CIBERNOTICIAS

SECURITY ENCRYPTION SYSTEMS

Cyberoam

NEXXT SOLUTIONS

Avira

open source

CONTENIDO

CREDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:

Consuelo de la Torre

c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre

m.delatorre@scprogress.com (+593 998053611)

Revisado por:

Arturo de la Torre

adltorre@scprogress.com (+593 999025294)

Síguenos en:

www.scprogress.com www.facebook.com/SCProgress/?fref=ts @SCProgressECU

Intervención o espionaje en teléfonos celulares y fijos?

Las comunicaciones han avanzado de forma vertiginosa, hace pocos años atrás, no teníamos ni la más remota idea de la utilización de teléfonos celulares o inalámbricos que nos permitan comunicarnos sin la necesidad de contar con una conexión física, menos aún, que podamos transmitir datos, contar con servicio de internet, revisar nuestros correos electrónicos, poder comunicarnos de forma inmediata a través de aplicaciones como WhatsApp, Facebook, etc., etc.

Toda esta nueva e innovadora tecnología si bien es cierto "***nos ha facilitado la vida***", pero también, nos trae diferentes tipos de riesgos, como son la intervención de nuestras comunicaciones, ya sea por familiares, razones laborales, amigos o novi@s curiosos o personas sin escrúpulos que pretenden robar la información almacenada en nuestros dispositivos, así como, el robo de identidad y datos personales.

En ocasiones no siempre es el robo de información, lo que los motiva a intervenir nuestros Smartphone, sino simplemente lo hacen, para escuchar nuestras conversaciones, o leer nuestros mensajes enviados a través de SMS o de las diferentes aplicaciones para chat, que tengamos instaladas.

Existe una infinidad de medios, con los cuales es muy fácil intervenir los teléfonos celulares, así como, los convencionales. Se ha creado software especializado que realiza esta actividad, lo único que debe hacerse es instalar la aplicación en el Smartphone que desea rastrear y la tecnología hace el resto. El programa envía la información a un servidor remoto al cual se puede acceder un usuario y contraseña.

"Se debe indicar que el espionaje a las comunicaciones, no tiene marcas de preferencia, se puede realizar a todos los celulares, pueden tratarse de equipos con sistemas operativos Android, iPhone, BlackBerry o Symbian. Con el software apropiado, podrán tener acceso a la ubicación geográfica del móvil, el registro de llamadas y mensajes de texto (SMS) que entran y salen de la línea celular, los mensajes y agendas de contacto de aplicaciones como Whatsapp, iMessages, Facebook o Skype, además de la posibilidad de conocer el historial del navegador de Internet que utiliza el dispositivo.

Una vez instalado, el software espía para celulares trabaja de forma silenciosa y no deja rastros, por lo que el usuario del smartphone no se dará cuenta de lo que está sucediendo y actuará con naturalidad en cuanto a sus interacciones con el teléfono"[1].

En la presente edición vamos a aclarar las formas en las cuales se pueden realizar las intervenciones, para que nuestros lectores tengan conocimiento de las formas en las cuales pueden robar su información, a través de los medios más simples de comunicación, y tomen las precauciones necesarias para evitar ser víctimas de este nuevo tipo de invasión a nuestra privacidad.

Las intervenciones telefónicas se pueden realizar de dos formas:

1. *"Mediante equipos sofisticados como los IMTSI/IMEI/GSM/3G Catcher cuyo costo es muy alto. Este tipo de equipos no solo pueden intervenir y grabar las llamadas sino también los mensajes SMS/MMS como los de Messenger de los populares*

[1] http://www.espiaparamoviles.com/intervenir-en-el-telefono-de-alguien-con-un-software-especial/

equipos BlackBerry, por ejemplo. Incluso es bueno aclarar que dichos equipos no necesitan conocer el número telefónico a espiar, basta con estar a cierta distancia del equipo (que muchas veces puede ser hasta de kilómetros), prenderlo en Random Mode y buscar en el ambiente el celular destino para realizar el espionaje.

Dependiendo de qué información manejes puede que estén usando estos equipos para espionaje directo hacia tu persona o empresa, en este caso como estos equipos son pasivos no tendrás ningún tipo de señal de la intervención y tu única solución es usar software de encriptamiento de voz y datos.

SCProgress representante en Ecuador de GSMK CryptoPhone, siempre a la vanguardia, cuenta con la mejor tecnología para comunicaciones seguras en Smartphone y teléfonos fijos.

2. *La segunda forma de intervención, mucho más económica y que puede ser usada para vigilar empleados, hijos adolescentes, etc., es instalar un software directo en los celulares destino. Hay varios modelos en el mercado que ofrecen copia de SMS, abrir el micrófono del celular automáticamente para escuchar conversaciones del ambiente, envío de logs de llamadas recibidas y realizadas, etc.*

   Estas aplicaciones son sigilosas por lo que son muy difíciles de detectar. Pero si el portador sospecha que lo están monitoreando, puede rastrear en el sistema para obtener indicios.

   Por ejemplo uno de los más usados da indicios de su instalación porque aparece en el celular bajo el nombre genérico SyncManager, aunque no es premisa única.

   Estos "soplones" digitales espías están asociados al IMEI del smartphone, código interno que transmite el aparato cuando se conecta a la red celular. Por lo tanto, aunque se le cambie la tarjeta SIM, el celular sigue siendo espiado. Y no sólo eso. Además, al detectar el cambio, el software envía al invasor el nuevo número, así que no puedes librarte fácilmente de él.

   En todo caso para este tipo de espionaje telefónico, deben tener el celular al menos 5 minutos en la mano para poder realizar la instalación OTA (Over the Air). Si tu celular siempre está a tu vista y en tu poder, no tienes por qué preocuparte. El acceso físico es obligatorio a menos que el dispositivo móvil que desea monitorear es un iPhone y usted sabe su iCloud ID y contraseña.

   Nosotros como especialistas, recomendamos usar los servicios con los que podemos determinar, según el modelo, si existe algún software espía instalado, y tomar las medidas necesarias para eliminarlo de tu smartphone y así evitar que seas víctima de espionaje.

La idea de encriptar contenido de comunicaciones se ha vuelto un objetivo importante para varios sectores, tras la revelación de los programas de vigilancia de la NSA el año pasado gracias a la filtración de documentos obtenidos por Edward Snowden.

El mundo de los Smartphone no es ajeno a ese interés, y por lo mismo ya han surgido programas que ofrecen mensajería de texto encriptada e incluso llamadas de voz."

FUENTE: http://espionajemexico.blogspot.com/2012/11/tips-para-saber-si-tu-telefono-celular.html.
http://www.audienciaelectronica.net/2014/07/aplicacion-promete-evitar-que-intervengan-llamadas-telefonicas/
http://www.espiaparamoviles.com/intervenir-en-el-telefono-de-alguien-con-un-software-especial

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- **Créditos sin garante hasta 3.000 dólares.**
- **Otorgamos créditos para consumo, emprendedores y microempresarios.**
- **Las tasas de interés más bajas del mercado.**
- **Inversiones a plazo fijo.**
- **Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.**

ASISTENCIA MÉDICA AMBULATORIA

Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de:

Medicina general, ginecología y pediatría

COBERTURA EN ASISTENCIA DENTAL

- Examen Clínico y Diagnóstico
- Higiene Dental
- Alivio del Dolor
- Rayos X Periapical

- Profilaxis (Limpieza Dental Profunda)
- Restauraciones en resina simple
- Extracciones Simples

Suites en Tonsupa – Esmeraldas por mantener las cuentas activas, pagos puntuales e inversiones.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204
www.cooprumi.fin.ec

Cómo saber si tu teléfono es interceptado.

Como ya lo indicamos anteriormente, el espiar teléfonos, si se cuenta con las herramientas adecuadas, es mucho más fácil de lo que imaginábamos, así también, no necesariamente debemos ser prominentes empresarios, o pertenecer a instituciones o empresas importantes, todos estamos expuestos a que husmeen nuestras actividades telefónicas, por cualquier motivo.

"Si tienes alguna razón para creer que tu teléfono celular o teléfono fijo está siendo interceptado, hay algunas pistas que puedes identificar para respaldar tus suposiciones. Sin embargo, muchos de estos indicadores podrían ser causados por otros motivos, así que, para estar seguro, tendrás que notar muchas señales y no valerte de solo una de estas. Cuando obtengas evidencia suficiente para respaldar tus sospechas, podrás acercarte a la Policía Nacional y solicitar ayuda. A continuación conocerás los indicadores que debes reconocer si sospechas que alguien ha instalado un dispositivo para escuchar tus conversaciones por el teléfono.

Primeras suposiciones:

1. Preocúpate cuando tus secretos se hacen conocidos. Si una información privada se hace conocida, indicaría que hay una posibilidad de que se haya infiltrado por medio de un teléfono interceptado. Específicamente si solo un número reducido de individuos en quien confías sabía al respecto. Además, si, en algún momento, discutiste esta información solo por teléfono.

   - Esto es importante, en particular, si te encuentras en una posición que te hace ser valioso y, por ello, alguien te quiera espiar. Por ejemplo, si tienes un puesto de alto nivel dentro de una compañía poderosa que se enfrenta con muchos competidores, podrías estar en peligro de convertirte en una víctima de la industria clandestina de la información.
   - Para verificar si tu línea telefónica es interceptada, puedes brindar una información que parezca importante a alguien que sabes que puedes confiar y que no lo divulgará. Si esa información se filtra, sabrás que alguien más estuvo escuchando la conversación.

2. Mantente alerta si recientemente has sufrido un robo. Nota con extrañeza si, recientemente, alguien allanó tu casa, pero no robó nada de valor. Algunas veces, esto sugiere que alguien ingresó a tu casa con la intención de colocar un interceptor en tu teléfono.

Señales de otros teléfonos:

1. Presta atención a sonidos de fondo. Si escuchas un gran sonido de estática u otro sonido de fondo cuando hablas por teléfono, es posible que el sonido provenga de una interferencia creada por un interceptor.
   - No confíes en esta sola evidencia, ya que el eco, el sonido de estática y otros sonidos se pueden causar por una interferencia casual o por una mala conexión.

- Sin embargo, el sonido de estática y otros sonidos de rasguidos o pequeños chasquidos se pueden causar por una descarga capacitiva que proviene de dos conductores que están conectados.
- Asimismo, un indicador más preciso es un zumbido agudo.
- Puedes identificar sonidos que tu oído no puede oír si utilizas un sensor de sonido de baja frecuencia. Si el indicador se eleva muchas veces por minuto, tu teléfono podría estar siendo interceptado.

2. Utiliza tu teléfono alrededor de otros aparatos electrónicos. Si sospechas que hay un interceptor en tu teléfono, camina cerca de una radio o televisión mientras hablas por teléfono. Aunque no notes una interferencia en el sonido de tu teléfono, esta podría suceder cuando estés cerca de otro aparato electrónico.

   - Asimismo, presta atención si escuchas un sonido de distorsión cuando no utilizas mucho el teléfono. La señal de un teléfono inalámbrico activo podría interrumpir la transmisión de datos, incluso sin que se instale un software o hardware adicional en tu teléfono. Sin embargo, una señal inactiva no haría dicha interrupción.
   - Algunos micrófonos ocultos e interceptores utilizan frecuencias parecidas a la banda de la radio FM. Por ello, si tu radio realiza un chillido cuando se le coloca en mono y se sintoniza en la parte lejana de la banda, indicaría que se está utilizando uno de estos aparatos interceptores.
   - De igual forma, los interceptores pueden interferir con la frecuencia de la televisión en los canales de frecuencia ultra-alta (UHF, por sus siglas en inglés). Utiliza una televisión con antena para verificar si hay interferencia en la habitación.

3. Escucha tu teléfono cuando no lo estés utilizando en una llamada. Este debería estar en silencio. Es probable que haya un software o hardware instalado si escuchas un sonido de pito, chasquido u otro sonido en tu teléfono, incluso, cuando no se utiliza en una llamada.

   - En especial, presta atención si escuchas un sonido de interferencia vibrante.
   - Si esto ocurre, podría sugerir que el micrófono y el altavoz están activos vía comunicación lateral por gancho conmutador, a pesar de que el teléfono no se utiliza. Las conversaciones que tienes por teléfono se podrían escuchar dentro de un radio de 20 pies (6 m).
   - En cuanto a una línea fija, una señal de que hay un interceptor es si escuchas un tono de marcar cuando tu teléfono está colgado. Verifica este sonido con la ayuda de un amplificador externo.

Señales de un interceptor de teléfono celular

1. Presta atención a la temperatura de la batería. Si la batería de tu teléfono celular se calienta inusualmente cuando no lo utilizas y no se te ocurre una razón para que esto ocurra, podría ser que haya un software que se ejecuta en segundo plano. Este estaría causando que tu batería esté en uso constante.

- Por supuesto, una batería caliente podría ser señal de que se la ha usado demasiado. Esto sucede, en especial, si tu teléfono celular tiene más de un año y se debe a que las baterías de los celulares tienden a deteriorarse con el tiempo.

2. Nota con cuánta frecuencia necesitas cargar tu teléfono. Si, de repente, tu batería se descarga sin razón alguna, provocando que la cargues el doble de lo normal, podría estar pereciendo debido a un software de interrupción que se ejecuta constantemente en segundo plano y consume la energía.

- Además, tendrás que considerar la frecuencia en que has utilizado tu teléfono. Si lo has utilizado mucho últimamente, la necesidad creciente de cargarlo se debería al hecho de que has usado más de su energía. Esto solo se aplica si difícilmente utilizas tu teléfono o no lo has utilizado más de lo normal.
- Puedes monitorear la vida de la batería de tu teléfono inteligente si utilizas una aplicación como BatteryLife LX (https://itunes.apple.com/app/batterylife-lx/id324066310?mt=8) o Battery LED (https://itunes.apple.com/us/app/battery-led/id332499063?mt=8).
- Asimismo, ten en cuenta que la batería de un teléfono celular perderá la habilidad de mantenerse cargado con el paso del tiempo. Si este cambio sucede después de tener tu teléfono por un año o más, este se debería a que la batería es vieja y se ha usado demasiado.

3. Trata de apagar tu teléfono. Si este proceso se retrasa o no se puede realizar, este comportamiento extraño indicaría que hay alguien controlando tu teléfono a través de un interceptor.

- Presta mucha atención para determinar si tu teléfono celular toma más tiempo de lo normal para apagarse o si la luz de fondo se mantiene encendida incluso después de apagarlo.
- Esto puede ser una señal de que tu teléfono celular es interceptado, pero también, podría ser que hay un fallo técnico en el hardware o software de tu teléfono y que no guarda relación con una intercepción del teléfono.

4. Estate atento a actividad inesperada. Si tu teléfono se ilumina, apaga, enciende o comienza a instalar una aplicación sin que tú hagas algo, habría alguien infiltrándose en tu teléfono y controlándolo a través de un interceptor.

- Por otra parte, esto podría suceder si hay una interferencia casual durante la transmisión de la información.

5. Estate atento a mensajes de textos inusuales. Si, recientemente, recibes mensajes de texto que consisten de caracteres, letras o números extraños proveniente de remitentes desconocidos, estos mensajes serían una gran señal de alerta de que hay un interceptor amateur en tu teléfono.

- Algunos programas utilizan los mensajes de texto para enviar comandos al teléfono celular que se tiene como objetivo. Estos mensajes aparecen cuando estos programas se instalan sin cuidado.

6. Presta atención a tu cuenta de teléfono. Si el costo de tu paquete de datos se incrementa y sabes que no es culpa tuya, puede haber alguien que lo utiliza a través de un interceptor.

    - Muchos programas de espionaje envían los registros de tu teléfono a servidores en línea y, para ello, utilizan tu paquete de datos. Los programas más viejos usaban una vasta cantidad de datos, haciendo que sea fácil detectarlos. Sin embargo, los programas más nuevos son más difíciles de detectar, ya que utilizan menos datos.

Confirmar tus suposiciones

1. Utiliza un detector de interceptor. Este es un aparato que puede conectarse a tu teléfono. Como su nombre lo sugiere, este detecta las señales externas y los interceptores, permitiéndote saber si tus suposiciones eran correctas y que alguien ha estado escuchando tus llamadas. Se cuestiona la utilidad de estos dispositivos, pero para lograr detectar un interceptor, este necesitará poder detectar cambios eléctricos o de señal en la línea telefónica mientras se examina. Busca un dispositivo que mida los niveles de obstrucción y de capacidad eléctrica, además de cambios de señal de alta frecuencia

2. Instala una aplicación. En el caso de los teléfonos inteligentes, puedes instalar una aplicación que detecta un interceptor y que detecta señales de intercepción, además de acceso no autorizado a los datos de tu teléfono celular.

FUENTES: http://es.wikihow.com/saber-si-tu-tel%C3%A9fono-es-interceptado

http://www.voip-news.com/articles/voip-blog/listen-up-17-signs-that-you-are-being-wiretapped-51940

http://www.makeuseof.com/tag/6-signs-cell-phone-tapped/

http://acisni.com/is-there-spy-software-on-my-cell-phone-how-to-detect-being-monitored/

Humor


COMPAÑERO, HÁBLEME POR AQUÍ. POR AHORA ESTE ES EL MODO MÁS SEGURO.


Ya, corta el teléfono
No, corta tú
Jaja ¡No!, corta tú
¡Ay no!, corten ustedes


Tu dinero o tu vida!
Espera! Soy un programador
y?
No tengo dinero ... ni vida
(c) 2007 CodeComics.com


CTRL+Z ! CTRL+Z !!


Abuela!

Cryptophone: comunicaciones confiables y seguras.

CryptoPhone dispone de modelos Smartphone, teléfonos fijos y satelitales que garantizan la privacidad de sus llamadas contra cualquier interceptación de la misma. Para establecer una comunicación segura ambas partes deben utilizar un CryptoPhone.

Los teléfonos son de origen alemán y siempre tendrán la seguridad de que se encuentran protegidos de todo tipo de intercepciones, en el caso de los teléfonos celulares los protege contra ataques maliciosos, ya sean troyanos, virus o malware.

Los teléfonos celulares, tiene una banda firewall que los protege de ataques, al estar monitoreando constantemente la actividad del mismo. Y su sistema de cifrado de almacenamiento de doble capa salvaguarda los datos en reposo contra el acceso no autorizado. Al operar con el sistema operativo personalizado y propietario en los teléfonos la seguridad del dispositivo se optimiza. También cuenta con un módulo de aplicación de permiso que controla el acceso a los datos, sensores y a la red ya sean estas 2G GSM, 3G UMTS/W-CDMA, Wireless y LAN.

¿Por qué adquirir un teléfono encriptado?

- Ofrece la mejor seguridad criptográfica disponible en el mercado.
- Es fácil de usar.
- El código fuente está publicado, lo que significa que está bajo una constante supervisión de expertos en seguridad.
- Ha sido desarrollado sin intervenciones de gobiernos y no provee acceso a terceros a las comunicaciones ni a las llaves de encripción.
- No existen backdoors.
- Es más económico que cualquier otro producto competitivo.
- Existe un programa gratuito para convertir casi cualquier PC en un teléfono fijo Cryptophone compatible.
- Está basado en equipamiento estándar lo que nos permite adquirir accesorios a precios normales de mercado.

El equipo que desarrolló este teléfono encriptado ha aplicado cerca de 15 años al análisis de su concepto. Durante este tiempo hemos intercambiado ideas con la principal gente de seguridad del mundo acerca de cómo desarrollarlo correctamente. Además sus técnicos tienen certificación de la OTAN, Servicios de Inteligencia de la Unión Europea y el Departamento de Estado de EE.UU, entre otras. Un concepto estuvo claro desde el comienzo: que el código fuente del sistema esté disponible para la comunidad criptográfica/académica (y al público en general). A nuestro conocimiento no existe ningún teléfono encriptado fijo, móvil o satelital en el mercado que ofrezca esta importante característica.

FUENTES: http://www.cryptlab.com/cryptophone.

Rincón de los Expertos

En la actualidad existen diferentes algoritmos de cifrado, todos ellos tienen diferentes propiedades que los fabricantes los explotan de acuerdo a la necesidad de las aplicaciones que desarrollan.

Para una mejor comprensión de los algoritmos de cifrado, les recomendamos leer los artículos técnicos publicados en:

http://s3.amazonaws.com/academia.edu.documents/33551175/IJETAE_1211_02.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1476553310&Signature=FpVPCCuwHluPxHrjiuuE8yM7uaY%3D&response-content-disposition=inline%3B%20filename%3DDES_AES_and_Blowfish_Symmetric_Key_Crypt.pdf

http://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/

Es muy importante, y los expertos de SCProgress recomiendan, familiarizarse con la herramienta Cryptool, que les permitirá desarrollar todo tipo de prácticas, aplicando los algoritmos antes indicados. Esta herramienta la podemos descargar de la URL:

https://www.cryptool.org/en/

Hoy en día la mejor forma de garantizar la seguridad de nuestras comunicaciones, para voz y datos, es aplicar el algoritmo de Diffie Hellman, un ejemplo ilustrativo de la aplicación del mismo, lo podemos en ver en el siguiente video:

https://www.youtube.com/watch?v=zW9vFS4Edcg

“Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas”

— John Chambers —

Empresas o personas interesadas en promocionarse en nuestra revista, por favor contactarse con c.delatorre@scprogress.com

Novedades

Conferencia de Investigación y Ciencia para la aplicación de la ley policial - CEPOL 2016.

La Conferencia de Investigación y Ciencia de Policía CEPOL Europea 2016 se llevó a cabo en la ciudad de Budapest-Hungría del 5 al 7 de Octubre en el EIT (European Institute of Technology), en la que participo como conferencista, nuestro Gerente Técnico Marco de la Torre y Asesor Tecnológico, Arturo de la Torre, junto a importantes expositores en el área de investigación en ciberseguridad de la Unión Europea.

El tema de la exposición a cargo de Marco de la Torre, fue "NETWORK FORENSIC ANALYSIS IN THE AGE OF CLOUD COMPUTING", el mismo que causo mucho interés en el público presente, su brillante participación dejó muy en alto a los profesionales en tecnología de seguridad informática de nuestra empresa y país.

La presentación puede ser descargada desde la página web de SCProgress en el siguiente enlace:

PRESENTACIÓN CEPOL BUDAPEST

Marco de la Torre
Gerente Técnico SCProgress

Jurgen Stock
Director de Interpol

Arturo de la Torre
Asesor de Proyectos de TICs SCProgress
Formando parte del Comité Tecnológico

En la Conferencia, también realizó su exposición el Director de Interpol, Jorge Stock, quién en su intervención declaró que la prioridad No. 1 a nivel mundial, a partir del año 2017, será la lucha contra el darknet y la ciberdelincuencia, que cada día se tecnifica aceleradamente.

Nuestro Asesor de Proyectos de TICs, Arturo de la Torre, participó activamente en las conferencias dictadas, y también formo parte del comité tecnológico de la CEPOL 2016.

SCProgress representante en Ecuador de la multinacional Alemana GSMK CryptoPhone

Nos complace en dar a conocer a todos nuestros clientes, que a partir del mes de octubre del presente año (2016), somos los representantes oficiales en el Ecuador de la importante y reconocida multinacional Alemana GSMK CryptoPhone, con presencia a nivel mundial. Su sede se encuentra en la ciudad de Berlín – Alemania.

GSMK es una empresa líder en servicios móviles de voz y de seguridad de los mensajes, siendo una de las más grandes e innovadoras en temas de encriptación de VoIP y seguridad móvil de 360 grados. Produce y comercializa los primeros teléfonos móviles, satelitales y de escritorio que proporcionan cifrado fuerte de voz de extremo a extremo, con el código fuente completo publicado para su revisión.

GSMK CryptoPhone proporciona, seguridad integrada sin problemas, brindando protección de toda la información que se intercambia telefónicamente, así como a los datos almacenados en su dispositivo móvil.

Esta es una más de las importantes alianzas estratégicas de SCProgress, realizadas en el constante esfuerzo para ofrecer soluciones globales óptimas de seguridad informática para nuestros clientes, nuestro mayor esfuerzo lo enfocamos en conseguir productos innovadores de calidad, directamente desde los mejores fabricante a nivel mundial, con excelente soporte técnico y precios sin competencia en el mercado.

Marco de la Torre de SCProgress y Bjorn Rupp CEO de GSMK CryptoPhone, en un local típico alemán, celebrando los acuerdos alcanzados entre las dos empresas en Berlín.

Arturo de la Torre Asesor de Proyectos de TICs SCProgress realizando la inspección de los equipos de encriptación, para voz y datos, satelitales.

Authorized GSMK CryptoPhone Distributor

www.scprogress.com

Octubre 2016