Desarrollo de un sistema basado en ASTERISK que permita investigar situaciones anómalas (bypass) en el Ecuador para la SUPERTEL

Calderón Hinojosa Xavier Alexander, José Gonzalo Béjar Albán. Facultad de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional (EPN). Quito, Ecuador.

Resumen **- La aparición de nuevos desarrollos tecnológicos ha facilitado el desarrollo de diferentes métodos de fraude en telecomunicaciones. Iniciando con una breve revisión de las principales tecnologías IP utilizadas en servicios de telefonía y los tipos de fraude en telecomunicaciones más comunes en el Ecuador, el presente trabajo se enfoca en los sistemas telefónicos "bypass" y métodos para combatirlos.**

Se realiza también un análisis del impacto económico que los sistemas "bypass" han tenido en el Ecuador entre el 2005 y el 2010 (5 años), en base a datos proporcionados por la SUPERTEL. A continuación, se realiza el diseño de un sistema para la detección de líneas telefónicas utilizadas en "bypass" y que implementa la técnica denominada "Prueba de lazo cerrado"; dicho sistema está compuesto por tres partes principalmente: una aplicación desarrollada en JAVA, una base de datos en MySQL, y una PBX ASTERISK. Finalmente, se presentan los resultados de las pruebas realizadas al sistema y se listan las conclusiones y recomendaciones alcanzadas.

Índices **- ASTEM, ASTERISK, Bypass, Fraude, PBX, Lazo cerrado, SISPRIN, SUPERTEL, Telefonía IP, VoIP.**

I. INTRODUCCIÓN

Los delitos en telecomunicaciones son un motivo de preocupación para empresas en el negocio, usuarios y estado. Aun cuando la tendencia actual es la convergencia de servicios, la regulación en el Ecuador tipifica los sistemas telefónicos "bypass" como un delito. En este sentido, la Superintendencia de Telecomunicaciones junto a las operadoras de telefonía del país combaten este tipo de ilícitos.

Mientras las tecnologías de la información y comunicación avanzan en el Ecuador, es necesario que el combate que realiza la SUPERTEL en conjunto con las operadoras se complemente con el desarrollo de herramientas que faciliten dicho trabajo.

Este trabajo se realizó con la colaboración de la Superintendencia de Telecomunicaciones y la Dirección Nacional de Investigación Especial en Telecomunicaciones. Fueron ellos quienes con su tiempo, experiencia e ideas contribuyeron para formular y completar este trabajo.

Hago un reconocimiento especial al Ing. Julio César Hidalgo, Director Nacional de Investigación Especial en Telecomunicaciones, por su apoyo y apertura. De igual forma al Ing. Xavier Calderón por su guía durante el desarrollo de este trabajo, al Ing. José María Gómez de la Torre y al Tnlg. Roberto Pérez.

II. CONCEPTOS DE TELEFONÍA

A través de los últimos años, la forma en que funciona la telefonía ha cambiado radicalmente. Hoy en día se utilizan técnicas de transmisión digitales y se ofrecen una gran variedad de servicios.

A. Telefonía Digital

Los sistemas digitales son una modernización de los métodos de comunicación analógicos ya que integran conceptos de modulación y codificación. Estas técnicas permiten transmitir voz a través de canales digitales optimizando su utilización.

En el Ecuador, la mayor parte de la red de telefonía pública (PSTN) es digital, sin embargo la última porción en la red telefónica a través de la cual el usuario accede al servicio (bucle de abonado) aún es analógica [2]-[4]-[5].

B. VoIP y Telefonía IP

Al contrario de la creencia popular, VoIP no es un sinónimo de Telefonía IP. Voz sobre IP (VoIP) es una tecnología que permite la transmisión de voz en paquetes de datos a través de redes IP. La telefonía IP es mucho más que solo VoIP. La telefonía IP integra servicios que tradicionalmente se ofrecían solo en centrales telefónicas y aprovecha la universalidad de las redes IP [1]-[2].

A. Telefonía IP

Telefonía IP es una evolución tecnológica de la telefonía tradicional. En este nuevo sistema, los servicios ofrecidos por la telefonía tradicional se suman a nuevos servicios y son ofrecidos a través de redes IP.

Los mensajes de voz y datos se transportan a través de redes de datos utilizando paquetes IP, permitiendo ofrecer servicios como llamadas telefónicas, fax, mensajes de voz, conferencias y muchos más [4]-[5]-[7].

B. Voz sobre IP

El protocolo de Voz sobre IP, o VoIP, es una tecnología que permite la transmisión de voz en una red IP utilizando

paquetes de datos. Gracias a VoIP es posible realizar llamadas telefónicas a través de una red IP como el Internet. La tecnología VoIP utilizada en Telefonía IP permite realizar llamadas dentro de la misma red y hacia la red de telefónica pública conmutada. Hoy en día, Los principales protocolos utilizados en VoIP son el Protocolo de Inicio de Sesión (SIP) y el Protocolo de Intercambio Entre ASETRISK (IAX) [6].

1) Protocolo de Inicio de Sesión: El Protocolo de Inicialización de Sesión, o SIP por sus siglas en inglés (*Session Initiation Protocol*), define los parámetros de señalización para iniciar, gestionar y terminar llamadas telefónicas, conferencias, video llamadas, mensajes de mensajería instantánea y servicios similares, conocidos como sesiones multimedia [6].

2) Protocolo de Intercambio Entre ASETRISK: El Protocolo de Intercambio entre ASTERISK, o IAX por sus siglas en Inglés (*Inter-Asterisk eXchange Protocol*), fue desarrollado con el fin de implementar un protocolo que requiera poco ancho de banda para conectar centrales telefónicas ASTERISK. Con el paso del tiempo, este protocolo ha sido utilizado también para conectar PBX's con terminales telefónicos y otros equipos, y no exclusivamente en la conexión entre PBX's ASTERISK [8].

TABLA 1
CÓDECS DE VOZ

Nombre	Tasa de bits (Kbps)	Muestreo (KHz)
G.711	64	8
G.721	32	8
G.722	64	16
G.729	8	8
GSM	13	8

Junto con estos protocolos de señalización, se utilizan *códecs* para digitalizar un mensaje de voz o audio y que pueda ser transmitido como paquete de datos. En la tabla 1 se describen las principales características de los *códecs* más utilizados en la actualidad [6].

III. FRAUDES EN TELEFONÍA

El móvil más común para cometer un delito en telecomunicaciones es el rédito económico, directo e indirecto. En particular, rédito económico indirecto se refiere a aquellos métodos que no buscan lucro en sí, como el rédito directo, sino evitar pagar por el servicio.

A. Fraude por suscripción

Aunque este fraude involucra el uso de servicios de telecomunicaciones, no se trata de un fraude técnico. Se presenta durante el proceso de registro de un nuevo usuario, cuando este presenta documentación falsa o de terceros con el fin de que los cargos por el servicio o los equipos sean cobrados a otra persona [3].

B. Refilling

Es un procedimiento mediante el cual se utiliza un país intermediario para reducir el costo de la conexión con el país destino. La empresa que origina la llamada no la direcciona hacia el país destino sino hacia un segundo país que tiene una tarifa menor, en este segundo país se direcciona nuevamente la llamada hacia su destino final [3].

C. Fraude a PBX

El fraude a PBX ocurre en compañías que cuentan con una PBX conectada a Internet. En este tipo de fraude, el defraudador aprovecha una falla de seguridad para tomar control de la PBX y originar llamadas sin la intención de pagar. Todo el consumo que los defraudadores realicen es facturado a la empresa responsable de la PBX [3].

Este tipo de fraude se ha vuelto más sencillo de realizar con la aparición de PBX basadas en software libre. Por lo general, en este tipo de PBX no se implementan las medidas de seguridad adecuadas para prevenir este tipo de fraude lo cual hace vulnerables a pequeñas y medianas empresas. Es importante recalcar que el problema no es de las PBX de software libre sino de sus administradores quienes no consideran la seguridad como un factor importante.

D. Sistemas Telefónicos "Bypass"

Se denomina sistema telefónico "bypass" a aquellos sistemas que ingresan llamadas internacionales a la red de telefonía pública (PSTN), haciéndola pasar como una llamada local. La operadora local identifica y cobra esta llamada como una llamada local, mientras que el defraudador la cobra en el extranjero a un costo un poco menor que una llamada internacional autorizada y de esta manera obtiene su ganancia. En la Fig. 1 se observa un diagrama de este tipo de sistemas [3]-[7].

En términos generales, un "bypass" está conformado por una pequeña central telefónica, un Gateway de salida internacional (conexión a Internet), y un Gateway de salida hacia la red telefónica pública (líneas telefónicas del operador local). Las líneas telefónicas utilizadas pueden ser de telefonía fija o móvil [3].

El principal móvil para los defraudadores es el beneficio económico que estos sistemas generan. Poniendo en una balanza el costo de terminación de una llamada internacional en Ecuador que está entre los 12 a 15 centavos por minutos junto a los costos de una llamada local que puede estar ser de 1 centavo para llamadas de telefonía fija o alrededor de 8 centavos en telefonía móvil (sin considerar promociones o planes con tarifas preferenciales), la ganancia puede ser de 7

centavos o más por minuto de tráfico. Considerando un grupo de 16 líneas en un sistema "bypass", la ganancia por minuto puede superar el 1,12 USD, lo cual representa alrededor de 1600,00 USD diarios. Esto hace atractivo este tipo de fraude pese a que es motivo de prisión según las leyes ecuatorianas vigentes [9].

Fig. 1 Diagrama de un sistema telefónico "bypass"

Existen 2 tipos de sistemas telefónicos "bypass", aquellos que reciben una llamada internacional y la terminan en la red pública como una llamada local, y aquellos que reciben una llamada local con destino internacional y la envían al exterior a través de enlaces clandestinos. En el Ecuador, prácticamente todos los sistemas "bypass" corresponden al primer caso ya que es en el cual existe rédito económico para el defraudador.

IV. Situación en el Ecuador

En el Ecuador, el organismo de control encargado del combate a los ilícitos en telecomunicaciones es la Superintendencia de Telecomunicaciones a través de la Dirección Nacional de Investigaciones Especiales en Telecomunicaciones. La Superintendencia trabaja de forma coordinada con las operadoras de telefonía investigando, desmantelando sistemas "bypass" y realizando acciones preventivas [12].

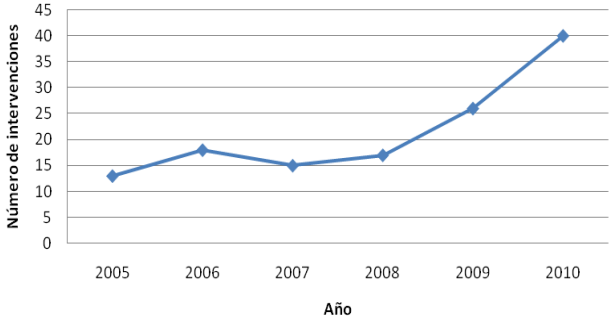

Fig. 2 Cantidad de intervenciones a sistemas telefónicos "bypass" realizadas por la SUPERTEL entre el 2005 y el 2010

Durante los 5 años posteriores al 2010, la cantidad de sistemas "bypass" desmantelados por la SUPERTEL ha aumentado, como se observa en la Fig. 2. En el 2005 se realizaron 13 intervenciones, mientras que en el 2010 la SUPERTEL intervino un total de 40 instalaciones clandestinas [12].

Esto se refleja, de igual forma, en la pérdida evitada por estas intervenciones. Como se observa en la Tabla 2, de no haberse realizado las intervenciones, este tipo de fraude habría generado una pérdida que superaría los 68 millones de dólares.

Estas cifras reflejan la severidad del impacto económico que pueden generar este tipo de fraude y la importancia de su combate. Las operadoras de telefonía más afectadas por este tipo de delito son CNT E.P., Claro y Telefónica Movistar, las más grandes en el Ecuador.

Tabla 2
Monto Estimado que se Evitó Perder por Acciones de la SUPERTEL

AÑO	MONTO
2005	3.486.033,00
2006	17.609.200,00
2007	8.801.691,00
2008	11.508.109,00
2009	11.646.597,00
2010	15.599.168,00
TOTAL	68.650.798,00

Las leyes ecuatorianas no tipifican a detalle cada caso de fraude en telecomunicaciones, sin embargo, los sistemas "bypass" están tipificados como delito penal en el artículo 422 del código penal, reformado mediante la "Ley Reformatoria al Código Penal No. 99-38" publicada en el Registro Oficial No. 253 del 12 de agosto de 1999 [11].

V. Diseño y Desarrollo del Sistema ASTEM

El diseño del sistema comienza con la identificación de las necesidades del usuario, en este caso la SUPERTEL. Entre los principales requerimientos de la SUPERTEL destacan:

- Realizar y recibir varias llamadas de prueba de forma simultánea utilizando líneas de telefonía fija y/o telefonía celular, y almacenar los CDR's.
- Programar la ejecución de pruebas de lazo cerrado utilizando tarjetas de telefonía pre-pagada.
- Identificar el número identificador de llamada (*Caller ID*) de las llamadas recibidas, y evaluar si pertenece a un origen nacional o internacional.

- Emitir una notificación vía e-mail al momento de recibir una llamada internacional con un número nacional en una prueba de lazo cerrado.

Con base en los requerimientos planteados, se determinó que el sistema debe tener varios módulos, como se observa en la Fig. 3. Entre dichos módulos destaca un gestor de llamadas de lazo cerrado, un monitor de llamadas, y una base de datos para almacenar los resultados obtenidos en las pruebas.

A continuación, se identificaron las tareas que debe realizar el sistema y se procedió a detallar los casos de uso que definen su diseño. Cada caso de uso representa un grupo de acciones que el sistema debe cumplir para llevar a cabo una tarea específica. Por ejemplo, los pasos para realizar una llamada de prueba y registrar los resultados.

Fig. 3 Componentes del sistema ASTEM

Una vez definidos los casos de uso y entrando en la programación, se procedió a detallar las Clases con sus métodos y atributos. Este es el paso previo al desarrollo del software ya que se definen los elementos del mismo. Las principales clases del sistema ASTEM realizan las llamadas de lazo cerrado y monitorean la actividad de la PBX para identificar y analizar el *Caller ID* de cada llamada de prueba.

Es importante notar que durante el desarrollo del sistema se realizaron varias mejoras al diseño del mismo. Estas mejoras se ajustaron a los casos de uso definidos durante el diseño cumpliendo con los requisitos definidos por la SUPERTEL para el sistema.

En el desarrollo también se pudo constatar que para este sistema se requiere entornos de desarrollo que permitan el manejo de hilos simultáneos. Esta es una característica necesaria para realizar el monitoreo de la PBX mientras se realizan las llamadas de lazo cerrado.

A. *Funcionamiento del sistema ASTEM*

La principal función del sistema ASTEM es realizar llamadas de lazo cerrado. Las llamadas pueden ser generadas una después de otra (consecutivamente), o varias al mismo tiempo (simultáneamente). De igual, las llamadas pueden ser ejecutadas inmediatamente o ser programadas para ejecutarse en cualquier fecha y hora futuras. Estas opciones se configuran el momento de solicitar las pruebas para que el servidor las procese.

El sistema utiliza tarjetas de telefonía pre-pagada para realizar las pruebas de lazo cerrado. Para esto, los datos de las tarjetas deben ser almacenados en el sistema. ASTEM, al iniciar una llamada, escucha en la línea telefónica la IVR de la tarjeta utilizada y sigue los pasos necesario para completar la llamada. Una vez que una llamada de prueba es recibida en el sistema, el monitor identifica y analiza el *Caller ID* recibido. Si el *Caller ID* corresponde a un número nacional, la llamada es considerada como sospechosa y se envía un correo electrónico con los datos de la llamada a un e-mail determinado. Finalmente, el sistema genera y guarda un CDR's de dicha llamada, en donde incluye la tarjeta de telefonía utilizada.

El sistema permite acceder a la base de datos de MySQL y realizar consultas sobre los resultados obtenidos. En la base de datos existen dos tablas. La primera guarda los CDR's generados por la PBX ASTERISK y la segunda guarda los CDR's generados por el sistema ASTEM.

Cada vez que se realiza una llamada de lazo cerrado, esta genera dos CDR's en la PBX, uno por la llamada saliente inicial y uno distinto por la llamada entrante, como se observa en la Fig. 4. Cada CDR recibe un número identificador único.

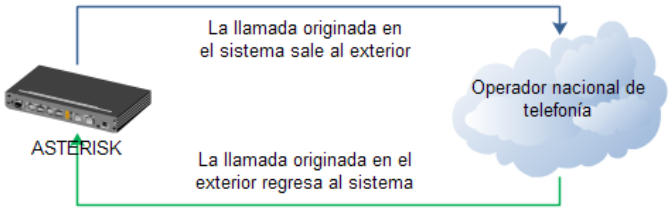

Fig. 4 Diagrama de las etapas de una llamada de lazo cerrado

El CDR generado por el sistema ASTEM para cada llamada de prueba guarda la hora de inicio y fin de la prueba, la tarjeta que se utilizó, los datos sobre los resultados obtenidos, el *Caller ID* recibido, y los números identificadores de los CDR's generados por ASTERISK durante la llamada de prueba.

ASTEM permite configurar las conexiones entre los elementos del sistema, los principales parámetros del plan de marcación y los canales analógicos y SIP configurados en la PBX, entre otras cosas.

B. *Funcionamiento de la PBX ASTERISK*

Las funciones de la PBX están limitadas a realizar las llamadas generadas en el sistema ASTEM y guardar los CDR's en la base de datos MySQL. Para esto, es necesario configurar los archivos de plan de marcación, parámetros de conexión con la base de datos y con el sistema ASTEM.

Cuando una llamada de lazo inicia, la PBX utiliza una línea telefónica para llamar a la IVR de la tarjeta de telefonía. Una vez que la IVR responde, la PBX sigue la grabación y completa la llamada de lazo, como se observa en la Fig. 4. Si la PBX detecta un problema durante la llamada o esta excede los tiempos máximos definidos, la llamada de lazo es terminada.

C. *Consideraciones de seguridad*

La seguridad en el sistema es muy importante ya que al utilizar una PBX el sistema puede ser vulnerable a Fraude de PBX. Además, la información guardada en el sistema es confidencial. Por este motivo, se consideraron aspectos de seguridad en 4 puntos del sistema: el sistema operativo, la aplicación núcleo de ASTEM, la base de datos, y la PBX ASTERISK.

La seguridad en el sistema operativo está relacionada con los servicios instalados. El servidor únicamente contiene la base de datos y la PBX ASTERISK como servicios disponibles. Se incluyó un servidor de correo electrónico configurado para procesar únicamente emails desde el sistema ASTEM. Además el servidor cuenta con contraseñas complejas. Por otro lado, la base de datos es accesible únicamente desde el servidor local y no recibe conexiones externas de ningún tipo.

El servidor no está conectado a Internet, lo cual añade un componente de seguridad ya que no es posible acceder a él remotamente.

En el sistema ASTEM se utiliza autenticación por desafío para permitir el acceso a los usuarios. Cuando un usuario intenta acceder debe ingresar su contraseña y el sistema resuelve un reto que consiste en realizar varias operaciones utilizando dicha contraseña. Si la contraseña es correcta, el reto es resuelto exitosamente y el usuario puede acceder a las opciones del sistema.

En la PBX se consideran varios aspectos de seguridad. Entre los más importantes están su plan de marcación y configuración del servicio. El plan de marcación en la PBX no permite ningún tipo de conexión externa y no esta definida ninguna forma para realizar llamadas que no sean generadas en el sistema ASTEM. Además, la PBX no contiene ninguna extensión configurada para usuarios, por lo cual no es posible realizar llamadas a través de un dispositivo SIP conectado a ella.

Finalmente, se ha configurado una única ruta de llamada que reproduce una grabación de un tono de timbre, de tal manera que en caso de que una llamada sea realizada desde la PBX lo único que haga es reproducir la grabación en mención.

VI. PRUEBAS Y RESULTADOS

Para probar el funcionamiento del sistema se plantearon 12 escenarios con objetivos específicos. En cada escenario se probó una función en particular del sistema en condiciones determinadas.

El sistema pasó todas las pruebas de funcionamiento y se obtuvieron los resultados esperados. Durante las pruebas se pudo constatar que el sistema cumple con los requerimientos del usuario.

VII. COSTO DEL SISTEMA

El costo del sistema está ligado directamente al trabajo de ingeniería que involucra el diseño de la solución y el desarrollo del mismo.

El costo del desarrollo está determinado por las horas de trabajo necesarias para escribir el programa, solucionar problemas durante el desarrollo, y realizar las pruebas necesarias para verificar su correcto funcionamiento.

Al costo del diseño y desarrollo se debe añadir el costo de implementación y soporte. En la Tabla 3 se recoge el costo total del sistema.

TABLA 3
COSTO DEL SISTEMA

Motivo	Valor (USD)
Equipos	2350,00
Diseño y desarrollo	28000,00
Implementación	1025,00
Soporte	1500,00
Subtotal:	32875,00
IVA:	3945,00
Total:	36820,00

VIII. CONCLUSIONES

En el Ecuador, los sistemas telefónicos no autorizados han aumentado en los últimos años. Los principales proveedores afectados han sido los de telefonía celular y CNT, en el caso de telefonía fija.

Los fraudes en telecomunicaciones tienen la característica de adaptarse a los avances tecnológicos. Nuevos desarrollos permiten a los defraudadores ingeniarse nuevas formas de cometer estos delitos. Por este motivo, el

tipo de sistemas "bypass" que se implementaban hace unos años es completamente diferente a los que se implementan hoy en día.

Existen diferentes métodos para combatir el fraude de sistemas telefónicos "bypass". Algunos de estos son preventivos y otros proactivos. Hoy en día, este tipo de fraudes se ha concentrado en la telefonía celular ya que esta, por su carácter inalámbrico, dificulta la tarea de ubicar físicamente las instalaciones clandestinas.

Las regulaciones con las que el Ecuador cuenta en el campo de las telecomunicaciones necesitan una actualización dado el progreso que este sector ha tenido en los últimos años. Es necesario que la ley contemple situaciones reales y sea más específica para determinar que es o que no es un delito en telecomunicaciones, y cuáles deben ser las sanciones.

El sistema desarrollado permite realizar llamadas de prueba simultáneas desde un mismo servidor, y controladas localmente. Estas llamadas son manejadas de forma independiente y generan sus propios CDR. Además, cuando un número es identificado como sospechoso, se envía una alerta vía correo electrónico.

IX. AGRADECIMIENTOS

El presente trabajo se debe en gran parte al apoyo y colaboración que brindaron los funcionarios de la Superintendencia de Telecomunicaciones en la Dirección Nacional de Investigación Especial en Telecomunicaciones y a los miembros de su laboratorio.

X. REFERENCIAS

Libros:

[1] FERNANDEZ, Luis; HERNANDEZ, Daniel. Plataforma para servicios de valor agregado basados en localización, en una red GSM, a partir de la medición de la intensidad de señal (Parte I), Volumen 20, Número 3, Venezuela, 2005.

[2] TANENBAUM, Andrew S. Redes de computadoras, 4ta edición, Editorial Pearson Educación, México, 2003.

[3] ING. MEZA, María José. Fraude en telecomunicaciones, 1ra edición, editorial Publi Asesores, Quito, 2008.

Artículos técnicos:

[4] NASER INGENIERÍA, Introducción a la Telefonía. Disponible: http://www.naser.cl/sitio/Down_Papers/Introduccion%20a%20la%20telefonia.pdf. Acceso: 15/10/2010.

[5] TERACOM TRAINING INSTITUTE, "Public Switched Telephonic Network". Disponible: http://www.telecommunications - tutorials.com/tutorial-PSTN.htm. Acceso: 24/11/2010.

[6] VoIP FORO, Protocolos VoIP. Disponible: http://www.voipforo.com/protocolosvoip.php. 20/02/2011.

[7] FCC, Información al consumidor. Disponible: http://www.fcc.gov/cgb/spanishlinks.html. Acceso: 17/01/2011.

[8] ASTERISKGUIDE, El protocolo IAX. Disponible: http://www.asteriskguide.com/mediawiki/index.php/El_Protocolo_IAX. Acceso: 08/02/2011.

[9] TELEFÓNICA DE ARGENTINA SA, Gerencia de Prevención y Control del Fraude. Prevención y Control del Fraude en las Telecomunicaciones, Argentina, 2009.

Artículos presentados en conferencias (no publicados):

[10] SUPERTEL; CNT; DIRECT TV. Taller internacional de delitos en telefonía y televisión por suscripción, Hotel DannCarlton, Quito, 2010.

Artículos legales:

[11] Ley Reformatoria al Código Penal No. 99-38. Reforma al artículo 422, publicada en el Registro Oficial No. 253 del 12 de agosto de 1999.

Oficios recibidos en base a solicitud:

[12] SUPERINTENDENCIA DE TELECOMUNICACIONES. Oficio IET-2011-00022, Pedido de información relacionado con servicios de telefonía internacional no autorizado, Quito, 2011.

XI. BIOGRAFÍAS

Xavier Alexander Calderón Hinojosa, nació el 16 de Agosto de 1972 en Quito-Ecuador, se graduó en el Colegio La Salle, especialidad Físico-Matemático en el año 1990. En el 2011 obtiene el título de Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional y en el 2002 se gradúa como Máster en Tecnologías de la Información en Fabricación en la Universidad Politécnica de Madrid. Actualmente trabaja en la Escuela Politécnica Nacional donde es profesor principal a tiempo completo, Miembro del Consejo de Departamento (Departamento de Electrónica y Redes de Información). Jefe del Laboratorio de Informática de la Facultad de Ingeniería Eléctrica y Electrónica y Director Proyecto Semilla. (xavier.calderon@epn.edu.ec)

José Gonzalo Béjar Albán, nació el 17 de marzo de 1988. Se graduó del Colegio San Gabriel, Bachiller en Ciencias Físico-Matemático, en el 2005. Posteriormente realizó sus estudios de pregrado en la Escuela Politécnica Nacional, donde obtuvo su título de Ingeniero en Electrónica y Redes de Información en el año 2011. Se desempeñó como pasante en la Dirección Nacional de Investigación Especial en Telecomunicaciones durante el 2010 y parte del 2011. Durante el primer semestre del 2012 se desempeñó como Ingeniero en Control de Fraude en Telefónica Ecuador (Movistar). En la actualidad se encuentra realizando una maestría "*M.S. in Telecommunications and Network Management*" en la Universidad de Syracuse, NY, Estados Unidos. (josebejar87@hotmail.com)