo fracciones II y V, incisos a) y d) y Vigésimo Cuarta fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción JOO de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años (sic)
Adscripción del Titular de la Unidad Administrativa	

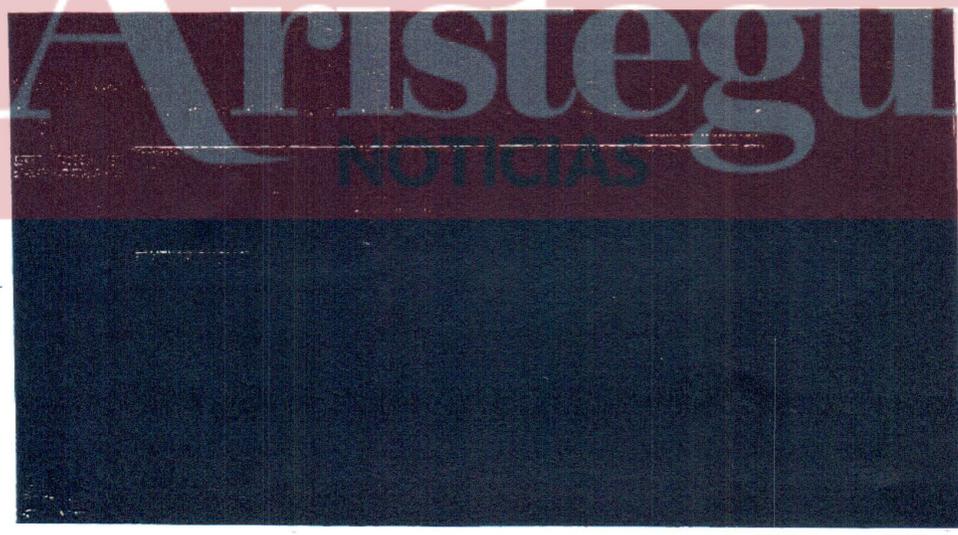
Los datos recogidos es organizados por grupos de interés (por ej., drogas, grupo A, grupo terrorista B, etc.) y cada grupo se compone de objetivos. Cada objetivo se compone de varios dispositivos que algunos agentes han instalados en ellos.

Los datos recogidos se muestran en una interfaz de usuario intuitivo fácil de utilizar y cuando corresponda emula popular visualización de aplicaciones comunes. La intuitiva interfaz de usuario está diseñada para un trabajo cotidiano. Los operadores pueden personalizar fácilmente el sistema ajuste sus métodos de trabajo preferido, definir reglas y alertas para temas específicos de interés.

El operador puede elegir ver los datos recogidos todo de blanco específico o sólo determinado tipo de información como información de ubicación, registro de calendario, correos electrónicos o mensajes instantáneos.

Calendario de Pegasus control pantalla se muestra en la figura 7.

Figura 7: Calendario de Monitoreo

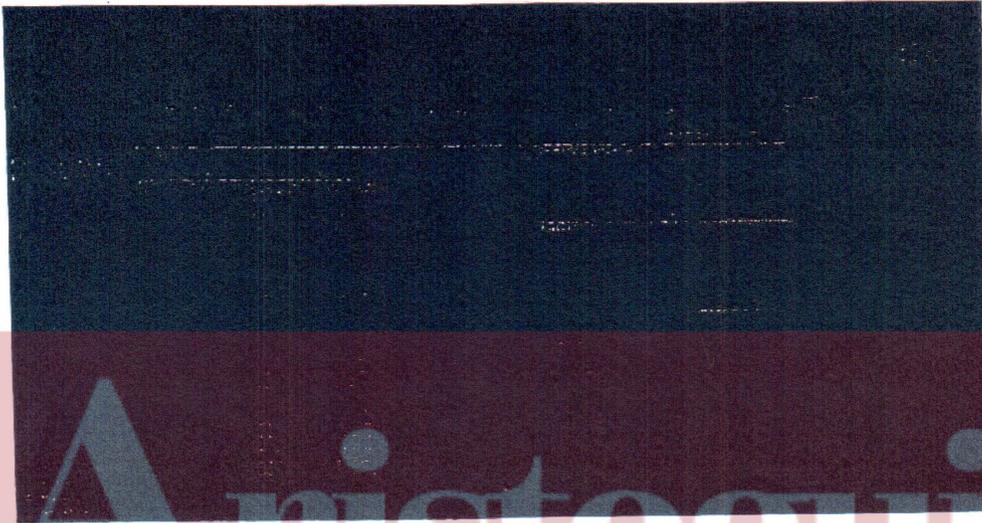


[Handwritten signatures and marks]

Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública (Gubernamental, Lineamiento Decimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción I de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Ámbito del Tránsito de la Unidad Administrativa	

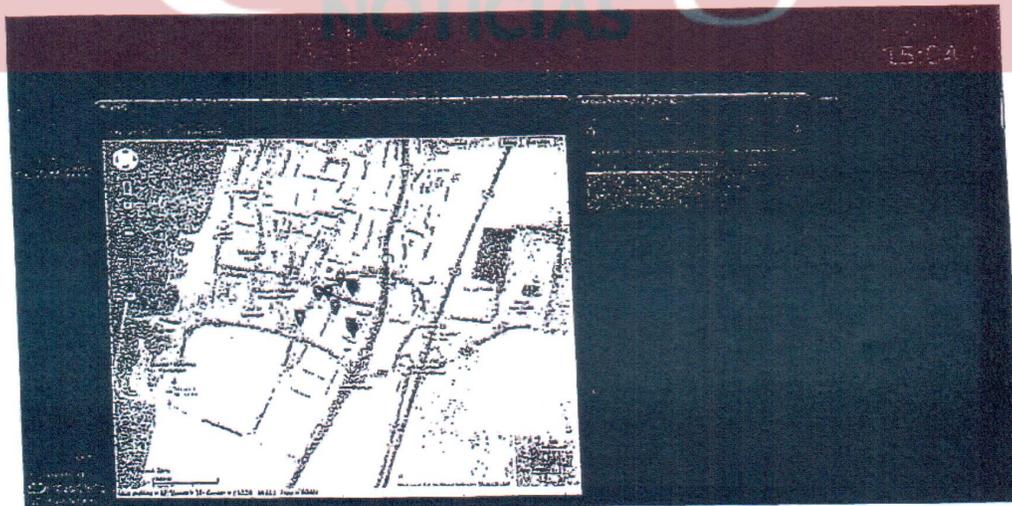
Pantalla intercepción registro de llamadas Pegasus y la llamada se muestra en la Figura 8.

Figura 8: Registro de Llamadas y Llamada Intercepción



Pantalla de seguimiento Pegasus ubicación se muestra en la figura 9.

Figura 9: Ubicación de seguimiento



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Fideicomiso de Transparencia y Acceso a la Información Pública Gubernamental, Decreto Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entes de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años* (sic)
Políticas del Titular de la Unidad Administrativa	

2: Presentación de los datos almacenados

Servicio / Tipo de Aplicación	Datos extraídos	Método de visualización
Mensajería Instantánea: 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	<ul style="list-style-type: none"> Chat de participantes (Nombres y Teléfonos) Contenido de conversación Datos y Tiempo Metadatos adjuntos (sin adjuntos) 	<ul style="list-style-type: none"> Cuadrícula Modo de conversación
Seguimiento de la ubicación	<ul style="list-style-type: none"> Fuente de datos (GPS/CELL-ID) Latitud Longitud Fecha y Hora 	<ul style="list-style-type: none"> Cuadrícula Mapa: <ul style="list-style-type: none"> - Visual en mapa - Ruta completa - Tipo de datos
Calendario	<ul style="list-style-type: none"> Objetivo de reunión Fecha de evento y tiempo de inicio 	<ul style="list-style-type: none"> Cuadrícula Vista mensual del calendario (emula calendario de clientes populares)
Detalles de contacto	<ul style="list-style-type: none"> Valores totales guardados en el total de contactos incluyendo fotos si están disponibles. 	<ul style="list-style-type: none"> Cuadrícula Tarjeta de contacto con detalles completos
Sonido ambiental grabado (grabación de micrófono)	<ul style="list-style-type: none"> Audio grabado Fecha y hora grabada Duración 	<ul style="list-style-type: none"> Cuadrícula Interfaz de reproducción
SMS	<ul style="list-style-type: none"> Dirección (entrante, saliente) Nombre de contacto Número de teléfono Contenido de mensaje Fecha y tiempo 	<ul style="list-style-type: none"> Cuadrícula
Intercepción de llamada	<ul style="list-style-type: none"> Dirección (entrante, saliente) Nombre de contacto Número de teléfono Contenido de mensaje Fecha y tiempo 	<ul style="list-style-type: none"> Cuadrícula Interfaz de reproducción
Email: 1. Aplicación de Email principal en todas las plataformas. 2. Aplicaciones Gmail en Android	<ul style="list-style-type: none"> Desde A CC BCC Tema Carpeta Cuenta Contenido de mensaje Fecha y Hora 	<ul style="list-style-type: none"> Cuadrícula HTML (emula correo de clientes populares)



PGR
 PROCURADURÍA GENERAL
 DE LA REPÚBLICA

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Protección Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales:	Totalmente
Fundamento Legal:	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, el Artículo 17 de la Constitución Política de los Estados Unidos Mexicanos y el Vigésimo Cuarto Artículo de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entes de la Administración Pública Federal.
Ley específica:	Artículo 40 Fracción 200 de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva:	Hasta 12 años (sic)
Fórmula del Titular de la Unidad Administrativa:	

Servicio / Tipo de Aplicación	Datos extraídos	Método de visualización
Recuperación de archivos	<ul style="list-style-type: none"> • Lista de carpeta (árbol) • Lista de archivos (cuadrícula) • Nombre del archivo • Fecha modificada • Tamaño de archivo 	<ul style="list-style-type: none"> • Cuadrícula • Vista de árbol
Toma de fotografía	<ul style="list-style-type: none"> • Fecha de modificación • Tamaño de archivo 	<ul style="list-style-type: none"> • Cuadrícula • Visualización de foto
Captura de pantalla	<ul style="list-style-type: none"> • Fecha y hora • Foto 	<ul style="list-style-type: none"> • Cuadrícula • Visualización de foto
Historial de búsqueda	<ul style="list-style-type: none"> • Fecha y hora • Imagen de captura de pantalla 	<ul style="list-style-type: none"> • Listado
Favoritos de búsqueda	<ul style="list-style-type: none"> • Nombre de sitio web (salvado como el objetivo, usualmente el nombre del sitio web por default) • Dirección URL del sitio web 	<ul style="list-style-type: none"> • Listado
Historial de llamadas (log de llamada)	<ul style="list-style-type: none"> • Dirección • Nombre de contacto • Número de teléfono • Duración • Fecha y hora 	<ul style="list-style-type: none"> • Cuadrícula
Información de dispositivo	<ul style="list-style-type: none"> • Nivel de batería • Tipo de conexión (ejemplo, 3G, WIFI) • MSISDN • IMEI • IMSI • Fabricante del dispositivo • Modelo de dispositivo • Versión de Sistema Operativo • Fecha de instalación • Tiempo de última conversación • País de origen del dispositivo • Servicio de red • Servicio de red en casa 	<ul style="list-style-type: none"> • Panel de control

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Corredor e la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, Inciso a) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	ARTÍCULO 40 Fracción JOO de la Ley que establece en Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años (12)
Rúbrica del Titular de la Unidad Administrativa	

Reglas y Alertas

El módulo de alertas de las reglas de las alertas del sistema al importante evento lleva a cabo. Las reglas deben definirse con antelación y ayudan a los operadores a revisar y tomar acciones en tiempo real, por ejemplo:

- **Geo-cercas:** o acceso zona caliente - alerta cuando objetivo llegar a una localización importante o licencia zona caliente - alerta cuando blanco dejó un lugar determinado alertas de Geo-cerca se basan en un perímetro alrededor de un lugar determinado, donde el operador define el tamaño del perímetro
- **Detección de conexión:**
 - Alerta Cuando se envía un mensaje desde / hasta el número específico
 - Alerta Cuando la llamada telefónica es protagonista desde / hasta el número específico.
- **Detección de contenido:** Alerta Cuando se utiliza la palabra / término / palabra definida en el mensaje codificado

Exportación de datos

El sistema está diseñado como un sistema end-to-end, proporcionando a sus usuarios con herramientas de recopilación y análisis. Sin embargo, entiende que existen requisitos de análisis avanzado datos y capacidades de fusión de otras fuentes, por lo tanto, el sistema permite la exportación de la información recopilada y una perfecta integración con back-end o el análisis de sistemas de terceros disponibles

Mantenimiento del Agente

Una vez que el agente está instalado en un determinado dispositivo, tiene que mantenerse con el fin de apoyar nuevas características y cambiar sus ajustes y configuraciones o a ser desinstalado cuando ya no está proporcionando inteligencia valiosa a la organización.

Actualización del Agente

Cuando se liberan las actualizaciones de los agentes que estén disponibles para instalar. Ahora están listos para la instalación en dispositivos nuevos objetivos o como actualizaciones existentes los agentes instalados en los dispositivos de destino estos nuevos agentes. Estas actualizaciones proporcionan nuevas funcionalidades, fallo de fijación, soporte para nuevos servicios o mejorar los agentes comportamiento global. Dichas actualizaciones son cruciales para mantener al agente funcional y operativa en el progreso sin fin del mundo de la comunicación y especialmente la arena Smartphone.

Existen dos tipos de actualizaciones de agente:



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	15 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y actividades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción IXX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Relativo del Titular de la Unidad Administrativa	

- Actualización opcional: no es obligatorio por el sistema. El usuario decide cuándo, si acaso, para actualizar el agente.
- Actualización obligatoria: de agente es obligatorio por el sistema. El supervisor debe actualizar al agente lo contrario que ninguna nueva información será monitoreada desde el dispositivo.

Actualización a veces requiere una instalación de un nuevo agente y a veces una pequeña actualización del agente existente. En ambos casos el usuario es el único para decidir cuándo realizar la actualización y por lo tanto debe planear esto por consiguiente.

Una vez que el comando de actualización fue enviado por el usuario, el proceso debería tomar sólo unos pocos minutos. El proceso podría tomar más tiempo si el dispositivo está apagado o tiene conexión de datos. En cualquier caso, la actualización se realizará una vez que disponga de una conexión de datos decente.

Configuraciones del Agente

Actualización a veces requiere una instalación de un nuevo agente y agente para ajustar por primera vez durante su instalación. Desde este punto, estos ajustes sirven al agente, pero siempre se pueden cambiar si es necesario. La configuración incluye la dirección IP para la transmisión de los datos recogidos, los comandos de forma son enviados al agente, el tiempo hasta que el agente se desinstala automáticamente si mismo (véase el mecanismo de autodestrucción para más detalles) y mucho más.

Desinstalación del Agente.

Cuando se realiza la operación de inteligencia o en el caso donde el objetivo ya no es con interés a la organización, se puede quitar y desinstalar el componente de software base ("agente") en el centrador de. Desinstalar es rápido, requiere una solicitud de usuario único y no tiene ningún efecto al mínimo en el dispositivo de destino. Los temas de usuario una solicitud para el agente de desinstalación que se envía al dispositivo.

Una vez que el agente se desinstaló desde ciertos dispositivos no deja ningún rastro alguno o indicaciones fue alguna vez existieron 4.

Mientras el agente está en funcionamiento en el dispositivo y existe una conexión entre él y los servidores que puede ser fácilmente y de forma remota desinstalado.

Desinstalar siempre se puede hacer remotamente sin importar lo que fue el método utilizado para la instalación.

Desinstalar físico también es una opción, si es necesario.

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Básico Octavo fracción II y V, Incisos a) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXV de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años* (sic)
Relación del Titular de la Unidad Administrativa	

Sitio del Cliente.

NSO es responsable de implementar y configurar el hardware del Pegasus y software en las instalaciones del cliente, asegurándose de que el sistema está trabajando y funcionando correctamente. A continuación se presentan los principales componentes instalados en el sitio del cliente:

Servidor Web

Que residen en las instalaciones del cliente, los servidores son responsables de lo siguiente:

- Instalación del agente y mantenimiento
- Agente de monitoreo: controlar remotamente, configurar y actualizar agentes instalados
- Transmisión de datos: recibir la recogida datos transmitidos desde los agentes instalados
- Terminales de los operadores

Módulo de Comunicaciones

El módulo de comunicaciones permite la interconectividad y la conexión a internet a los servidores.

Módulo de comunicación celular

El módulo de comunicación celular permite la instalación remota del agente Pegasus al dispositivo de destino utilizando módems celulares o pasarelas SMS.

Módulo de permiso

El módulo de gestión de permisos Pegasus define y controla las características y El contenido disponible permitido para cada usuario en función de su papel, el rango y jerarquía.

Almacenamiento de Datos

Los datos recogidos que se extrajo y vigilados por los agentes se almacenan en un dispositivo de almacenamiento externo. Los datos están bien respaldados y con resiliencia completo y redundancia para prevenir fallas y tiempo de inactividad.

Seguridad de Servidores

Todos los servidores residen dentro de la red del cliente confiable, detrás de las medidas de seguridad que puede implementar así como medidas de seguridad que suministramos específicamente para el sistema.



Fecha de la Clasificación	México, D.F., a 18 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, <u>Lineamiento Didaxo Octavo</u> fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 10 Fracción JCO de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Ámbito del Titular de la Unidad Administrativa	

Hardware

El hardware estándar del sistema está desplegado en varios servidores conectados juntos par de estantes. El equipo se encarga de balanceo de carga avanzada, compresión contenido, administración de conexión, cifrado, enrutamiento avanzado y altamente configurable servidor vigilancia del estado de monitoreo

Consolas de operador

Los terminales del operador punto final (PC) son la principal herramienta que los operadores de activar el sistema Pegasus, iniciar las instalaciones y los comandos y ver los datos recopilados

Aplicación Pegasus

La aplicación de Pegasus es la interfaz de usuario que está instalada en el terminal de operador. Proporcionan los operadores con la gama de herramientas para ver, ordenar, filtro, gestionar y alerta para analizar la gran cantidad de datos recogidos de los agentes de los objetivos

Redes Públicas

Aparte de ferretería e instalación del software en las instalaciones del cliente, el sistema Pegasus no requiere ninguna interfaz física con los operadores de red móvil local. Sin embargo, puesto que se transfieren los datos y las instalaciones del agente sobre las redes públicas, wemakes que se transfiera en la más eficiente y segura, todo el camino de vuelta a los servidores del cliente:

Redes de Anonimato

Pegasus anonimizar transmisión Network (red) está construido de anonimizar los nodos de conectividad que se distribuyen en diferentes lugares alrededor del mundo, permitiendo a agente conexiones ser dirigido a través de diferentes caminos antes de llegar a los servidores de Pegasus. Los nodos anónimos servir a sólo un cliente y se pueden configurar el cliente si es necesario.

Ver más información en la sección de transmisión red de anonimato de Pegasus.

Dispositivos de Destino

La arquitectura antes mencionada permite a los operadores a emitir las nuevas instalaciones, extraer, monitorear y activamente recopilar datos desde dispositivos de objetivos.

Nota: La Pegasus es un sistema de misión crítica de inteligencia, por lo tanto es completamente redundante para evitar averías y fallos. El sistema maneja grandes cantidades de datos y tráfico 24 horas al día y es escalable para apoyar el crecimiento del cliente y necesidades futuras

*Fecha de la clasificación	México, D.F., a 18 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Libramiento Octavo fracción II y V, fracciones c) y d) y Vigésimo Cuarto fracción II de los Libramientos Generales para la clasificación y desclasificación de la Información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Ámbito del Tránsito de la Unidad Administrativa	

Solución de Hardware

Las especificaciones de hardware para el funcionamiento del sistema Pegasus depende del número de agentes instalados concurrentes, el número de estaciones de trabajo, la cantidad de datos almacenados y por cuánto tiempo deben guardarse.

Todo el hardware necesario es suministrado con el sistema al despliegue y requerir personalización local que tiene que ser manejado por el cliente en función de que las direcciones. Si es necesario, hardware puede adquirirse por el cliente en función de las especificaciones proporcionadas por nosotros.

Operadores de Terminales

Los operadores de las terminales son unidades estándar de escritorio, con las siguientes especificaciones:

- Procesador: Core i5
- Memoria: 3 GB de RAM
- Disco Duro: 320 GB
- Sistema operativo: Windows 7

Sistema de Hardware

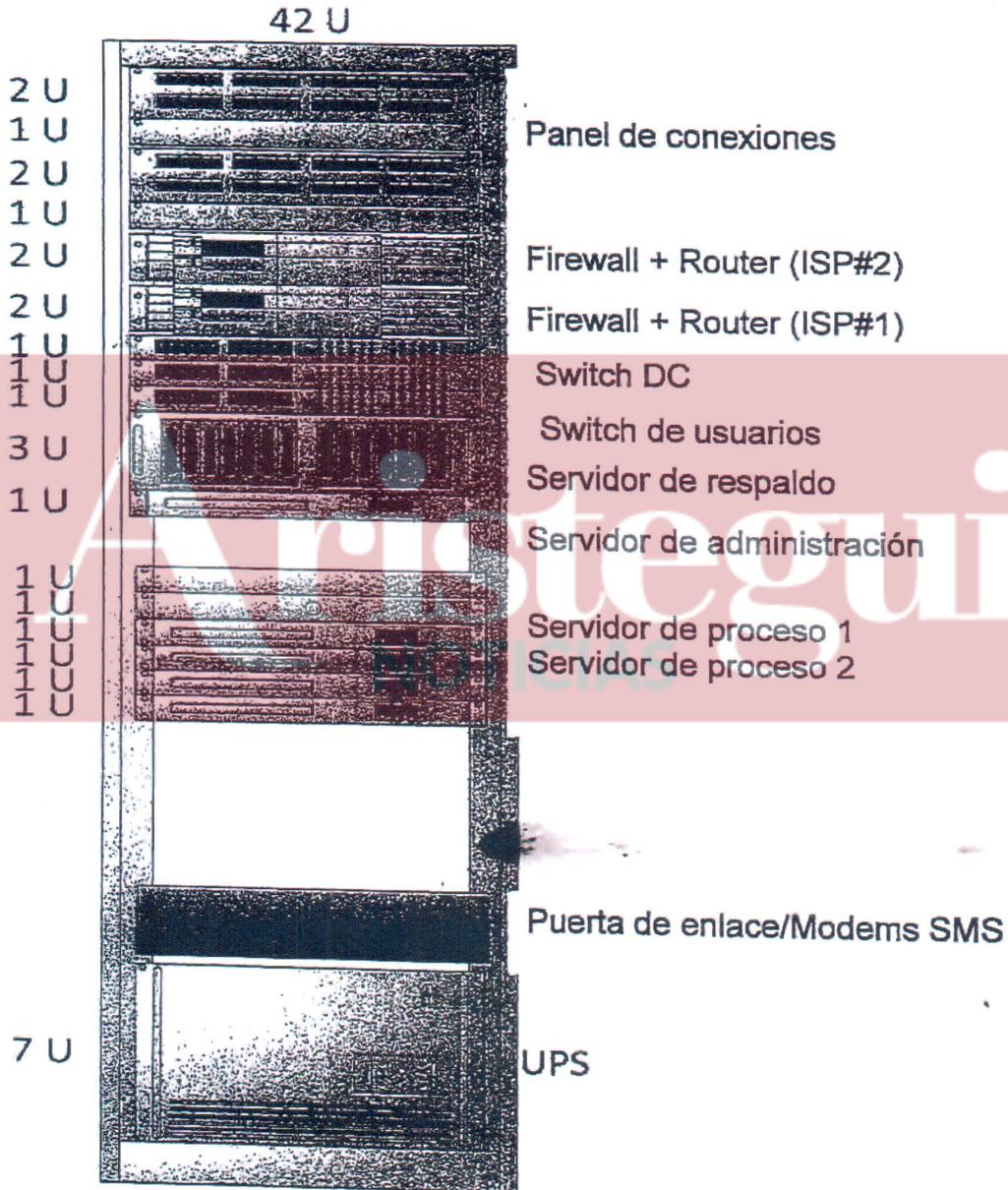
Para apoyar plenamente la infraestructura del sistema, el siguiente hardware se requiere:

- Dos unidades de 42U gabinete
- redes hardware
- 10TB de almacenamiento
- 5 servidores estándar
- UPS
- celular módems y tarjetas SIM

El esquema de hardware del sistema se muestra en la figura 11.

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Libramiento Dicho Cuarta fracción II y VI, incisos c) y d) y Vigésimo Cuarto fracción II de los Libramientos Generales para la clasificación y desclasificación de la Información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción JOG de la Ley que establece los Bases de Coordinación del Sistema Nacional de Seguridad Pública
Periodo de reserva	Hasta 12 años" (sic)
Régimen del Tablero de la Unidad Administrativa	

Figure 11: Pegasus Hardware



Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley de Planeación y el artículo 149 de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 46 Fracción XCG de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Adscripción del Titular de la Unidad Administrativa	



Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Analítica e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Básico Octavo fracción II y V, artículos 13 y 14 y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción IXXI de la Ley que establece los Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años* (sic)
Política del Titular de la Unidad Administrativa	

Formación y configuración del sistema

Somos responsables de la configuración del Sistema y capacitación antes de su entrega al cliente

Prerrequisitos del sistema

Instalación correcta del sistema Pegasus, requiere los siguientes preparativos para el site y la sala.

- 2 sistemas de aire acondicionado (18° C) para sala y site, regulados de manera independiente.
- 6 tomas eléctricas (20A) por rack.
- 2 enlaces de ATM simétrico de ISP diferente. Cada enlace con 10 direcciones IP estáticas (deben ser dos diferentes proveedores):
 - ISP #1: Fibra óptica basada en red (20 MB dedicado)
 - ISP #2: Ethernet categoría-7 basado en cable. (20 MB dedicado)
- 1 enlace simétrico.
 - ISP #3: Fibra óptica basada en red (200 MB no dedicados)
- 2 conexiones E1 PRI, cada una conteniendo 10 extensiones (deben ser dos diferentes proveedores)
- Corriente regulada con tierra física para la sala y site.
- 1 UPS de 30 KVA para el site.
- Lámparas de emergencia para sala y site.
- Alarma contra incendios.
- Salida de emergencia con señalización.

Una vez entregado el espacio, proporcionaremos todo el equipo y mobiliario necesario para óptimo funcionamiento del sistema sin costo alguno para la Procuraduría General de la República, así como en caso de requerir algún tipo de adecuación en el espacio que nos sea proporcionado solicitaremos la autorización del administrador del contrato cubriendo todos los gastos.

Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, párrafos c) y d) y Vigésimo Cuarto fracción I de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXII de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Período de reserva	Hasta 12 años (sic)
Relación del Tipo de la Unidad Administrativa	

Configuración del Sistema

- La solución será desplegada en el sitio del cliente por nosotros personal
- Duración implementación generalmente requiere trabajo 6-8 semanas de trabajo
- Ambiente operativo los requisitos deben cumplirse
- Configuración del Sistema incluye instalación de hardware y software, y además apoyan la integración al medio ambiente local y sistemas
- Apoyo y adaptaciones a las versiones de firmware del dispositivo local diferente

Entrenamiento

Tras la instalación del sistema, tenemos personal llevará a cabo sesiones de entrenamiento completo. La formación puede tener lugar en el sitio o en cualquier otro lugar requerido por el cliente, incluyendo que la sede. Sesión de entrenamiento incluye lo siguiente:

- Uso del Sistema Básico
- Arquitectura del Sistema
- Uso de Sistema Avanzado Y Funciones
- Ejercicios de Simulación en Modo Real

La cantidad recomendada de los asistentes es con respecto al número de operador de consolas instalado

Plan de despliegue de nivel alto

El proceso de adaptación, instalación y pruebas del sistema en un nuevo sitio de atención al cliente en listados en Tabla 3

PCIR
 Centro Nacional de Planeación
 Administrativa

Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Administrativa e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	15 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Didimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la Información de las Dependencias y entes de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción JOO de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Ámbitos del Título de la Unidad Administrativa	

Tabla 3: Plan de despliegue de Pegasus

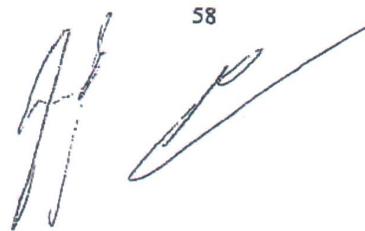
PLAN DE DESPLIEGUE DE "PEGASUS"	NOVIEMBRE					DICIEMBRE			
	1 AL 2	3 AL 9	10 AL 16	17 AL 23	24 AL 30	1 AL 7	8 AL 14	15 AL 21	22 AL 31
DIAS/SEMANA									
FASE 1 PREOPERATIVOS	ATP J94	Adquisición de equipamiento							
		Integración de sistemas							
FASE 2 IMPLEMENTACIÓN									
FASE 3 ENTRENAMIENTO Y FINALIZACIÓN							Proceso de transferencia de dispositivos		

Fase 1 – Preparaciones:

- Se definen los requisitos para un procedimiento de prueba de aceptación (ATP) junto con el cliente
- Adquisición de hardware y software y personalización para responder a las necesidades y requerimientos del cliente.
- Cuando sea necesario, el sistema Pegasus está integrado con los sistemas e infraestructuras locales
- Adaptaciones del sistema a las redes móviles locales

Fase 2- Implementación:

- Pruebas del Sistema
- Instalación de hardware
- Adaptaciones del sistema para versiones de firmware del dispositivo local

58


*Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Prevención Antiterrorista e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas a confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Libros de Orden Ocho fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción 100 de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (sic)
Tutor del Valor de la Unidad Administrativa	

Fase 3 – Formación y Terminación

- Simulación y detallado sistema de entrenamiento, situaciones de la vida real practicando
- Cliente ATP como se define en fase 1

Prueba de Aceptación del Sistema (SAT)

Hemos adquirido una experiencia considerable en la instalación y ejecución del sistema de Pegasus. El siguiente plan de prueba de aceptación verifica que el sistema funciona como sea necesario y valida que la correcta funcionalidad ha sido entregada. Describe el alcance del trabajo a realizar y el enfoque adoptado para ejecutar las pruebas adecuadas para validar que el sistema funciona como mutuamente acordado con el cliente.

Las pruebas se dividen en 3 etapas:

- Pruebas de funcionalidad
- Pruebas de red y proveedores
- Pruebas específicas de cliente sastra

Un sistema oficial mano desde el cliente se realiza una vez que el sistema ha sido implementado, probado y demostrado.

Mantenimiento, Soporte y Actualizaciones

Nos ofrece, como valor predeterminado, un año de servicios de mantenimiento, soporte y actualizaciones. Estos servicios incluyen

Mantenimiento y Soporte

Proporcionamos servicios de mantenimiento y soporte de nivel tres niveles que incluye

- Nivel 1: Sistema estándar operaciones problemas de correo electrónico y soporte telefónico
 - Nivel 2: Resolución proactiva de ingenieros dedicados problemas o técnica inspeccionará, examinar y resolver problemas técnicos comunes, poniendo sus mejores esfuerzos, asistencia remota usando software de escritorio remoto y una red privada Virtual (VPN) cuando así lo solicite
 - Nivel 3: Fallo sistema de fijación y las actualizaciones de sistema importantes desperfectos
- Soporte telefónico: además de lo anterior mencionado, proporcionamos el teléfono y correo electrónico de apoyo a cualquier pregunta y el problema que se plantea.

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservas
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley de los Libros de Comercio Artículo 1000 fracción II y Vigésimo Cuarta fracción II de los Libros de Comercio para la clasificación y desclasificación de la información de las dependencias y unidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XX de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años (12)
Rolístico del Titular de la Unidad Administrativa	

Además, el cliente será capaz de añadir la siguiente asistencia

- Asistencia en el sitio planeado o de emergencia
- Sistema de monitoreo de salud

Grados (Upgrades)

Tenemos comunicados importantes mejoras al sistema Pegasus pocas veces al año. Estas mejoras incluyen generalmente:

- Nuevas características
- Nuevo sistema operativo/dispositivos es compatible
- Características a medida según los requerimientos del cliente
- Corrección de errores

PARTIDA	DESCRIPCIÓN	SUBTOTAL
1	<p>SISTEMA PEGASUS 500 OBJETIVOS, INCLUYE:</p> <ul style="list-style-type: none"> - Hardware del sistema Pegasus. - Software del sistema Pegasus para 500 objetivos de manera simultánea. - Los siguientes sistemas operativos son compatibles con el sistema Pegasus: BlackBerry, Android, iOS, Symbian. - Incluye Software y la instalación de hardware, configuración y despliegue. - Implementación del sistema en redes y dispositivos que se indiquen. - Se ejecutará dentro de los 90 días contados a partir de la fecha de firma del contrato. - Incluye capacitación técnica del equipo local, formación operativa misma que se llevará a cabo en idioma español. Capacitación en línea para dar soporte. - Se incluye 1 año de garantía para el hardware / firmware y software contada a partir de la puesta en marcha 	\$27,600,000.00
	SUBTOTAL	\$27,600,000.00
	I.V.A.	\$4,416,000.00
	TOTAL	\$32,016,000.00



Tech Bull

EL ADMINISTRADOR DEL CONTRATO

LIC. MOISES EDUARDO BOLAÑOS BONILLA
DIRECTOR GENERAL DE INFORMACION SOBRE ACTIVIDADES DELICTIVAS DEL CENTRO NACIONAL DE PLANEACION, ANALISIS E INFORMACION PARA EL COMBATE A LA DELINCUENCIA.

FACTURA

26

GRUPO TECH BULL, S.A. DE C.V.
GTB131011FYA
Homero No. 538 Int. No. 303 Polanco Reforma Miguel Hidalgo, DF 11550 México

REGISTRO DE PEDICIÓN: Homero 538 303, Polanco Reforma, 11550, Miguel Hidalgo, DF, México FECHA: 11/11/2014 18:38:07

CLIENTE: PROCURADURÍA GENERAL DE LA REPÚBLICA

RFC: PGR850101RC6

DOMICILIO: AV. PASEO DE LA REFORMA No. 211-213 CUAUHTÉMOC DELEG.

COLONIA: CUAUHTEMOC

CIUDAD: MEXICO D.F.

CP: 06500

ESTADO: DISTRITO FEDERAL

PAÍS: MÉXICO

CANTIDAD	UNIDAD	CONCEPTO / DESCRIPCIÓN	VALOR UNITARIO	IMPORTE
----------	--------	------------------------	----------------	---------

1.00	UNIDADES	ANTICIPO 35% SISTEMA PARA LA REALIZACION DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURIA GENERAL DE LA REPUBLICA DENOMINADO "PEGASUS 500" REFERENTE AL VALOR TOTAL DE \$32,016,000.00 USD INCLUYENDO IVA	9,660,000.00	9,660,000.00
------	----------	--	--------------	--------------

MONTE CON LETRA VEINTE MILLONES DOSCIENTOS CINCO MIL SEISCIENTOS DOLARES 00/100

MODO DE PAGO TRANSFERENCIA BANCARIA NUMERO DE CUENTA DE PAGO IDENTIFICADA

CONDICIÓN DE PAGO: PAGO EN UNA SOLA EXHIBICION VERSIÓN: 3 2

SUBTOTAL: 9,660,000.00
IVA 16%: 1,545,600.00
TOTAL: 11,205,600.00



ESTE DOCUMENTO ES UNA REPRESENTACION IMPRESA DE UN CFDI EFECTOS FISCALES AL PAGO PAGO EN UNA SOLA EXHIBICION

Serie del Certificado del emisor: 00001000000301119419
Folio fiscal: 3DAFF0F3-BB19467E-8DFF-178D6F5CDB1A
No de Serie del Certificado del SAT: 00001000000202864883
Fecha y hora de certificación: Noviembre 11 2014 - 18:38:11
Régimen Fiscal: Regimen General de Ley Personas Morales

SELLO DIGITAL DEL CFDI

SELLO DEL SAT

CADENA ORIGINAL DEL COMPLEMENTO DE CERTIFICACIÓN DIGITAL DEL SAT