ESCUELA POLITECNICA NACIONAL

ESCUELA DE INGENIERIA

“ANALISIS DE ESTRATEGIAS PARA CONTROL DE FRAUDE EN LA TELEFONIA FIJA COMO MECANISMO PARA ASEGURAR LOS INGRESOS DE LAS EMPRESAS DE TELECOMUNICACIONES”

PROYECTO PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

CHRISTIAN MARCELO GALLARDO YANCHAPAXI

DIRECTOR: Ing. ERWIN BARRIGA

Quito, agosto 2006

DECLARACION

Yo Christian Marcelo Gallardo Yanchapaxi, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Christian Marcelo Gallardo Yanchapaxi

CERTIFICACION

Certifico que el presente trabajo fue desarrollado por Christian Marcelo Gallardo Yanchapaxi, bajo mi supervisión.

_____

Ing. Erwin Barriga
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a Dios y la Virgen que me han guiado a lo largo de mi vida y dado fortaleza para alcanzar mis anhelos y objetivos.

A mis padres Gloria y Marcelo por el sacrificio realizado; por su paciencia, apoyo incondicional y su confianza; por brindarme la oportunidad de aprender, mejorar y culminar mis estudios.

A mis hermanos: Juan Carlos por sus consejos, apoyo y compañía. Al pequeño David que ha alegrado mi corazón.

A la Escuela Politécnica Nacional, Carrera de Ingeniería en Electrónica y Telecomunicaciones, por su acertada enseñanza que me ha permitido forjarme personal y profesionalmente.

A mi director de tesis, Ing. Erwin Barriga por sus observaciones, apreciaciones, recomendaciones, sugerencias, correcciones y orientaciones en la formulación del protocolo de tesis.

A la Superintendencia de Telecomunicaciones, Dirección de Investigación Especial en Telecomunicaciones y Centro de Atención al Usuario, por el asesoramiento y colaboración para la realización de este proyecto.

A mis amigos por todas las penas y alegrías vividas.

A todas aquellas personas que me ayudaron y contribuyeron en la realización del presente proyecto, hago extensivo mi más sincero agradecimiento.

Christian G.

DEDICATORIA

A Dios y la Virgen que me han guiado a lo largo de mi vida.

A la memoria de mi madre, "Mamá Cuti" de quien he aprendido a luchar hasta en las condiciones más dificiles. Ella con su amor y ejemplo me ha mostrado que la vida está llena de oportunidades y felicidad.

A mis padres Gloria y Marcelo por inculcar en mí el amor, el sentido de responsabilidad, la fuerza de voluntad y las ganas de luchar por mis sueños.

A mis hermanos: Juan Carlos y David por su amistad, comprensión y compañía.

A todas las personas que han creído en mí...

Christian G.

ÍNDICE

CAPÍTULO III
ESTUDIO COMPARATIVO DE CURVAS DE TRÁFICO Y ANÁLISIS DE PÉRDIDAS ECONÓMICAS 118

ÍNDICE DE TABLAS

CAPÍTULO II

CAPÍTULO III

ÍNDICE DE FIGURAS

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

RESUMEN

El fraude en la telefonía afecta a toda operadora de telecomunicaciones y proveedor de servicios. El fraude reduce las ganancias, afecta a los buenos clientes y dificulta la eficiencia operacional. Las posibilidades tecnológicas para realizar fraude son inmensas, y considerando que actualmente se cuenta con la información y equipo necesario, los sistemas que permiten cometer fraudes son fácilmente implementados. Los costos reales del fraude pueden ser superiores a los ingresos perdidos. El impacto real raramente es cuantificado lo que reduce la visibilidad de la eficacia de medidas y acciones a tomar.

Cada tipo de fraude involucra diversos motivos, medios, modos y métodos, a pesar de las variaciones de actos ilícitos es posible reducir significativamente las perdidas que implica a las empresas telefónicas, considerando un adecuado sistema de detección, control y gestión del fraude en Telecomunicaciones, para proveer herramientas preventivas y correctivas en contra del fraude lo que permitirá asegurar los ingresos de las empresas de telecomunicaciones.

El proyecto “Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones” ha sido puesto a consideración de la Dirección General de Investigación Especial en Telecomunicaciones de la Superintendencia de Telecomunicaciones, la cual a manifestado[1] que el documento en mención aporta dentro de la comprensión del alcance con que dichos ilícitos afectan tanto técnica como económicamente a las empresas operadoras de telecomunicaciones debidamente autorizadas.

---

1 **ANEXO K.** Análisis realizado por la Dirección General de Investigación Especial en Telecomunicaciones de la SUPTEL del documento “Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones”

PRESENTACIÓN

En el presente proyecto se realiza el análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones. Para ello el contenido del proyecto se ha dividido en cuatro capítulos que se resumen de la siguiente manera:

Capítulo I **"Fundamento teórico".** Se analizan aspectos relacionados a estafas en telecomunicaciones como son: alternativas tecnológicas para control de fraude, consideraciones acerca del fraude, fraude relacionado con la interconexión de redes, el triangulo del crimen, gerencia de fraude y aseguramiento de ingresos. Además se considera el marco jurídico y sanciones impuestas de acuerdo al código penal frente a procedimientos ilícitos.

Capítulo II **"Fraude en telefonía fija".** Se analiza la estructura para clasificación de fraudes, la cual separa ordenadamente los diferentes tipos de fraude más frecuentes en la telefonía fija, permitiendo conocer la forma ilícita de operar, forma de detección, herramientas correctivas y preventivas para asegurar los ingresos de las Empresas de Telecomunicaciones.

Capítulo III **"Estudio comparativo de curvas de tráfico y análisis de perdidas económicas".** Se analiza la curva correspondiente al tráfico telefónico internacional según datos publicados por la FCC (Federal Communications Commission) y la curva correspondiente al tráfico telefónico de las operadoras nacionales según datos publicados por la SUPTEL (Superintendencia de Telecomunicaciones), el estudio de estas curvas permite observar el progreso que ha tenido el tráfico telefónico internacional y su tendencia de crecimiento que debió existir si no hubiera desviación de un importante volumen de tráfico que termina en rutas ilegales, y obtener una estimación de pérdidas de minutos y el perjuicio económico debido al fraude en telefonía.

Capítulo IV **"Conclusiones y recomendaciones".** Se presentan las conclusiones y recomendaciones que se han podido deducir en el desarrollo del proyecto.

Anexos:

Anexo A **"Glosario"**. Se presentan los términos utilizados en el desarrollo del proyecto, con definición o explicación de cada uno de ellos.

Anexo B "**Ley Especial de Telecomunicaciones Reformada**". Se presentan los artículos que la constituyen, los cuales sirven de marco jurídico para combatir el fraude en telecomunicaciones.

Anexo C "**Artículo 422 del Código Penal**". Artículo con el cual se sanciona los procedimientos ilícitos de prestación de servicios de telecomunicaciones, siendo el que mejor se acopla frente a los tipos de delitos analizados en el presente proyecto.

Anexo D **"Bandas de frecuencias satelitales"**. Se presenta la banda, su designación y el tipo de servicio típico utilizado en transmisiones satelitales.

Anexo E **"Intervenciones realizadas por la Superintendencia de Telecomunicaciones a estaciones de radiodifusión, sistemas de televisión por cable, y sistemas de By pass, que operaban sin autorización. (Documento proporcionado por la SUPTEL)"**. Se indica el cuadro de intervenciones realizadas por la Superintendencia de Telecomunicaciones a estaciones y sistemas de telecomunicaciones que operaban sin autorización, periodo comprendido desde agosto de 1992 hasta el 6 de junio de 2006.

Anexo F **“Configuración de equipos de telecomunicaciones”**. Se realiza a manera de ejemplo la asignación de direcciones IP, números telefónicos y configuración del equipo utilizado para implementar los sistemas tipo By pass.

Anexo G **“Interconexión internacional. (Documento proporcionado por la SUPTEL)”.** Se presentan los procedimientos requeridos para que operadores internacionales puedan intercambiar su tráfico.

Anexo H **“Operadoras que poseen concesión de servicio de telecomunicaciones y están autorizadas a cursar tráfico telefónico internacional. (Documento proporcionado por la SENATEL)”.** Se indican las operadoras telefónicas fijas y móviles legalmente establecidas en Ecuador.

Anexo I **“Ejercicios prácticos referentes al fraude en telecomunicaciones”.** Se presentan ejercicios prácticos y respuestas sugeridas relacionadas a diversos tipos de fraudes en telecomunicaciones.

Anexo J **“Equipos”.** Se adjuntan las hojas de características técnicas consultadas a los diferentes fabricantes de los equipos que se utilizan en la implementación de sistemas tipo By pass.

Anexo K **“Análisis realizado por la Dirección General de Investigación Especial en Telecomunicaciones de la SUPTEL del documento “Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones”. (Documento proporcionado por la SUPTEL)”**. Se presenta el documento con las observaciones realizadas por la Dirección General de Investigación Especial en Telecomunicaciones de la SUPTEL, acerca del contenido del proyecto de titulación.

CAPÍTULO

I

Fundamento teórico

CAPÍTULO I

FUNDAMENTO TEÓRICO

1.1 INTRODUCCIÓN

El fraude en las telecomunicaciones constituye un negocio muy lucrativo para el infractor, causa pérdidas millonarias y se da en todas las administraciones telefónicas del mundo. A pesar de los esfuerzos de las empresas y de las sumas millonarias que se ven obligadas a invertir para combatirlo, no es posible controlarlo totalmente pues el problema evoluciona al ritmo de la tecnología.

El nuevo esquema de competencia de las telecomunicaciones implica mayores facilidades para la obtención de los servicios, mayor disponibilidad y variedad de los mismos, las diferencias en la regulación entre los países, la diferencia entre tarifas de llamadas y cargos de acceso es un escenario propicio para el cometimiento de este ilícito.

El fraude se realiza de muchas formas. Desde el empleado que utiliza, en provecho propio, los servicios de la empresa para la cual labora; hasta las organizaciones criminales de cobertura nacional o internacional que proveen sus servicios de telecomunicaciones de manera anónima y secreta.

Otro factor que ha facilitado la comisión de diversos tipos de fraude es la interconexión de prácticamente todos los sistemas informáticos del mundo a través de las redes de arquitectura abierta. En este sentido, el advenimiento del Internet ha acelerado las posibilidades, la frecuencia y la magnitud de los delitos que a diario se cometen.

El fraude en telecomunicaciones se produce en todos los países del mundo, incluyendo al Ecuador, con pérdidas económicas importantes en las operadoras ANDINATEL S.A., PACIFICTEL S.A. y ETAPA, producidas principalmente por el tráfico telefónico internacional ilegal denominado By Pass, como también por el fraude interno.

Ante la necesidad, cada vez más apremiante, de contener el fraude en el área de las telecomunicaciones, se han venido desarrollando en la industria, equipos, software y sistemas tendientes a reforzar las acciones para la prevención y el control de las estafas. Existen en el mercado una serie de opciones para combatir los fraudes que se dan en telefonía fija, los cuales dependerán del proceso de la estafa, los métodos y recursos tecnológicos utilizados para cometer el acto ilícito.

Sin embargo, a pesar de que se pueda, técnicamente controlar el fraude en gran medida, siempre serán posibles nuevos tipos de estafas. Por ello, se requiere, en complemento, un marco legal estricto que permita tipificar estos delitos y penalizarlos adecuadamente.

1.2 DEFINICIÓN DE FRAUDE

El fraude se define como la aplicación deshonesta de servicios de telecomunicaciones, en los cuales el usuario no tiene la intención de pagar por los servicios utilizados.

El fraude afecta a toda operadora y proveedor de servicios de telecomunicaciones; ya sean aquellas que ya están establecidas o aquellas que recién están entrando al mercado. El fraude reduce las ganancias, afecta a los buenos clientes y dificulta la eficiencia operacional. Los costos reales del fraude pueden ser muy superiores a los ingresos perdidos; como por ejemplo: el desvío de recursos, inversiones innecesarias en la red, pérdida de clientes.

El impacto real raramente es cuantificado, lo que reduce la visibilidad de la eficacia de medidas y acciones a tomar.

1.3 BREVE DESCRIPCIÓN DE TIPOS DE FRAUDES

Son diversos los criterios para clasificar los distintos tipos de fraude que se cometen en los servicios y redes de telecomunicaciones, existen varios tipos de estafas en telefonía fija que dependerán en gran medida de la naturaleza de los recursos que estén siendo manejados, se los ha clasificado de acuerdo al perjuicio que causan:

- Fraude realizado por terceras personas donde es perjudicado el cliente final.
- Fraude realizado por terceras personas donde es perjudicada la operadora de telefonía.
- Fraude donde pueden intervenir otros operadores (con y sin licencia) afectando al resto de las operadoras de telefonía.

1.3.1 FRAUDE REALIZADO POR TERCERAS PERSONAS DONDE ES PERJUDICADO EL CLIENTE FINAL

Manipulación de armarios y robo de líneas telefónicas

Consiste en acceder sin la correspondiente autorización a los armarios de las operadoras telefónicas para generar llamadas que finalmente serán facturadas a los clientes perjudicados, por quedar registradas sobre su línea tomada ilegalmente.

Manipulación de PBX

Consiste en ingresar a las PBX de los clientes, empresas, instituciones, etc. accediendo en forma remota o local sin autorización, la configuración incorrecta de un PBX permite a intrusos el uso de sus facilidades para la realización de llamadas fraudulentas.

Llamadas efectuadas mediante el uso no autorizado de tarjetas telefónicas

Consiste en el uso indebido, sin consentimiento del titular, de los códigos de las tarjetas telefónicas y/o tarjetas de telefonía pública para la realización de llamadas fraudulentas.

Generación de llamadas telefónicas mediante engaño

Consiste en generar llamadas hacia determinados destinos, generalmente internacionales, mediante procedimientos engañosos que no le son aclarados debidamente al usuario, el cual desconoce que le serán facturadas posteriormente.

1.3.2 FRAUDE REALIZADO POR TERCERAS PERSONAS DONDE ES PERJUDICADA LA OPERADORA DE TELEFONÍA

Fraude en teléfonos públicos

Consiste en dañar y/o alterar técnicamente y/o eludir los controles de los equipos provistos por las compañías telefónicas, evitando el pago de las llamadas generadas.

Pagos fraudulentos

Consiste en efectuar pagos fraudulentos de facturas y/o consumos telefónicos correspondientes a las llamadas telefónicas realizadas por el defraudador.

Fraude de suscripción

Consiste en la solicitud de nuevas líneas telefónicas y/o nuevos servicios de telecomunicaciones utilizando identidad inventada no existente en la realidad y/o utilizando la identidad de un tercero sin su consentimiento o autorización para la realización de llamadas fraudulentas y evitar cancelar la factura telefónica.

Ingeniería social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, convirtiéndose quizás en el método de ataque más sencillo, menos peligroso para el atacante y uno de los más efectivos.

1.3.3 FRAUDE DONDE PUEDEN INTERVENIR OTROS OPERADORES (CON Y SIN LICENCIA) AFECTANDO AL RESTO DE LAS OPERADORAS DE TELEFONÍA

Call back

El Call back es un sistema, generalmente computarizado, que re-origina las llamadas, de tal forma que se tarifen y se facturen como si fueran llamadas telefónicas con origen o como si fueran hechas desde el extranjero.

Refilling

Consiste en el procedimiento mediante el cual el país que origina el tráfico lo enruta a un tercer país, que no es el destino final. Ese tercer país re-enruta este tráfico hasta su último destino.

By pass

El By pass encamina directamente el tráfico que viene del exterior hacia las centrales telefónicas locales, sin pasar por la central de tráfico internacional (es decir, se evita la tarifación de la llamada internacional y se la convierte en una llamada local).

1.4 ALTERNATIVAS TECNOLÓGICAS PARA CONTROL DE FRAUDE

El soporte técnico es clave para administrar los procesos informáticos y el proceso global de control de fraude, actualizar e integrar nuevas tecnologías para prevención, detección y control y para dar soporte de evaluaciones técnicas.

Es fundamental que el producto permita la detección del comportamiento anormal y que sea adaptable a la infraestructura existente, a los servicios ofertados y a su posterior desarrollo. Un adecuado análisis de la información obtenida permite al analista discriminar los casos probables minimizando el tiempo que se invertiría en la búsqueda de falsas alarmas y potencializando el esfuerzo hacia la detección y prevención del fraude. Existe software capaz de permitir al analista descubrir el método con que se comete el fraude.

Se debe contar con un sistema de adquisición de datos capaz de establecer perfiles de comportamiento por cada usuario individual, ya sea residencial o de negocio, su localización y el tipo de servicio que está utilizando, y comparar dicho comportamiento con patrones normales y fraudulentos, así el sistema puede generar alarmas cuando se detectan comportamientos que salen fuera del patrón.

Debe ser factible realizar consultas de llamadas por medio de claves para conocer la identidad del suscriptor, la duración de las llamadas, el destino de éstas y las especificaciones del servicio utilizado, con la posibilidad de detectar las cuentas de mayor riesgo y el monitoreo de patrones de llamada y duración de las mismas, uso excesivo de determinados servicios, llamadas solapadas e identidades de suscriptores celulares cambiadas.

Un elemento importante a tener en cuenta es la adecuada discriminación de la información que se va a analizar para evitar el uso innecesario de recursos en el estudio de la información. Pero si se requiere información detallada en el caso de un proceso judicial la información procedente de los CDR debe estar disponible.

Lo más importante a considerar al momento de seleccionar un sistema de detección de fraude, independiente del proveedor de tecnología de redes y conmutación, es que sea adaptable a la adquisición de datos provenientes de cualquier dispositivo, tanto para redes de telefonía fijas, móviles o redes basadas en IP. La plataforma debe ser flexible y escalable para todos los tamaños de redes y para pequeños o grandes volúmenes de CDR.

El sistema evalúa las reglas de fraude sobre las estadísticas de consumo para cada abonado cuantificando el valor de las llamadas una vez que se produce la valorización de los registros de comunicación, generando estadísticas de consumo individuales por día y por mes. Luego se realiza la evaluación del CDR valorizado mediante una fórmula para determinar si constituye un fraude, almacenando la información y generando una alarma si se establece la existencia potencial de fraude.

La funcionalidad de este producto está en que es flexible para adaptarse a innovaciones, es un modelo que soporta múltiples productos y servicios, así como la integración del núcleo del negocio en un solo sistema de información. Además, permite al usuario modelar la aplicación y crear nuevos productos en tiempo real.

1.5 CONSIDERACIONES ACERCA DEL FRAUDE

La telefonía fija ha desarrollado notoria, acelerada y constantemente las telecomunicaciones en todas las naciones; no obstante, como sucede en gran parte del ámbito tecnológico, a la par con su progreso, se crean mecanismos que permiten a ciertos individuos o grupos aprovecharse del servicio con distintos fines ilícitos.

1.5.1 MÚLTIPLES OPERADORES, PRINCIPALES INCONVENIENTES

La liberación del mercado y el ingreso de nuevos operadores para ofrecer servicios de telecomunicaciones han ocasionado que la competencia desleal se multiplique para los diferentes servicios existentes, con lo que el fraude también se ha desarrollado, a continuación se mencionan algunos de los servicios que se ofrecen en la actualidad.

- Telefonía local alámbrica.
- Telefonía local inalámbrica.
- Telefonía de larga distancia internacional.
- Telefonía pública.
- Telefonía celular.
- Servicio de transmisión de datos.
- Voz sobre IP (VoIP).

Los servicios antes mencionados tienen que ser ofrecidos a los clientes por medio de la red de telecomunicaciones, ya que seria ilógico que éstos sean ofrecidos por redes diferentes o que usuarios de un servicio no puedan conectarse o comunicarse con usuarios de otro operador.

Lo que lleva a la obligatoriedad que los operadores de diferente servicios se conecten entre sí, lo que ocasiona que se tengan múltiples puntos de interconexión, múltiples operadores introduciendo tráfico internacional, diferentes o particulares modos de negociar para cada operador con sus clientes y finalmente esto ocasionaría confusión en los usuarios de estos servicios.

En este escenario donde actúan diferentes operadores de telecomunicaciones, es donde se presentan los siguientes problemas:

- Competencia desleal entre operadores.
- Problemas en las liquidaciones mensuales.
- Tráfico internacional, proveniente de varios operadores.
- Introducción del tráfico internacional como local.
- Introducción del tráfico de larga distancia nacional como local.
- Falta de estabilidad en el mercado.
- Confusión de los usuarios.
- Imposible para el ente regulador ejercer los controles adecuados.
- Incumplimiento de los estándares de calidad.

1.5.2 MOTIVACIONES PARA COMETER FRAUDE

Entre las principales motivaciones para cometer un fraude se tiene:

- Obtención de dinero fácil y rápido mediante empresas que fácilmente pueden ocultar actividades ilegales.
- Sanciones leves para las personas que son identificadas en operaciones ilícitas.
- Fragilidad en el marco regulatorio del país donde se cometerá el fraude.

- Facilidades tecnológicas para cometer el fraude de forma remota.
- Falta de oportunidades para obtener trabajos dignos, a personas que disponen de un alto conocimiento técnico.
- Facilidades de asesoramiento e infraestructura prestada por empresas extranjeras, que motivan la instalación de sistemas ilegales, con la finalidad de obtener mejores precios que los ofrecidos por las empresas legalmente establecidas.

1.5.3 FACTORES QUE PERMITEN EL CRECIMIENTO DEL FRAUDE

Entre los principales factores para que se incremente el fraude tenemos:

- La gran facilidad que existe para adquirir información y el uso de muy variadas tecnologías para producir fraude.
- La competencia que existe entre las empresas, produce menores exigencias en la selección de clientes.
- El control interno realizado en las empresas operadoras de telecomunicaciones es insuficiente para detener el fraude.
- El uso de varias tecnologías para producir fraude, en especial las que tienen que ver con la voz sobre Internet que en la mayoría de los países no ha sido regulada.
- Acciones realizadas por el personal infiltrado en varios departamentos de las empresas operadoras de telecomunicaciones, este personal forma parte de los grupos de fraude y facilita desde el interior de las empresas el cometimiento de actos ilícitos.
- Falta de visión de los directivos en las empresas operadoras de telecomunicaciones, lo cual se traduce en despreocupación por los ingresos que se dejan de percibir y por consiguiente no se implementa las políticas necesarias para montar una plataforma tecnológica que permita combatir el fraude.

1.5.4 INDICADORES Y CONTROL DE FRAUDE.

Los principales indicadores sobre la presencia de un fraude son:

- Alteraciones en la facturación.
- Historial de falta de pago.
- Múltiples cuentas con similar nombre y dirección.
- Errores en la facturación.
- Datos de clientes repetidos en los registros de suscripción.

1.5.5 ASPECTOS QUE SE DEBEN CONTROLAR

Los principales aspectos que se deben controlar para un efectivo control del fraude son los siguientes:

- Los indicadores de utilización de servicios
- La información de seguridad y el adecuado acceso a los servicios.
- Establecer óptimos sistemas de monitoreo y detección.
- Sistemas de alerta por cambios de dirección sorpresivos.

1.5.6 CONSIDERACIONES SOBRE EL CONTROL DEL FRAUDE

- El fraude nunca podrá ser eliminado, pero puede ser reducido significativamente.
- Es importante focalizar el control interno en las operadoras de telecomunicaciones.
- Establecer procedimientos para el mejoramiento de los sistemas de control.
- Es importante evaluar periódicamente la vulnerabilidad de los sistemas.
- Se debe utilizar toda la información disponible para combatir el fraude.
- Es importante establecer el intercambio de información entre empresas operadoras de telecomunicaciones y organismos de control.

1.5.7 RAZONES POR LAS CUALES EL FRAUDE ES CUANTIFICADO

El fraude al ser cuantificado permite:

- Estimar el alcance de las denuncias.
- Definir las inversiones que sean necesarias.
- Establecer la relación entre las pérdidas y las ganancias.
- Realizar estudios acerca de la tendencia económica de las operadoras.

1.5.8 ASPECTOS COMUNES QUE DEBEN CONSIDERARSE

Los aspectos comunes que se presentan en actos ilícitos, generalmente abarcan las siguientes consideraciones:

- Es importante focalizar las pérdidas provocadas por el fraude y no los ahorros.
- Los elementos que rodean una actividad fraudulenta pueden ser confusos.
- La terminología que se emplea para el fraude es diferente en cada país.
- Un sistema antifraude no es infalible, tiene aspectos que le hacen vulnerable.

1.5.9 MEDICIONES Y NIVEL DE FRAUDE

Para realizar las mediciones y niveles de fraude, se deben establecer los siguientes procedimientos:

- Establecer procesos básicos para la administración e implementación del control.
- Estudio, interpretación y cuantificación de resultados.
- Procedimientos en los que se considere todos los procesos de la empresa.
- Se deben fijar metas y objetivos.

1.5.10 PRINCIPALES PERJUDICADOS EN EL FRAUDE TELEFÓNICO

Existen dos principales perjudicados en el fraude telefónico, que son: el abonado y el operador legalmente establecido.

Para el caso del abonado que es perjudicado por los inescrupulosos que se roban su línea y le dan uso indebido, cargándole con llamadas que por lo general son internacionales, cuyo perjuicio se ve reflejado en la planilla telefónica que tiene que pagar.

Las empresas operadoras tienen que implementar sistemas y procedimientos que mantengan informado al abonado de los posibles tipos de fraude y las precauciones que debe tener para no ser victima de este delito.

1.6 FRAUDE RELACIONADO CON LA INTERCONEXIÓN DE REDES

Conceptos de interconexión.

El objetivo de la Interconexión de Redes es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario, es decir que los aspectos técnicos particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Para la prestación de servicios de Telecomunicaciones la interconexión es una obligación, e incluye acceso a diferentes redes, infraestructura y servicios.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

Problemas de las interconexiones.

La interconexión de prácticamente todos los sistemas informáticos del mundo a través de las redes de arquitectura abierta es un factor que ha facilitado la comisión de diversos tipos de fraude. En este sentido, el advenimiento del Internet ha acelerado, las posibilidades, la frecuencia y la magnitud de los delitos que a diario se cometen.

Los problemas comunes que se presentan en la interconexión de redes y servicios de telecomunicaciones son:

- La interconexión y el control del tráfico de la información no recibe la atención y el control que se merece.
- Los contratos para establecer una interconexión son largos y muy complejos.
- Para establecer la interconexión se necesitan enrutamientos definidos, esto produce dificultades en la comunicación entre redes diferentes.
- No se tiene prioridad para analizar las deudas y discrepancias originadas en interconexiones.
- La falta de seguridades en la interconexión de redes permite a personas (Hackers) el tener acceso a la información y manipularla a su conveniencia.

Red telefónica pública versus Internet.

- Los costos por los servicios que brinda una red pública convencional son mucho más altos que los de Internet.

- Las redes públicas convencionales utilizan sistemas de procesamiento centralizados, pues todos los servicios que prestan se realizan en las centrales telefónicas, a diferencia de esto los servicios que se presentan en Internet cuentan con servidores de acceso que se encuentran distribuidos alrededor de todo el mundo.

- Los servicios que ofrecen las redes públicas convencionales dependen de la inteligencia con la que cuentan las centrales telefónicas, frente a esto, Internet está formada por muchos equipos terminales dotados de inteligencia, lo cual permite al usuario, tener control en el uso de las aplicaciones.

- Los servicios que se brindan a través de una red pública son rígidos y para su mejoramiento se necesita de grandes inversiones económicas, a diferencia de los servicios de Internet que permiten flexibilidad, y además, comprenden una inmensa gama de alternativas que necesitan pequeñas inversiones económicas, lo que se traduce en beneficios para los usuarios.

- Los servicios que se brindan a través del Internet permiten la implementación de servidores inteligentes que interactuarán con equipos inteligentes como computadoras personales y teléfonos de última generación, además incorporan ayudas gráficas y audio para su funcionamiento, estos servidores comparados con las tradicionales redes de telefonía pública, son más competitivos en cuanto a precios y mejoras tecnológicas.

1.7 EL TRIÁNGULO DEL CRIMEN

La forma como se desarrolla el crimen en cualquier actividad tiende a seguir un proceso común, el cual es considerado un ciclo cerrado representado de una manera triangular, en el que intervienen el motivo, método y oportunidades, los mismos que actuando de una manera conjunta e ilícita permiten llevar a cabo el proceso fraudulento, en el ámbito de las telecomunicaciones se tiene:

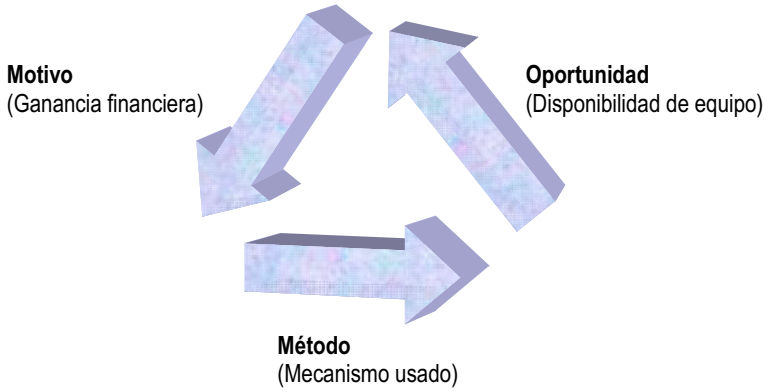


Figura 1.1. Triángulo del crimen[1]

Motivo

El motivo es el objetivo fundamental del fraude. Los motivos que comúnmente llevan a las personas o empresas a cometer actos ilícitos incluyen:

- Ganancia financiera.
- Bajos costos de operación.
- Rápido retorno de inversión.
- La codicia.

---

1 IBC. INTERNATIONAL BUSINESS COMMUNICATIONS, Curso: Renueve Assurance & Fraud Management Americas, 2002

Método

Los métodos del fraude son la descripción detallada para cometer actos ilícitos. Estos métodos varían por producto, servicio y por red, generalmente incluye: VSAT, VoIP y Conexiones ilegales.

Oportunidad

Las oportunidades aprovechadas, por las personas o empresas que pretenden o están realizando actos ilícitos, generalmente son:

- Disponibilidad rápida del equipo.
- Falta de regulación y ley.
- Ninguna medida penal, o sanciones leves aplicadas ante el ilícito.

1.8 GERENCIA DE FRAUDE Y ASEGURAMIENTO DE INGRESOS

El proceso de afrontar la problemática del Fraude en telecomunicaciones tiene dos aspectos muy importantes:

El primero se refiere a la detección de estafas, para lo cual se utiliza los sistemas de gerencia de fraude, los que permiten detectar y controlar situaciones anómalas en la utilización de un servicio de telefonía.

El segundo se refiere al proceso de garantizar y maximizar los ingresos de un operador de telefonía, para lo cual se utiliza los sistemas de aseguramiento de ingresos, los que permiten cerciorar que todos los ingresos sean debidamente medidos, facturados y cobrados con la máxima eficiencia.

1.8.1 GERENCIA DE FRAUDE

La implementación de una gerencia de fraudes demanda cambios organizacionales, cambios en los procesos, en los sistemas técnicos y en las operaciones de estos sistemas, pero sobre todo un cambio de mentalidad de los funcionarios y el apoyo de la alta gerencia de las empresas.

Un adecuado sistema de gerencia de fraude requiere por parte de los operadores el desarrollo de una estructura funcional y operativa que debidamente organizada de cómo resultado la conformación de un equipo de trabajo que responda de manera pro activa para la detección y el manejo del fraude.

La estructura organizacional de una gerencia de fraudes deberá estar conformada por un equipo de trabajo que incluya en su desempeño las fases de control, cada una de las cuales debe cumplir roles específicos. Cuando se menciona un equipo de trabajo no significa que se requiere un excesivo número de personas, siendo las fundamentales el analista y los auxiliares de fraude, cada uno de ellos con funciones y responsabilidades definidas.

1.8.1.1 Elementos de gerencia de fraude

Para tener un cuadro completo de los riesgos de fraude es necesario que se especifiquen las amenazas y vulnerabilidades de la empresa, también cuantificar el potencial de impacto en términos financieros directos e indirectos.

De esta forma poder constituir una gerencia de fraude eficiente la cual permitirá minimizar las oportunidades de pérdidas, optimizar las soluciones y evitar duplicación de esfuerzos, el enfoque del plan contempla los siguientes elementos:

Figura 1.2. Elementos de gerencia de fraude[2]

Comprensión del problema – evaluación y análisis de riesgos.

La comprensión del problema es el pilar fundamental de una administración exitosa. Desde una evaluación de riesgos más amplia hasta revisiones y análisis más específicos, para dar un adecuado direccionamiento al desarrollo de estrategias.

Definición de estrategias.

La definición de estrategias es un factor primordial para la implantación exitosa de controles administrativos, desarrollada a partir de un análisis de riesgos, se puede determinar cómo, dónde y cuándo aplicar los controles.

---

2 IBC. INTERNATIONAL BUSINESS COMMUNICATIONS, Curso: Renueve Assurance & Fraud Management Americas, 2002

Desarrollo organizacional.

Se deben definir la responsabilidad y apropiación de la administración del fraude: revisión organizacional, diseño de la estructura del equipo, selección de recursos, definición de procesos y programas apropiados de entrenamiento y toma de conciencia.

Especificación y planeamiento de contra-medidas.

Los controles deben ser planificados y aplicados apropiadamente. En el caso de contra-medidas externas, tales como la adquisición de un sistema detector de fraude, es necesario que haya una definición clara de los requisitos y del proceso de selección.

Implementación de controles.

Hasta los controles más apropiados pueden tornarse ineficaces debido a una implementación inapropiada. El desarrollo de procedimientos de apoyo y el asegurar una integración apropiada con toda la empresa son elementos fundamentales para la implementación de cada control.

Definición de mecanismos de medición e Informes.

La visibilidad continua asegura el correcto funcionamiento y progreso de la empresa, para lo cual se consideran parámetros como: mecanismos eficaces de clasificación, medición e informes, lo que permitirá ayudar en el entendimiento y facilitará la administración.

1.8.1.2 Equipo de gerencia de fraudes

El equipo de gerencia de fraudes está enfocado en la gestión de asegurar y aumentar el valor del negocio tanto para las empresas de telecomunicaciones como para los usuarios de la misma. Añade valor al negocio a través de la integración de elementos fundamentales, como aseguramiento de ingresos, gestión de fraude y optimización de la empresa con actividades claves del negocio.

En el tema del fraude el tiempo es oro, por ello cabe recalcar que los equipos más eficientes empiezan a actuar antes de que los defraudadores cometan los errores que hacen que los sistemas de detección activen las alarmas y los identifiquen.

El equipo de trabajo incluye en su desempeño las fases de control de fraude, las cuales giran en torno al control de fraudes en telecomunicaciones.

Figura 1.3. Fases de control de fraude[3]

3 IBC. INTERNATIONAL BUSINESS COMMUNICATIONS, Curso: Renueve Assurance & Fraud Management Americas, 2002

Prevención.

El área encargada de la prevención debe ser capaz de analizar los procesos para identificar su vulnerabilidad, por ejemplo en las áreas de cobros y facturación, para establecer procedimientos y procesos de control, elaborar estadísticas, analizar las tendencias que tienen las acciones de fraude y sus posibles causas.

La investigación post facturación es necesaria para monitorear y corregir los errores, detectar y referir casos sospechosos e identificar patrones de alto uso y/o zonas de alta incidencia.

Entre las tareas de prevención y control se deben priorizar el registro de las líneas en listas negras, atención especial a series de teléfonos públicos no autorizados para larga distancia, líneas con consumos sospechosos o sin posibilidad de verificación de sus consumos y como medida radical el cierre de destinos identificados como fraudulentos.

Los aspectos considerados por el equipo de gerencia de fraude para preparar y disponer con anticipación los recursos necesarios en contra de actividades ilícitas que perjudican a la empresa y usuarios son:

- Análisis de procesos.
- Establecer prácticas, políticas y procedimientos.
- Estructurar procesos de control de fraudes.
- Evaluar la vulnerabilidad de nuevos productos.
- Desarrollar tecnología preventiva.
- Elaborar estadísticas.
- Análisis de tendencias de fraude y causas.
- Establecer programas educacionales.

Detección.

El área que debe cumplir la fase de detección debe tener entre sus funciones la de monitorear los patrones de uso y referir los casos detectados para su investigación, de ser descubiertos nuevos patrones o comportamientos documentarlos para su estudio y seguimiento.

A pesar de que cada tipo de fraude implica la adopción de determinadas acciones de detección, entre las actividades y mecanismos utilizados para realizarla se deben tener en cuenta principalmente la adquisición de la tecnología apropiada que administre adecuadamente los sistemas de información destinados al monitoreo y control de los patrones de uso.

Los parámetros a tener en cuenta en un proceso de detección en el área de las telecomunicaciones son:

- Consumos promedios y máximos.
- Cantidad de llamadas, duración y su valor referidos a un periodo de tiempo.
- Seguimiento a las líneas, no solo sobre la información general sino seguimiento y verificación de los consumos y pagos.
- El monitoreo en tiempo real de llamadas de larga duración.
- El monitoreo en tiempo real de llamadas de corta duración.
- Llamadas a un destino o número específico.
- Análisis de los reportes de las centrales, rutas internacionales, cantidad y duración de las diferentes rutas.
- Análisis de los reportes del servicio al cliente, acerca de llamadas sospechosas, del reporte de destinos restringidos o destinos bajo seguimiento.
- Atención a los parámetros constantes en los reclamos de los usuarios.

Investigación post-facturación.

El equipo de gerencia de fraude y los usuarios del servicio trabajan en forma conjunta para determinar si se han producido parámetros anormales en la facturación, los aspectos que se consideran son:

- Realizar investigaciones de llamadas desconocidas realizadas o recibidas por los usuarios.
- Corregir errores de facturación.
- Referir casos de sospecha de fraude.
- Identificar patrones de alto uso y/o zonas de alta incidencia.

Disuasión.

La disuasión es un mecanismo que debe estar presente permanentemente tanto interna como externa a la empresa para evitar el cometimiento de fraude. Es necesario no solamente persuadir al personal, sino formar a los responsables en los organismos reguladores, de policía y de justicia para su acción efectiva en contra de actividades ilícitas.

El equipo de gerencia de fraude previene el inicio de actividades fraudulentas convenciendo al posible agresor de que su ataque no podrá desarrollarse y fracasará, haciéndolo desistir de su propósito de cometer fraude, para lo cual se consideran los aspectos:

- Desarrollar operaciones pro activas contra el fraude.
- Desarrollar investigaciones reactivas.
- Entrenar y coordinar operaciones con organismos de seguridad.
- Recomendar mejoras en la legislación contra el fraude.

Soporte técnico.

Las herramientas usadas con frecuencia por el equipo de gerencia de fraude son los servicios de software y hardware, lo cual implica que es esencial el correcto funcionamiento y actualización de los mismos, se consideran los aspectos:

- Administrar procesos informáticos.
- Integrar nuevas tecnologías de prevención, detección y control.
- Dar soporte a evaluaciones técnicas de nuevos productos.
- Dar soporte técnico al proceso global de control de fraudes.

Perfiles del personal.

Adicionalmente a los aspectos antes mencionados, es importante la formación humana y capacidad técnica del equipo de gerencia de fraude para un desarrollo honesto y eficiente de actividades, los perfiles incluyen:

Perfil técnico.

- Manejo de computadoras.
- Dominio de softwares, servicio al cliente.
- Técnicas de investigación.
- Conocimientos de fraudes en telecomunicaciones.

Perfil humano.

- Capacidad de análisis.
- Creatividad.
- Trabajo en equipo.
- Honestidad.
- Servicio al cliente.

1.8.1.3 Proceso de gerencia de fraude

El proceso de gerencia de fraude es la clave de cualquier mecanismo de mejoramiento, ya que asegura un enfoque completo y continuo para aumentar la rentabilidad y mejorar el desempeño de las empresas de telecomunicaciones, y por ende proporcionar servicios de buena calidad para el usuario.

Es posible administrar cualquier negocio sin buenos mecanismos de medición ni informes pero esto es extremamente peligroso; por lo cual un proceso de gerencia de fraude apropiado es primordial para la continuidad del éxito, conduciendo proyectos para mejorar los márgenes de ganancia y asegurar los negocios.

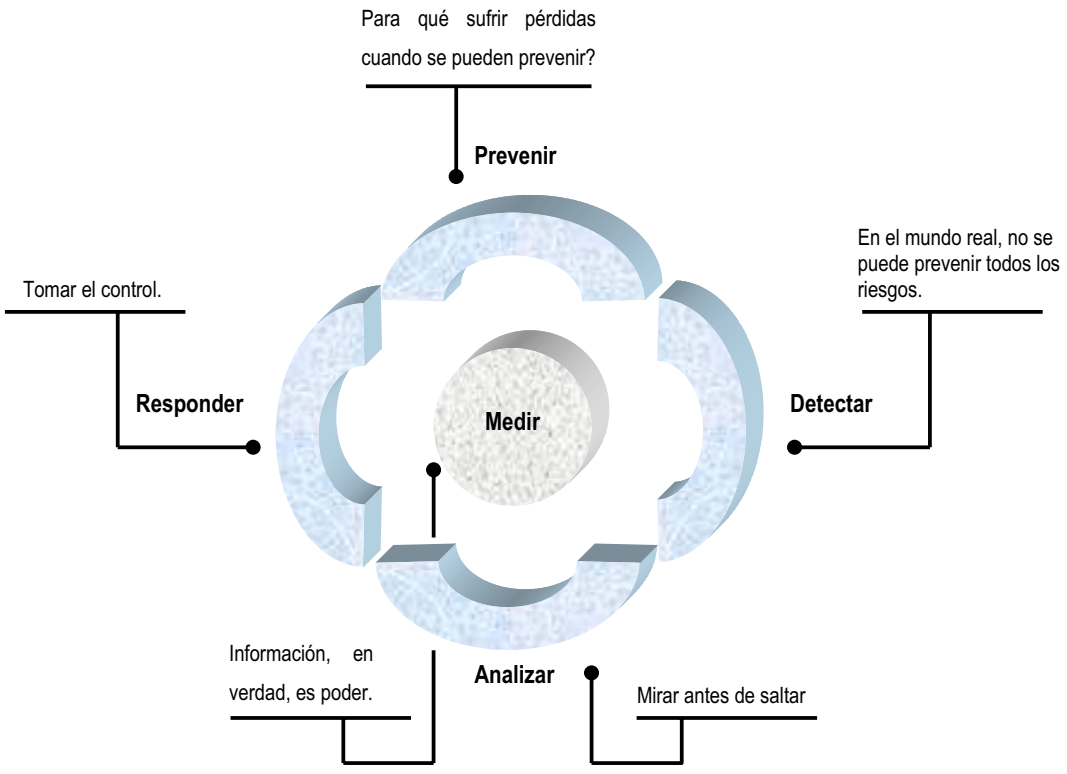


Figura 1.4. Proceso de gerencia de fraude [3]

Medir.

La Medición permite comprender dónde estamos, establecer metas hacia dónde queremos llegar y vigilar nuestro desempeño durante el camino.

Prevenir.

Se pueden adoptar medidas preventivas para controlar los costos; minimizando el fraude, fallas en la seguridad y fuga de ingresos. La especificación, implementación y operación de tecnologías actualizadas funcionando de una manera conjunta permiten reducir los riesgos de forma significativa.

Detectar.

La detección puede originarse tanto interna como externamente a la empresa, pero se debe saber dónde buscar, muchas actividades de detección pueden ocurrir usando componentes operacionales ya existentes, como por ejemplo, elementos de red, plataformas de productos, mecanismos de facturación, herramientas contables de interconexión, sistemas controladores de tráfico, y con una capacitación apropiada del personal.

Analizar.

Un análisis táctico, efectivo y estratégico apoyado por las herramientas adecuadas, proporcionará la claridad para el desarrollo adecuado de la empresa. Conocer el problema antes de actuar ayudará a aumentar la efectividad de la acción escogida.

Responder.

Existen varios tipos de respuestas que dependerán en gran medida de la naturaleza de los riesgos que estén siendo manejados. Ya sea una respuesta táctica que trate rápidamente un determinado problema, o una respuesta estratégica que traerá una mayor efectividad futura o para atenuar las pérdidas. Las decisiones apropiadas e implementaciones oportunas son factores críticos para el éxito.

1.8.2 ASEGURAMIENTO DE INGRESOS

El aseguramiento de ingresos está definido como: El concepto de cómo garantizar y maximizar los ingresos de un operador de telecomunicaciones.

La esencia del aseguramiento de ingresos es cerciorar que todos los ingresos sean debidamente medidos, facturados y cobrados con la máxima eficiencia y con costos mínimos, generando un máximo beneficio para las actividades actuales y futuras de la empresa.

La necesidad de llevar a cabo un proceso de aseguramiento de ingresos nace por las muchas oportunidades de pérdidas de ingresos, como por ejemplo:

- Errores en las tarifas o sistemas de descuentos.
- Errores en al creación de cuentas.
- Datos corruptos.
- Inadecuada liquidación de tráfico basado en la confianza de la información presentada por proveedores de interconexiones que pueden causar problemas.
- La información de clientes es inadecuada e incompleta.
- La información del sistema de facturación no está protegida adecuadamente.

- Las tablas del sistema de facturación no están siendo actualizadas de manera oportuna.
- Los errores en los procesos de tarifación y facturación no están siendo resueltos en forma oportuna.
- No se factura correcta y oportunamente el uso del servicio.
- Errores en los software de los switches o de plataformas lo que significa que el CDR no se genera bajo ciertas circunstancias.
- Incorrecta configuración de los switches que causa la no generación de los CDR's (situación que puede producirse en forma accidental o deliberada).
- Errores en los procesos de recolección de los CDR's.
- Controles inadecuados sobre los archivos de errores generados del procesamiento de CDR's.

Para asegurar ingresos, las actividades desarrolladas por la empresa se relacionan con diversos procesos y áreas operacionales de la organización, se contempla los siguientes elementos:

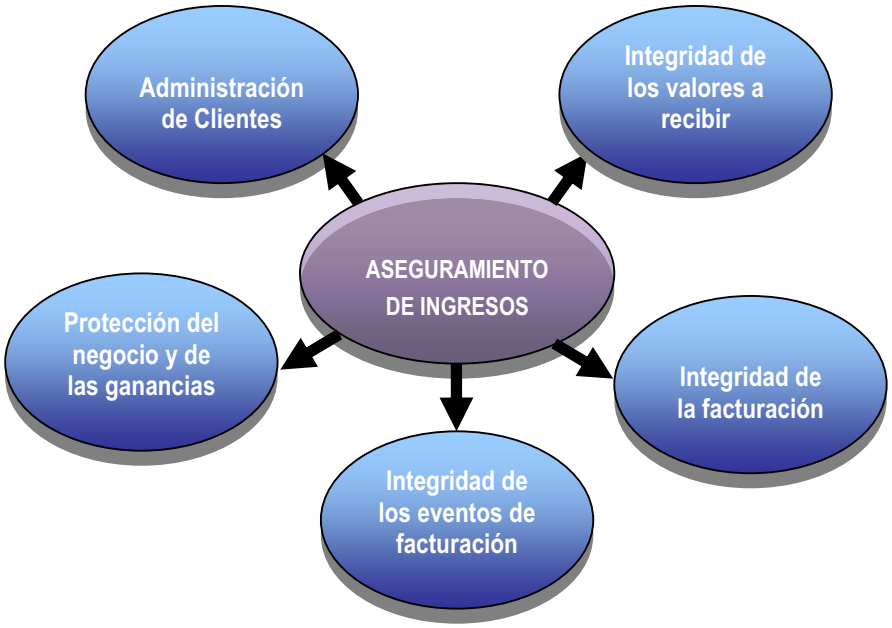


Figura 1.5. Elementos de aseguramiento de ingresos[4]

4 IBC. INTERNATIONAL BUSINESS COMMUNICATIONS, Curso: Renueve Assurance & Fraud Management Americas, 2002

Integridad de los eventos de facturación.

Los registros de facturación realizados en forma automática o manual pueden ser afectados por muchas condiciones generadas en los procesos operacionales o por los clientes y por lo tanto, una revisión cuidadosa sumada al análisis de riesgos es de suma importancia para garantizar la integridad del flujo de ingresos.

Integridad de la facturación.

Cada flujo de registros de facturación debe ser diseñado, monitoreado y auditado para asegurar que los datos recibidos, procesados y entregados a los demás sistemas dependientes sean como debieran ser, resultando finalmente en una factura completa y exacta para ser entregada al cliente correcto o al socio proveedor de servicio.

Integridad de los valores a recibir.

Una vez que los servicios son facturados, los pagos tienen que ser recaudados y administrados apropiadamente, lo que permitirá un tratamiento seguro de resultados para la empresa. Para reducir riesgos y mejorar la eficiencia son esenciales una detallada contabilidad de las recaudaciones, como las políticas y mecanismos contables aplicados.

Protección del negocio y de las ganancias

Un completo enfoque de Aseguramiento de Ingresos cerciorará que el riesgo es reducido, y de presentarse fraude, fallas en la seguridad o desastres críticos en el negocio, estos sean manejados en niveles aceptables.

Administración de Clientes.

Los clientes son la fuente fundamental de ingresos. Una administración ineficaz ocasiona una deserción de clientes y facilita el fraude. Una administración eficaz garantiza y asegura los ingresos presentes y futuros.

Cada área en contacto con el cliente debe ser considerada para optimizar el proceso de aseguramiento de ingresos. De la misma forma, cada interacción con el cliente necesita ser estructurada y administrada apropiadamente.

Un adecuado proceso de aseguramiento de ingresos permite obtener resultados positivos, como son:

- Mejores flujos de efectivo como resultado de ciclos de facturación más cortos.
- Volúmenes menores en el centro de llamadas debido a la disminución de errores en las facturas
- Reducción en las quejas de los clientes debido a la disminución de errores de facturación.
- Disminución de quejas por parte del cliente debido a problemas de facturación, lo cual reduce el nivel de reserva de ingresos requerido.
- Mejor capacidad para balancear y controlar los sucesos en el flujo de ingresos, validando que nada se haya perdido. Lo que se debe facturar se factura.
- Menor potencial de publicidad negativa.
- Propiedad y responsabilidad exclusiva del proceso de facturación de principio a fin.

1.9 MARCO JURÍDICO PARA COMBATIR EL FRAUDE

La Ley Especial de Telecomunicaciones Reformada[5] que rige en Ecuador sirve de marco jurídico para combatir el fraude, fundamentalmente sus artículos están basados en las prohibiciones o restricciones del uso indebido o no autorizado de los servicios de telecomunicaciones.

En relación a los procedimientos ilícitos de prestación de servicios de telecomunicaciones se imponen las sanciones de acuerdo al código penal, siendo el que mejor se acopla frente a este tipo de delitos el artículo 422[6] de dicho código.

---

5 **ANEXO B.** Ley Especial de Telecomunicaciones Reformada

6 **ANEXO C.** Artículo 422 del Código Penal

CAPÍTULO

II

Fraude en telefonía fija

CAPÍTULO II

FRAUDE EN TELEFONÍA FIJA

2.1 ESTRUCTURA PARA CLASIFICACIÓN DE FRAUDES

Existen varias formas diferentes de llevar a cabo un fraude en telefonía fija las que dependerán en gran medida de la naturaleza de los recursos que estén siendo manejados.

Para identificar, medir y reportar problemas se necesita de un sistema de clasificación. El sistema de clasificación debe separar ordenadamente los diferentes tipos de fraude en una estructura fácil de usar, la clasificación se realiza de acuerdo a parámetros como son:

Estructura para clasificación de fraudes		
1.	**Motivos**	Razón básica del por qué el defraudador lleva a cabo un fraude.
2.	**Medios**	Herramientas que sirven para desarrollar y efectuar el fraude.
3.	**Modos**	Clasificación genérica de cómo el defraudador realiza un fraude.
4.	**Métodos**	Detalle de cómo el defraudador realiza un fraude.

Tabla 2.1. Estructura para clasificación de fraudes

Desglosando la tabla 2.1 de una manera detallada se tiene:

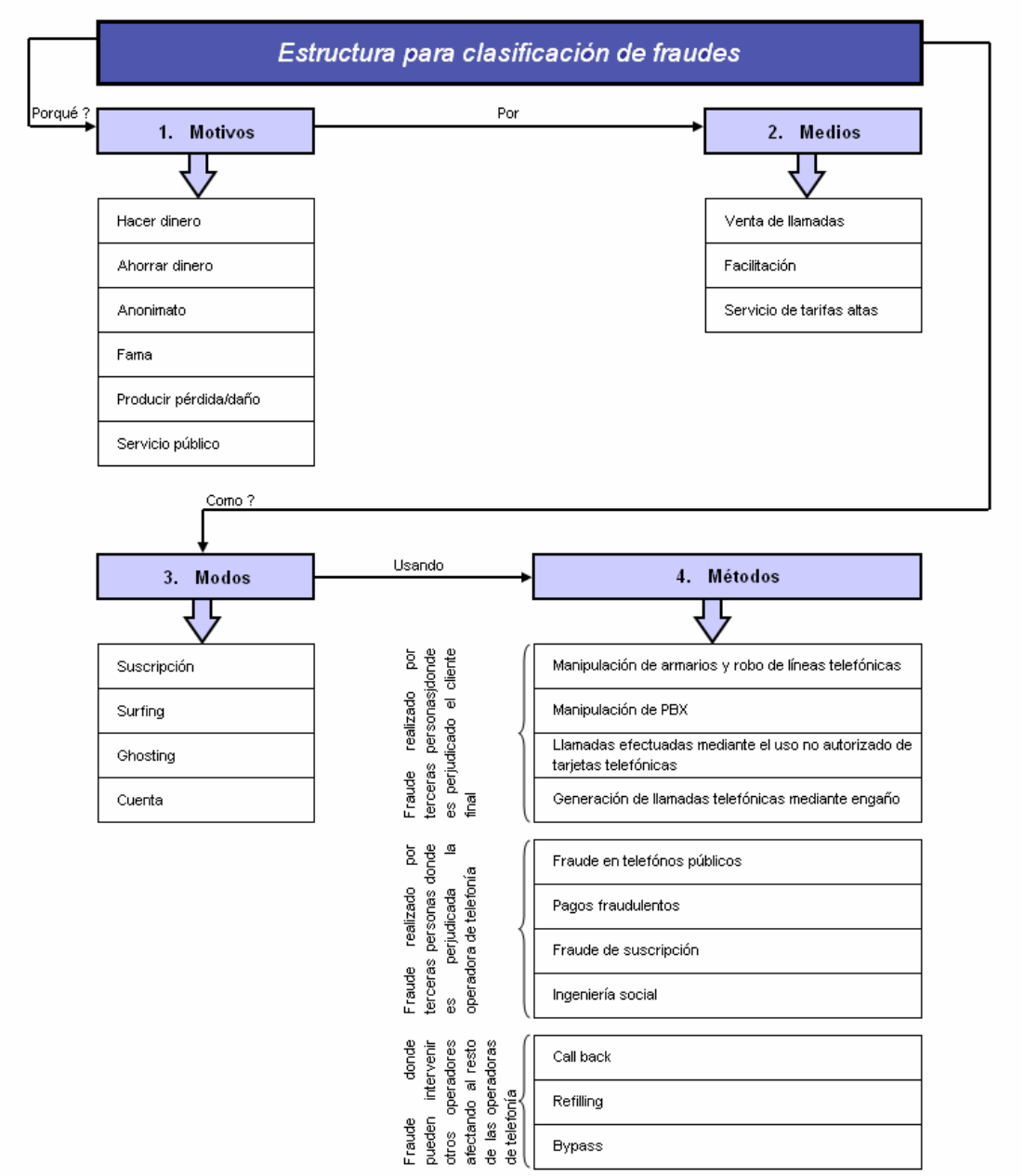


Tabla 2.2. Estructura detallada para clasificación de fraudes

2.1.1 MOTIVOS

El motivo es la razón básica del por qué el defraudador lleva a cabo un fraude, los aspectos que se consideran son:

- El motivo ayuda a entender por qué se comete el fraude.
- Ataques de fraudes específicos cambiarán con la tecnología, pero no así el motivo de fondo.
- Los procesos y contramedidas cambian con la motivación.

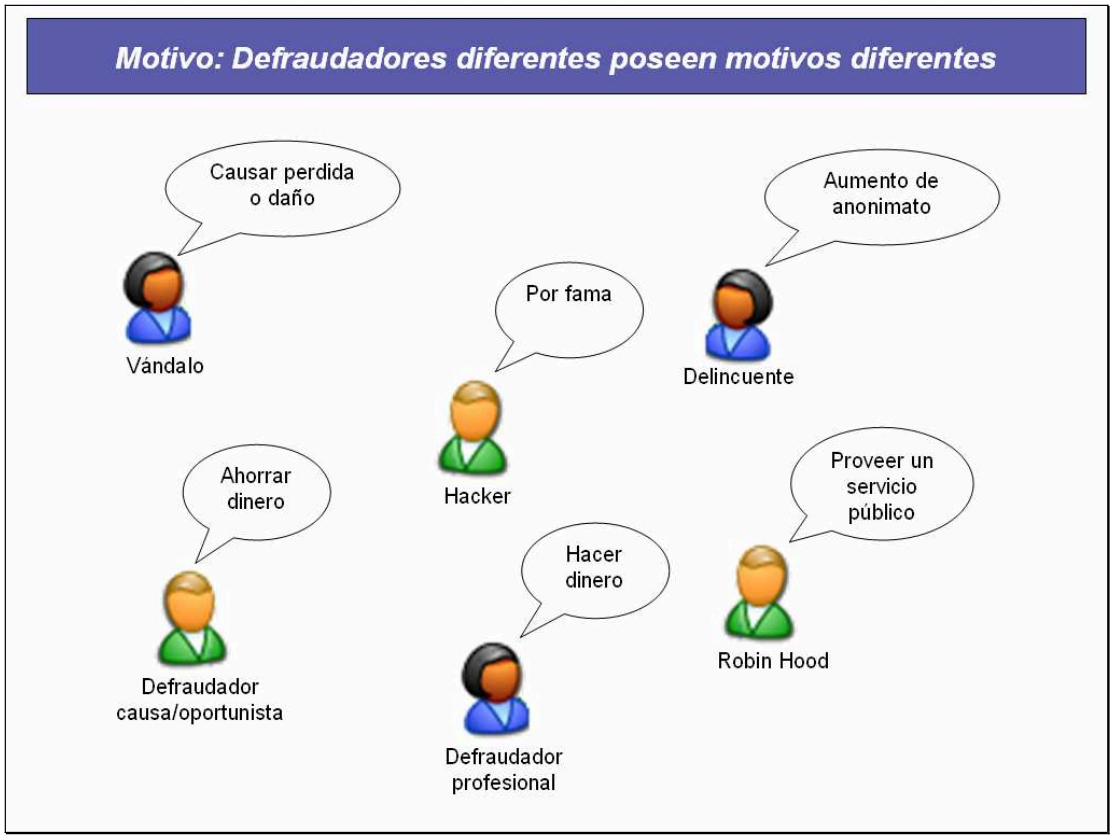


Figura 2.1. Defraudadores diferentes poseen motivos diferentes

2.1.2 MEDIOS

Herramientas que sirven para desarrollar y efectuar el fraude.

2.1.2.1 Venta de llamadas

Consiste en la venta de llamadas de alto valor (normalmente internacionales) por debajo de su valor de mercado con la intención de evadir el pago por las llamadas vendidas. Entre las razones de existencia de la venta de llamadas se tiene:

- Condiciones políticas y sociales en los países de destino.
- Grandes diferencias de tarifas internacionales entre los países.
- Imposibilidad de efectuar llamadas entre dos países (dificultades técnicas).

2.1.2.2 Facilitación

Consiste en promover o incentivar actividades fraudulentas entregando productos, métodos, o información, generalmente a cambio de ciertas compensaciones. Algunos de los aspectos a considerarse son:

- A menudo se realiza por funcionarios internos, a cambio de una compensación económica.
- Usualmente se lo realiza sin esperar compensación económica, como en el caso de favorecer a amigos, colegas, familia.
- Al mantener las actividades fraudulentas de una manera organizada, estas pueden pasar desapercibidas, implicando pérdidas masivas.

2.1.2.3 Servicio de tarifas altas

Consiste en el aumento deshonesto de tarifas económicas que el proveedor de servicios recibe de sus usuarios, es decir, el usuario se ve afectado por pagar costos excesivos sin embargo lo hace por necesitar los servicios. Los servicios de telecomunicaciones usualmente requeridos por los usuarios son: telefonía local alámbrica, telefonía local inalámbrica, telefonía de larga distancia internacional, telefonía pública, telefonía celular, servicio de transmisión de datos, voz sobre IP.

Entre los indicadores de fraude por servicio de tarifas altas se tiene:

- Llamadas fuera del promedio de duración, lo que indica que el servicio está siendo ocupado por distintos usuarios con fines diferentes.
- Múltiples llamadas de duración corta y con el mismo patrón (Puede indicar el uso de equipos de auto discado).

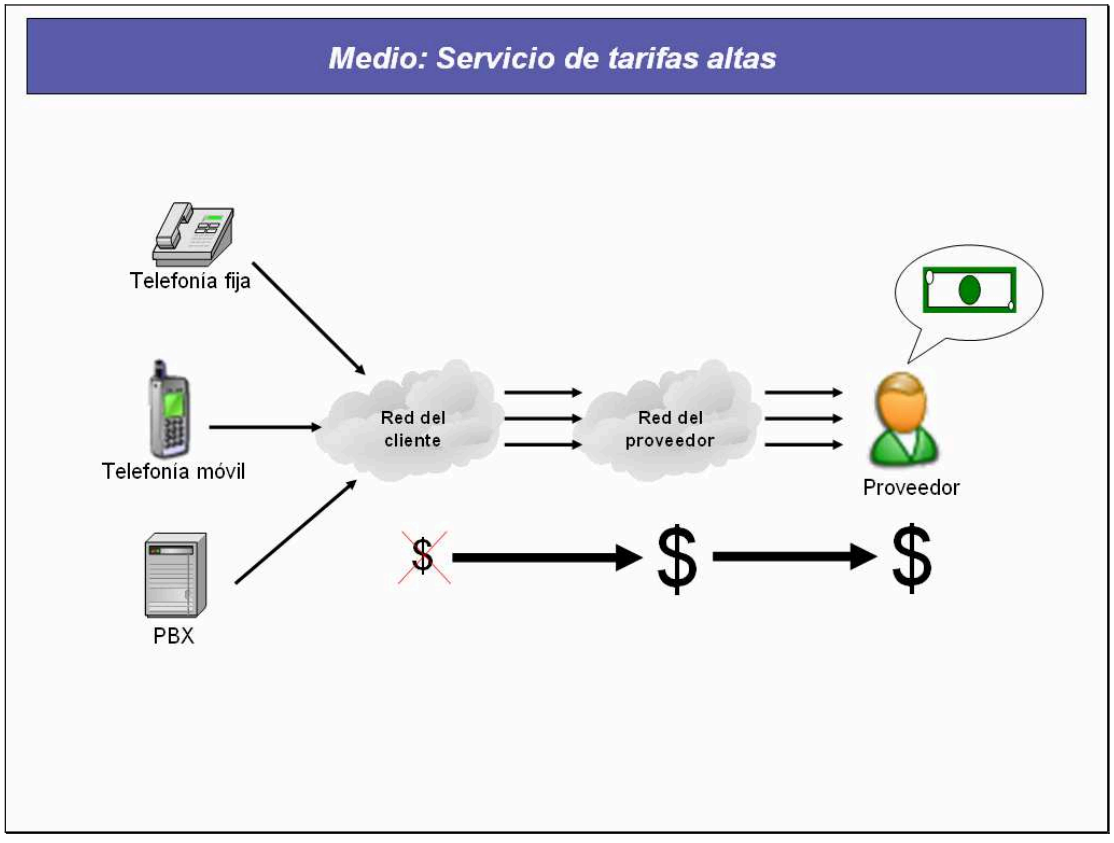


Figura 2.2. Servicio de tarifas altas

2.1.3 MODOS

Es la clasificación genérica de cómo un defraudador realiza un fraude.

2.1.3.1 Suscripción

Fraude de suscripción, consiste en la solicitud de nuevas líneas y/o nuevos servicios mediante identidad inventada no existente en la realidad y/o utilizando la identidad de un tercero sin su consentimiento o autorización.

2.1.3.2 Surfing

Fraude de surfing, consiste en el uso de una cuenta o servicio de otra persona sin su consentimiento o autorización.

Indicadores de fraude surfing.

- No existe fraude de surfing sin el riesgo de una pérdida financiera y una perdida de clientes. Entre algunas de las anomalías que se observan son: llamadas extrañas, horario, origen / destino, frecuencia, duración, uso de otros servicios, comportamiento de la red.

- La empresa operadora debiera identificar el fraude antes que el cliente lo haga. Entre algunas de las anomalías que se observan son: facturas relativamente altas, uso de llamadas gratuitas, bloqueo de acceso, reclamo de llamadas / facturas, problemas con atención a clientes.

2.1.3.3 Ghosting

Fraude de ghosting, consiste en la manipulación de la red o de los sistemas de modo que afectan la producción, procesamiento o valor de los CDR`s activando cuentas no facturables.

Indicadores de fraude ghosting.

- El fraude de ghosting es difícil de detectar directamente. Entre algunas de las anomalías que se observan son: número de clientes activos en la central y en facturación, CDR`s generados contra CDR`s cobrados.

- Puede requerir un análisis detallado para descubrir indicadores indirectos. Entre algunas de las anomalías a observar son: facturas con valor cero, login`s de acceso, abuso de autoridad.

2.1.3.4 Cuenta

Cada elemento del comportamiento del cliente es un indicativo de un fraude potencial.

Indicadores de fraude de cuenta.

- Los indicadores pueden ser internos o externos. El fraude en las cuentas si es un problema interno, normalmente es difícil de detectar.

  Internos: abuso de autoridad, falta de documentación, reembolso y ajustes, falta de pagos en otras cuentas.

  Externos: aumento / persistencia en los reclamos, reembolsos y ajustes.

2.1.4 MÉTODOS

Es el detalle de cómo un defraudador realiza un fraude, los aspectos que se consideran respecto al tipo de método utilizado son:

- Varía de acuerdo al motivo, modo y el medio.
- Defraudadores sofisticados combinan productos y servicios para optimizar el éxito del fraude.
- Estos pueden ser extendidos a otras operadoras y redes.
- Define las vulnerabilidades y métodos a través de la evaluación del riesgo.
- El defraudador se esforzará en aumentar los beneficios del fraude.

Los métodos se los ha clasificado de acuerdo al perjuicio que causan:

- ↗ Fraude realizado por terceras personas donde es perjudicado el cliente final.
- ↗ Fraude realizado por terceras personas donde es perjudicada la operadora de telefonía.
- ↗ Fraude donde pueden intervenir otros operadores (con y sin licencia) afectando al resto de las operadoras de telefonía.

2.1.4.1 Fraude realizado por terceras personas donde es perjudicado el cliente final

2.1.4.1.1 Manipulación de armarios y robo de líneas telefónicas

Consiste en acceder sin la correspondiente autorización a los armarios de las operadoras telefónicas para generar llamadas que finalmente serán facturadas a los clientes perjudicados, por quedar registrados sobre la línea tomada ilegalmente.

Forma ilícita de operar.

El defraudador viola las seguridades de los armarios telefónicos con la finalidad de manipular las regletas realizando conexiones no autorizadas de las líneas telefónicas que son instaladas en un local clandestino para generar llamadas ilícitas.

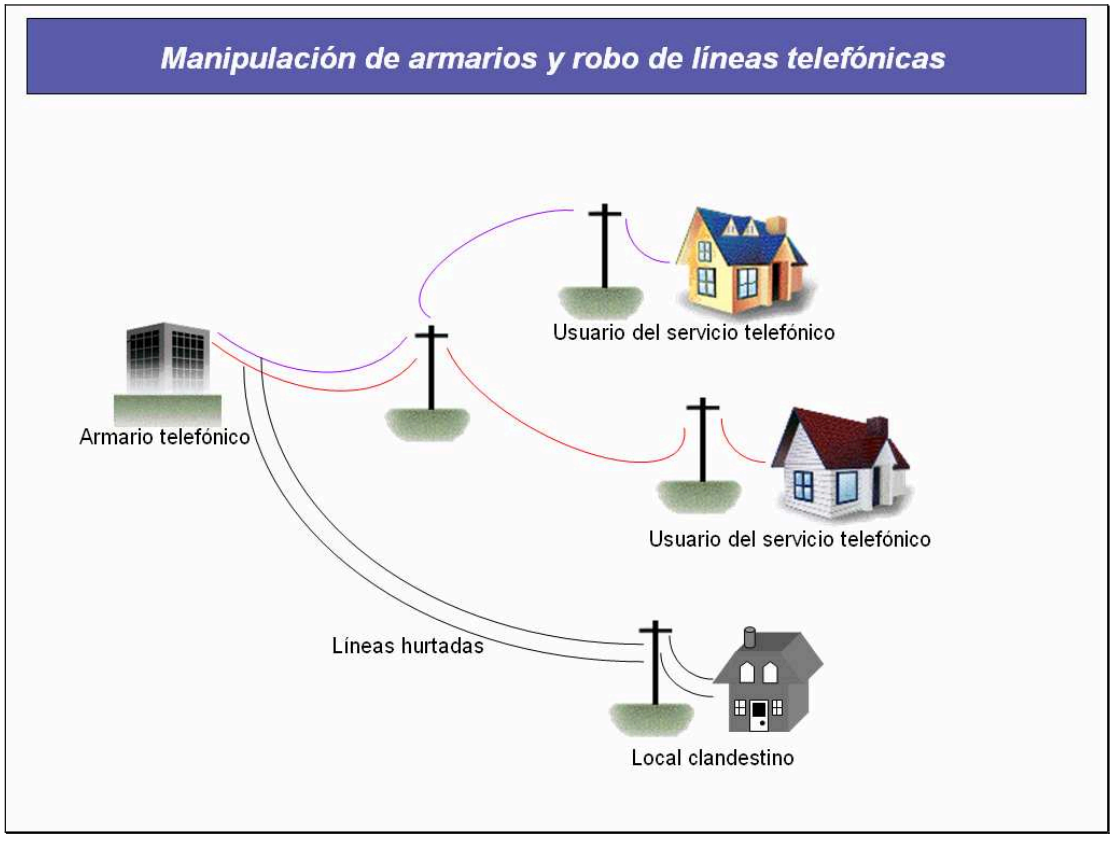


Figura 2.3. Manipulación de armarios y robo de líneas telefónicas

Forma de detección.

No se cuenta con un método específico para la detección de la manipulación de armarios y robo de líneas telefónicas, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica tiene en cuenta los cambios abruptos del comportamiento del uso de la línea telefónica en aspectos como son: facturación relativamente alta, llamadas al extranjero, horario, origen / destino, frecuencia, duración, uso de otros servicios, comportamiento de la red.

- Frente a este tipo de anomalías, el personal de planta externa de la operadora telefónica realiza una inspección al lugar en el cual está instalado el armario telefónico y mediante reconocimiento visual se constata si las regletas han sido manipuladas.

- En caso de manipulación de las regletas, mediante inspección visual del par correspondiente a las líneas telefónicas manipuladas se ubica el lugar en el cual se está haciendo uso indebido de las mismas.

- Con las pruebas del ilícito, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante la manipulación de armarios y robo de líneas telefónicas para realizar llamadas telefónicas de manera ilegal, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[1].

---

1 **ANEXO C.** Artículo 422 del Código Penal

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- Proteger con mayor seguridad los armarios telefónicos.

- Contar con dispositivos que permitan alertar a la operadora telefónica de la manipulación indebida de los armarios telefónicos.

- Los usuarios del servicio de telefonía, deben percatarse de la facturación alta y de llamadas realizadas a números telefónicos desconocidos, ya que la utilización de líneas hurtadas se hace principalmente por la noche y hacia destinos en el exterior.

2.1.4.1.2 Manipulación de PBX

Consiste en ingresar a las PBX de los clientes, empresas, instituciones, etc. accediendo en forma remota o local sin autorización, la configuración incorrecta de un PBX permite a intrusos el uso de sus facilidades para la realización de llamadas fraudulentas.

Este tipo de fraude usualmente ocurre cuando el personal que tiene acceso a las facilidades del PBX puede programar las líneas mediante un número externo y realizar llamadas cargándolas a la factura del PBX.

Forma ilícita de operar.

El defraudador a través de los puertos de mantenimiento utilizados para el acceso remoto (vía MODEM), accede y manipula la configuración del PBX para generar llamadas ilícitas.

Forma de detección.

No se cuenta con un método específico para la detección de la manipulación de PBX, sin embargo los aspectos a considerarse comúnmente son:

- La persona autorizada para el manejo y programación del PBX tiene en cuenta los cambios abruptos del comportamiento del uso de las líneas telefónicas en aspectos como son: llamadas realizadas fuera del horario de uso habitual del PBX, destinos de las llamadas telefónicas realizadas, frecuencia, duración, comportamiento de la red.

- Frente a este tipo de anomalías, la persona encargada del PBX pone en conocimiento al personal de seguridad de la institución para que se realice la inspección necesaria.

- En caso de confirmación del uso fraudulento del PBX, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante la manipulación del PBX, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[2].

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar los siguientes aspectos:

- Incorporar contraseñas para acceder al software de configuración del PBX, las mismas que deben ser conocidas únicamente por la persona autorizada para el manejo del PBX.

  En caso de la existencia de contraseñas, se las debe cambiar frecuentemente para evitar que puedan ser descubiertas fácilmente.

- Restringir los puertos de configuración del PBX para que tenga acceso solo la persona autorizada para el manejo del PBX.

- Incorporar dispositivos de alerta del uso indebido del PBX a través de un sistema de alarma, redes neuronales, que permitan realizar el monitoreo considerando parámetros como son el tráfico telefónico, los número a los cuales se realizan llamadas, etc.

---

2 **ANEXO C.** Artículo 422 del Código Penal.

2.1.4.1.3 Llamadas efectuadas mediante el uso no autorizado de tarjetas telefónicas

Consiste en el uso indebido, sin consentimiento del titular, de los códigos de las tarjetas telefónicas y/o tarjetas de telefonía pública para la realización de llamadas fraudulentas.

El fraude es cometido utilizando tarjetas de llamada pre pago, post pago, y/o tarjetas de telefonía pública, es por eso necesario que los procesos de configuración y aprovisionamiento de la tarjeta, así como su utilización segura deban ser tomados en cuenta constantemente por los proveedores y sus usuarios.

Figura 2.4. Tipos de tarjetas telefónicas

Forma ilícita de operar.

El defraudador viola y/o genera los códigos de las tarjetas telefónicas y/o hurta tarjetas de telefonía pública para realizar llamadas ilícitas.

Forma de detección.

No se cuenta con un método específico para la detección del uso indebido de tarjetas telefónicas, sin embargo los aspectos a considerarse comúnmente son:

- La persona propietaria de las tarjetas telefónicas debe tener en cuenta los cambios abruptos en aspectos como son: llamadas realizadas fuera del horario de uso habitual, destinos de las llamadas telefónicas realizadas, frecuencia, duración.

- Frente a este tipo de anomalías, la persona afectada pone en conocimiento a las autoridades correspondientes para que se realice la inspección necesaria.

- En caso de confirmación del uso no autorizado de las tarjetas telefónicas, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante el uso no autorizado de tarjetas telefónicas, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[3].

---

3 **ANEXO C.** Artículo 422 del Código Penal

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- El usuario de las tarjetas telefónicas debe evitar dar los códigos, ya que en posteriores ocasiones se podría abusar de los mismos y cargar el costo de las llamadas realizadas al titular de las tarjetas telefónicas.

- El usuario de las tarjetas telefónicas debe evitar dejarlas abandonadas ya que el defraudador podría fácilmente copiar el código y/o hurtarlas para hacer uso indebido de la tarjeta.

2.1.4.1.4 Generación de llamadas telefónicas mediante engaño

Consiste en generar llamadas hacia determinados destinos, generalmente internacionales, mediante procedimientos engañosos que no le son aclarados debidamente al usuario, el cual desconoce el monto que le será facturado posteriormente.

Forma ilícita de operar.

El defraudador publica propaganda por medio de avisos en los cuales se indica la prestación de varios servicios vía telefónica como son horóscopos, chistes, llamadas eróticas, etc. Generalmente el defraudador ofrece los servicios sin estar legalmente facultado para operar.

En la propaganda no se especifica el precio a pagarse por realizar la llamada telefónica y solicitar algún servicio. Provocando que el usuario realice llamadas que posteriormente serán facturadas a precios altos.

Forma de detección.

No se cuenta con un método específico para la detección de llamadas realizadas por engaño, sin embargo los aspectos a considerarse comúnmente son:

- El usuario engañado tiene en cuenta los cambios abruptos en la facturación de las llamadas telefónicas, en la cual constata el cobro injusto por la utilización de los servicios ilegales.

- Frente a este tipo de anomalías, el usuario afectado pone en conocimiento a las autoridades correspondientes para que se realice la inspección necesaria.

- En caso de confirmar que se ofrece los servicios sin estar legalmente facultados para operar, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante la generación de llamadas telefónicas mediante engaño, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[4].

---

4 **ANEXO C.** Artículo 422 del Código Penal

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- El usuario antes de acceder a los distintos tipos de servicios vía telefónica debe percatarse del costo y el lugar de destino de la llamada telefónica, ya que la llamada está siendo originada por el usuario y en caso de que los servicios a los cuales a accedido tengan permiso para operar, la perdida económica perjudica directamente al usuario.

- Generalmente quienes hacen uso de este tipo de servicio vía telefónica son aquellas personas que permanecen gran parte del día en el hogar, como es el caso de los empleados, más no por el usuario al que se encuentra registrada la línea telefónica.

  Por esta razón es conveniente bloquear la línea telefónica y disponer de códigos de seguridad para realizar llamadas, los códigos deben ser de conocimiento solo del usuario propietario de la línea telefónica.

- El ente regulador puede conocer de los avisos publicados en la prensa, que ofrecen estos servicios.

2.1.4.2 Fraude realizado por terceras personas donde es perjudicada la operadora de telefonía

2.1.4.2.1 Fraude en teléfonos públicos

Consiste en dañar y/o alterar técnicamente y/o eludir los controles de los equipos provistos por las compañías telefónicas, evitando el pago de las llamadas generadas.

Figura 2.5. Teléfonos públicos de varias operadoras telefónicas

Forma ilícita de operar (caso 1: Manipulación de teléfonos públicos.)

Desde un teléfono público al marcar una combinación de números que representan códigos se puede acceder a la configuración del teléfono, los códigos son de conocimiento único de los técnicos de la empresa telefónica; sin embargo, el defraudador, al llegar a conseguir los códigos, manipula el teléfono público provocando su desconfiguración permitiéndole realizar llamadas fraudulentas.

Al tratarse de un teléfono público que funciona con monedas, el defraudador simula el pago de la llamada realizada ya sea con el uso de monedas falsas o extranjeras, también comete fraude saqueando el teléfono y robando las monedas.

Al tratarse de un teléfono público que funciona con tarjeta, el defraudador adultera las tarjetas telefónicas con el objetivo de recargar el saldo y poder realizar llamadas fraudulentas.

Forma ilícita de operar (caso 2: Boxing.)

Técnica utilizada para obtener llamadas gratuitas o a valores reducidos, este tipo de fraude se comete mediante la utilización de un dispositivo generador de tonos de frecuencia para simular las frecuencias que se generan en la central telefónica.

- “Red box”: Caja roja. Produce un tono similar al emitido con el uso de monedas en teléfonos públicos para evitar cobros.

- “Black box”: Caja negra. Envía señal/tono indicando que la llamada no fue atendida para evitar cobros.

- “Blue box”: Caja azul. Manipulación de la señal “in - band” para reducir costos de las llamadas.

  Al realizarse una llamada local desde el teléfono público y mientras el teléfono destino esta timbrando se opera el mecanismo lo que provoca la desconexión del timbrado en el teléfono destino, dejando al usuario (defraudador) del teléfono público conectado a la red, el cual puede generar llamadas de larga distancia que serán facturadas como llamadas locales.

Forma de detección.

No se cuenta con un método específico para la detección de la manipulación de teléfonos públicos, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica tiene en cuenta los cambios abruptos en el uso de teléfonos públicos en aspectos como son: llamadas de larga duración realizadas frecuentemente al exterior, horario en el que se realiza las llamadas, uso de otros servicios, comportamiento de la red.

- Frente a este tipo de anomalías, el personal de planta externa de la operadora telefónica realiza una inspección al lugar en el cual está instalado el teléfono público y mediante reconocimiento visual se constata si el teléfono ha sido manipulado.

- En caso de manipulación del teléfono público, la operadora telefónica pone en conocimiento de la anomalía a las autoridades pertinentes para que se realice la investigación necesaria y poder dar con el defraudador.

- Debido a que para realizar la investigación, las autoridades deben estar constantemente observando el comportamiento de los usuarios del teléfono público para poder determinar quien es el defraudador, el proceso para la detección puede tardar un tiempo considerable.

- Con las pruebas del ilícito y reconocido al defraudador, se procede a imponer las sanciones respectivas.

Herramientas correctivas.

Como herramienta correctiva ante la manipulación de teléfonos públicos para realizar llamadas telefónicas de manera ilegal, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[5].

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- Proteger con mayor seguridad los teléfonos públicos.

- Contar con dispositivos que permitan alertar a la operadora telefónica de la manipulación indebida de los teléfonos públicos.

- La operadora telefónica debe Incorporar dispositivos de alerta de la generación de llamadas fraudulentas a través de un sistema de redes neuronales, que permita realizar el monitoreo considerando parámetros como son el tráfico telefónico, los número a los cuales se realizan llamadas, duración de las llamadas, horario de uso del teléfono público, etc.

---

5 **ANEXO C.** Artículo 422 del Código Penal

2.1.4.2.2 Pagos fraudulentos

Consiste en efectuar pagos fraudulentos de facturas y/o consumos telefónicos correspondientes a las llamadas telefónicas realizadas por el defraudador.

Forma ilícita de operar.

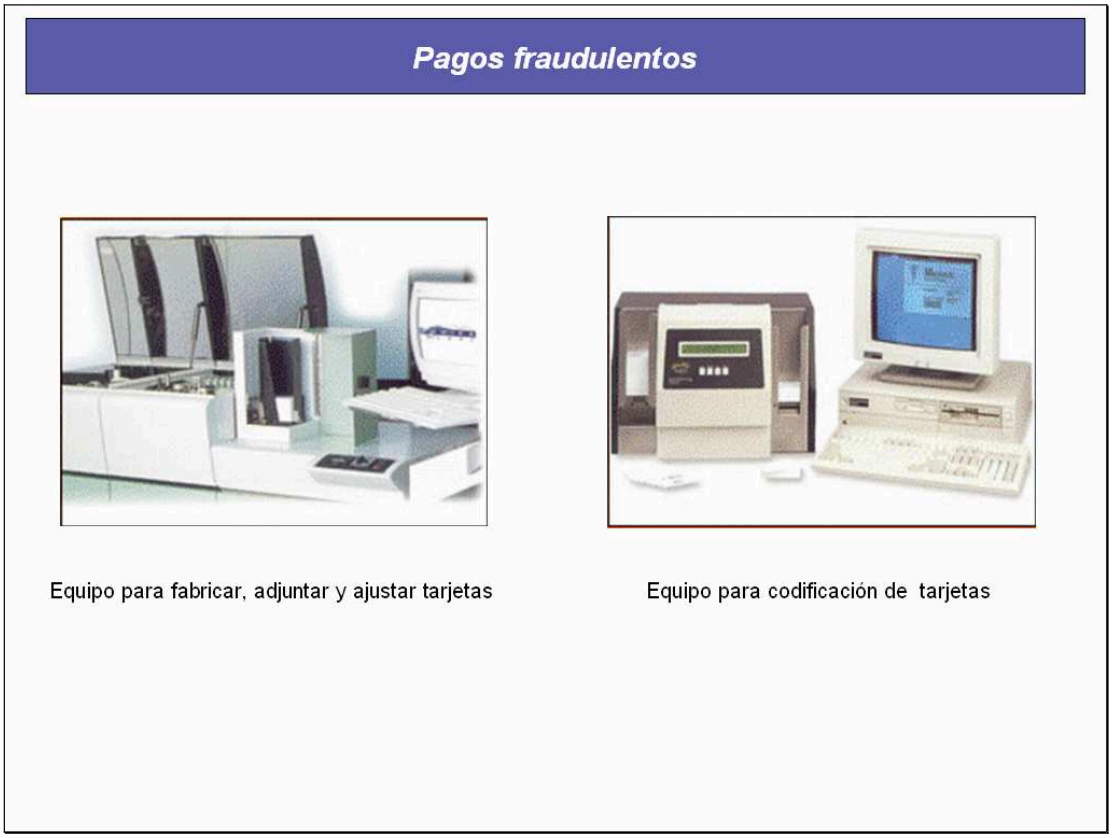
El defraudador mediante tarjetas de crédito o débito que han sido robadas, duplicadas o adulteradas y cheques robados o adulterados realiza el pago de las facturas telefónicas.

Dándose dos tipos de casos:

- El perjudicado es la operadora telefónica, cuando las tarjetas de crédito y/o cheques han sido adulterados para realizar el pago de las facturas telefónicas.

- El perjudicado es el propietario de las tarjetas de crédito y/o cheques, cuando dichos documentos han sido robados para realizar el pago de las facturas telefónicas.

En Internet se puede encontrar varios proveedores de equipos para fabricar tarjetas de crédito, equipos que generalmente se los adquiere mediante pedido vía correo electrónico (e-mail).



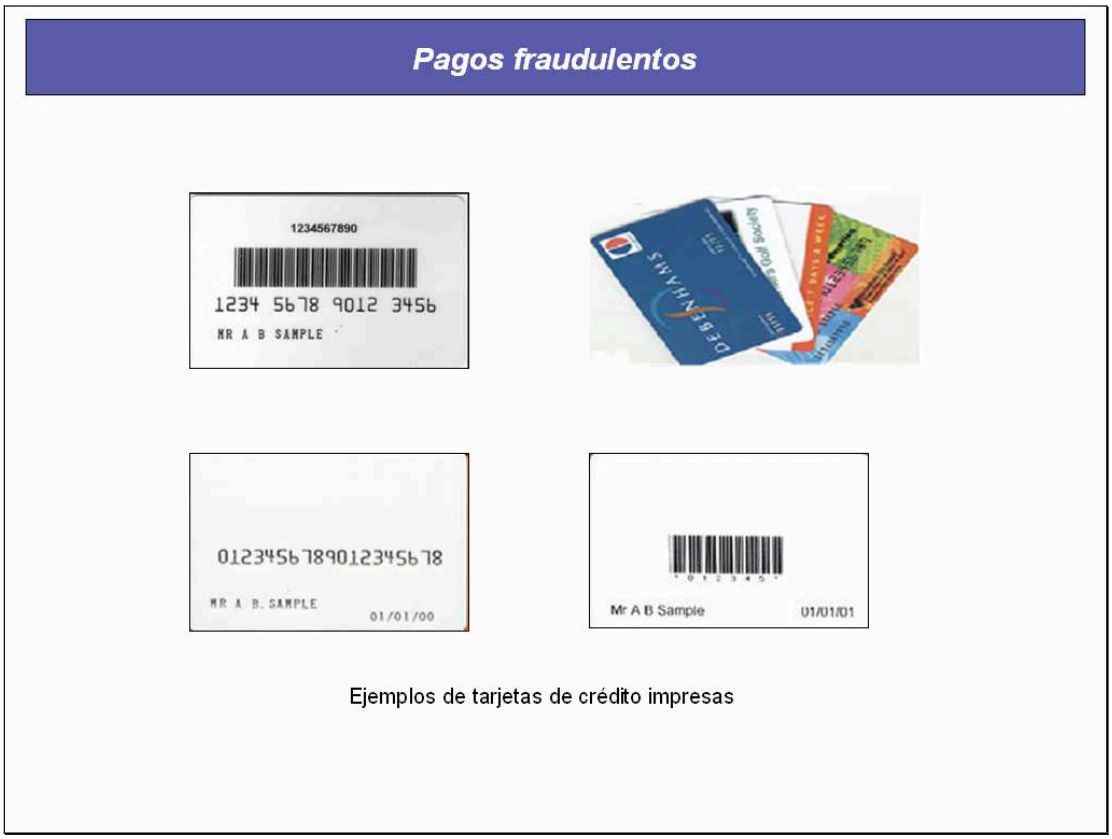


Figura 2.6. Equipos para fabricar tarjetas de crédito y ejemplos [30]

Forma de detección.

No se cuenta con un método específico para la detección de pagos fraudulentos, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica tiene en cuenta los antecedentes del uso del servicio por parte del usuario, en el cual se observa el cumplimiento o no del pago de las facturas telefónicas, al presentarse un patrón anormal en dicho aspecto la operadora telefónica pone en conocimiento a las autoridades correspondientes para que se realice la inspección necesaria.

- Al tratarse del usuario engañado, este tiene en cuenta los cambios abruptos en la facturación de las tarjetas de crédito y/o cheques en los cuales se constata el cobro injusto por la utilización de los servicios telefónicos realizados por el defraudador.

- Frente a este tipo de anomalías, el usuario afectado pone en conocimiento a las autoridades correspondientes para que se realice la inspección necesaria.

- En caso de confirmar el uso fraudulento de las tarjetas de crédito y/o cheques, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante los pagos fraudulentos para cancelar las tarifas telefónicas, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[6].

---

6 **ANEXO C.** Artículo 422 del Código Penal

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- La operadora telefónica debe incorporar sistemas en base a redes neuronales, que permita realizar el monitoreo del tráfico telefónico y poder observar si existen o no anomalías en varios parámetros como son principalmente, los números a los cuales se realizan llamadas, duración de las llamadas, horario de uso del teléfono público,

- El usuario de las tarjetas de crédito y/o cheques debe evitar dejarlos abandonadas ya que el defraudador podría robarlos y hacer uso indebido de los mismos.

2.1.4.2.3 Fraude de suscripción

Consiste en la solicitud de nuevas líneas telefónicas y/o nuevos servicios de telecomunicaciones utilizando identidad inventada no existente en la realidad y/o utilizando la identidad de un tercero sin su consentimiento o autorización para la realización de llamadas fraudulentas y evitar cancelar la factura telefónica.

Esta es la modalidad de fraude más común en la telefonía, tanto fija como móvil, debido a la facilidad para utilizar los documentos o falsificarlos.

Forma ilícita de operar.

El defraudador solicita los servicios de telecomunicaciones utilizando información que no corresponde realmente a sus datos personales con la intención de realizar llamadas fraudulentas y no cancelar la factura telefónica.

Dándose dos tipos de casos:

- El perjudicado es la operadora telefónica, cuando la solicitud de nuevas líneas telefónicas y/o nuevos servicios de telecomunicaciones ha sido realizado utilizando identidad inventada.

- El perjudicado es la persona a quien corresponde los datos proporcionados por el defraudador para la solicitud de nuevas líneas telefónicas y/o nuevos servicios de telecomunicaciones.

Forma de detección.

No se cuenta con un método específico para la detección del fraude de suscripción, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica tiene en cuenta los antecedentes del uso del servicio por parte del usuario, en el cual se observa el incumplimiento del pago de las facturas telefónicas, al presentarse dicha anomalía la operadora telefónica pone en conocimiento a las autoridades correspondientes para que se realice la inspección necesaria.

- Al tratarse de la persona a quien corresponde los datos proporcionados por el defraudador, este tiene en cuenta los cambios abruptos en la facturación de las llamadas telefónicas, en la cual se constata el costo injusto por la utilización de los servicios de telecomunicaciones.

- Frente a este tipo de anomalías, la persona afectada pone en conocimiento a las autoridades correspondientes para que se realice la inspección necesaria.

- En caso de confirmar el uso fraudulento de los servicios de telecomunicaciones utilizando identidad inventada no existente en la realidad y/o utilizando la identidad de un tercero sin su consentimiento o autorización, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante el fraude de suscripción para evitar cancelar las tarifas telefónicas, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[7].

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- Antes de proporcionar nuevas líneas telefónicas y/o nuevos servicios de telecomunicaciones, la operadora telefónica debe:
  - Agotar todos los recursos de análisis antes de entrar en contacto con el cliente, por ejemplo verificar listas negras, otros teléfonos, agencias de crédito, etc.
  - Abordar con preguntas que sólo el defraudador no podría responder.

- Antes de proporcionar nuevas líneas telefónicas y/o nuevos servicios de telecomunicaciones, se debe confirmar los datos del usuario quien ha solicitado los servicios, mediante inspecciones realizadas por el personal correspondiente de la operadora telefónica.

---

7 **ANEXO C.** Artículo 422 del Código Penal

2.1.4.2.4 Ingeniería social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían, convirtiéndose quizás en el método de ataque más sencillo, menos peligroso para el atacante y uno de los más efectivos.

El atacante, defraudador, puede aprovechar el desconocimiento de mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema que se maneja en la operadora telefónica para poder engañarlas en beneficio propio.

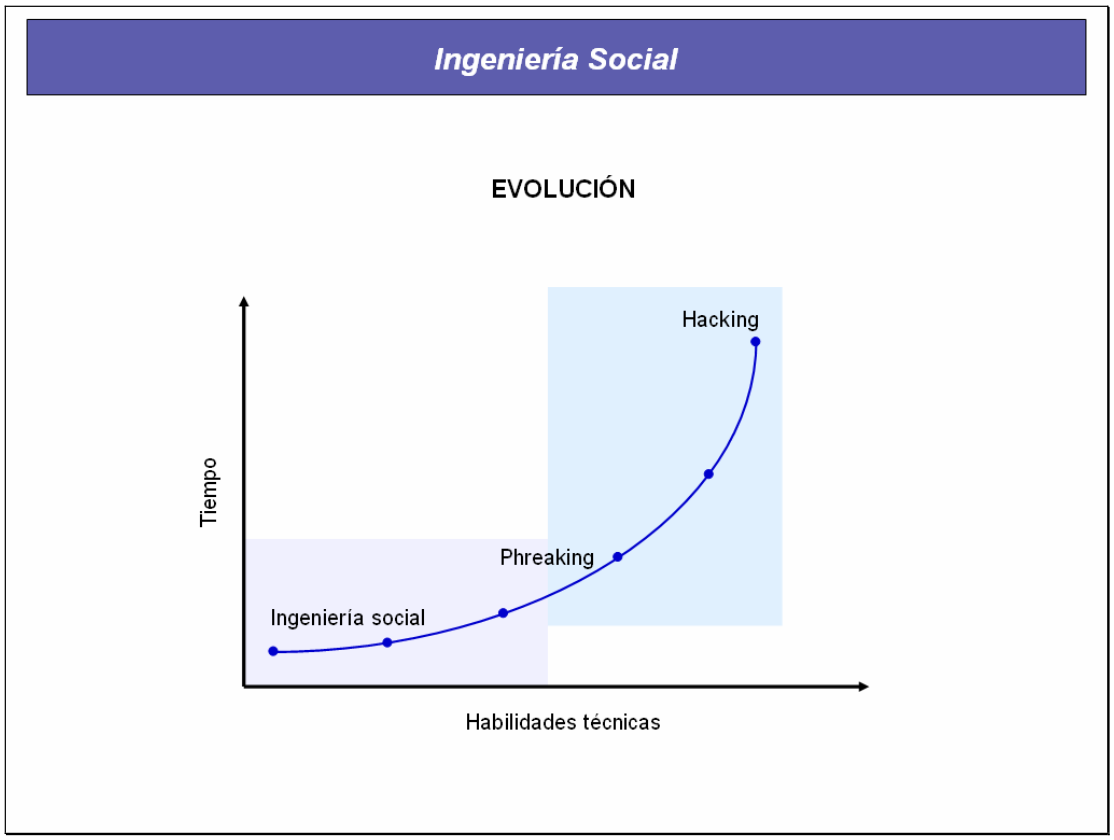


Figura 2.7. Evolución de la Ingeniería social[8]

8 FML SECURING BUSINESS, Curso: Detección, Control y Gestión del Fraude en Telecomunicaciones, 2005.

Principales características de la ingeniería social:

- Es complemento al phreaking y hacking.
- Truco planificado para obtener información, como son:
  - Manuales.
  - Disquetes
  - Memos
  - Procedimientos.
- Permite ataques sofisticados.

Personas y justificaciones para practicar la ingeniería social:

- El espía y el detective: Es su trabajo.
- El Gobierno: Por seguridad de la nación.
- El timador: Su medio de vida (el dinero).
- El hacker: Por curiosidad.

Forma ilícita de operar.

- El ingeniero social usualmente habla en un lenguaje técnico, lo que permite confundir a la gente, la cual entiende una parte o nada de la conversación respondiendo siempre que si.

- El ingeniero social usualmente realiza encuestas inocentes a los familiares de las victimas, edades, nombres, etc.

- El ingeniero social usualmente envía ofertas increíbles vía mail (ahí se introduce el troyano).

- Un ingeniero social, defraudador, usa comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos.

- Los ingenieros sociales utilizan una serie de tretas, artimañas y engaños elaborados, cuyo fin es confundir a la persona relacionada con el sistema que se maneja en la operadora telefónica o, peor todavía, lograr que comprometa seriamente la seguridad de sus sistemas.

- Los ingenieros sociales aprovechan sentimientos variados como curiosidad, la avaricia, el sexo, la compasión o el miedo, lo que permite conocer todo acerca de la víctima y poder predecir como actuará frente a determinados estímulos.

- De esta forma se consigue el objetivo de obtener información de otra persona sin que esta se percate que esta revelando información sensible, lo que permite poder acceder y manipular el sistema que utiliza la operadora telefónica.

Forma de detección.

No se cuenta con un método específico para la detección del fraude de ingeniería social, sin embargo los aspectos a considerarse comúnmente son:

- La persona autorizada para manejar el sistema debe tener en cuenta los cambios abruptos en ciertos parámetros como son la facturación de las llamadas telefónicas, el tráfico telefónico generado, etc.

- Al presentarse anomalías en alguno de los parámetros, la persona autorizada pone en conocimiento de las autoridades correspondientes para que se realice la inspección necesaria.

- En caso de confirmar que se está cometiendo fraude al manipular la información registrada en el sistema que utiliza la operadora telefónica, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante el fraude de ingeniería social para acceder y manipular el sistema que utiliza la operadora telefónica, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[9].

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- Capacitar al personal que trabaja en la operadora telefónica, desde los operarios hasta el personal de limpieza, para que sepan identificar un ataque por parte de un ingeniero social.

- Analizar con antivirus todos los correos que reciba la operadora telefónica.

- El personal que trabaja en la operadora telefónica no debe informar telefónicamente las características técnicas de la red, ni nombre de personal a cargo, etc.

- Se debe realizar un control de acceso físico al sitio donde se encuentra los ordenadores e implementar y/o fortalecer políticas de seguridad a nivel de Sistema Operativo.

---

9 **ANEXO C.** Artículo 422 del Código Penal

2.1.4.3 Fraude donde pueden intervenir otros operadores (con y sin licencia) afectando al resto de las operadoras de telefonía

En estos tipos de fraude se enruta de manera ilícita el tráfico telefónico internacional evitando usar o usando de manera indebida las centrales legalmente establecidas que conforman la red telefónica.

El tráfico de llamadas entrantes al Ecuador es aproximadamente 8 veces mayor que el de las llamadas salientes y en este mismo sentido se comete el ilícito [10] al cursar tráfico telefónico internacional mediante modalidades fraudulentas como son principalmente el Call back, Refilling y By pass. A continuación se indica el proceso normal e ilícito de establecimiento de una llamada telefónica a clonar.

2.1.4.3.1 Llamada telefónica internacional normal

El proceso de establecimiento de una llamada telefónica internacional normal se lo realiza a través de la red pública de telefonía, la cual es compartida entre muchos usuarios, y cualquier usuario puede establecer comunicación con cualquier otro usuario, incluyendo servicios de larga distancia.

La red pública de telefonía se encarga de cursar el tráfico telefónico, principal fuente de ingresos de una operadora de telefonía fija, lo cual exige mantener un alto nivel de disponibilidad de la red. Para conseguirlo se debe cuidar el ámbito operativo (detectar y corregir los problemas que pueden estar ocurriendo en la red: congestión, baja calidad, cortes, fraude, etc.) y la planificación de la red (adecuado dimensionamiento de los elementos que la componen).

---

10 Revista trimestral CIEEPI, Publicación: 07/24/2003.

Para conocer el estado de la red de telefonía se hace uso de la información de las centrales telefónicas que la componen; la tecnología digital de las centrales telefónicas permite recoger internamente información de su estado y ponerla a disposición de sistemas externos.

La información obtenida de las centrales telefónicas que forman la red de telefonía refleja datos como el número de intentos de llamada, las llamadas completadas, las llamadas rechazadas, las cuales permiten determinar el grado de congestión, el nivel de utilización, el porcentaje de recursos libres, entre otros.

En el análisis de la información de una central telefónica debe tenerse en cuenta que forma parte de una red de telefonía, de ahí que es importante tener conocimientos del estado de las centrales telefónicas con las que está conectada para poder ofrecer una visión de conjunto.

La integración de información de las centrales telefónicas que conforman la red de telefonía no es sencilla porque las operadoras generalmente incorporan varias centrales de diferentes suministradores, estos suministradores ofrecen para las centrales un sistema de gestión propietario que puede ser incompatible con las centrales de los demás proveedores.

La operación de la red de telefonía se basa en la información obtenida en tiempo real para actuar sobre los problemas que están ocurriendo en ese momento, la información es almacenada en una base de datos para el estudio de la evolución del tráfico.

Una red telefónica adecuadamente gestionada garantiza principalmente:

- Prestación de servicio con alta calidad.
- Detección, prevención y control de fraudes.
- Minimizar la congestión y maximizar la utilización de los recursos.
- Reducción de los costos de operación.

Para indicar el proceso normal de enrutamiento de tráfico telefónico internacional se ha tomado como ejemplo la realización de una llamada telefónica desde los Estados Unidos hacia el Ecuador.

En la figura 2.8 se indican los elementos que conforman la red telefónica, y las etapas que intervienen en el establecimiento de la llamada telefónica internacional normal.

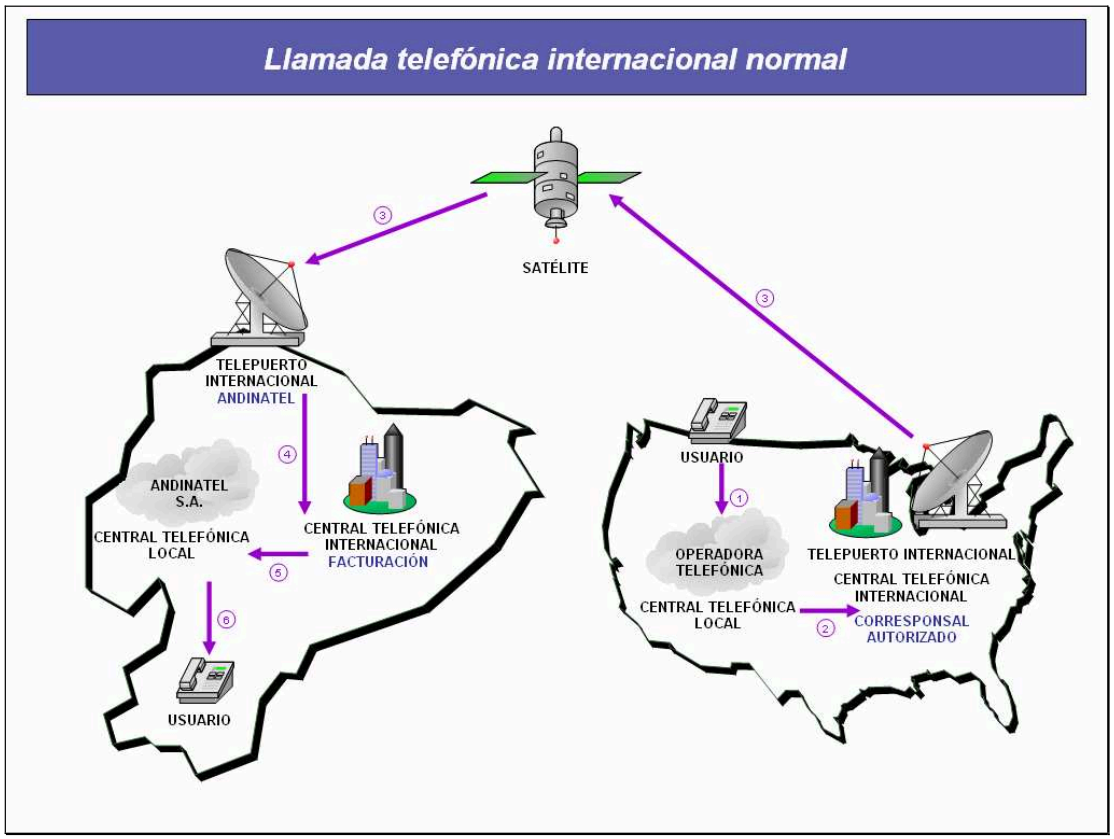
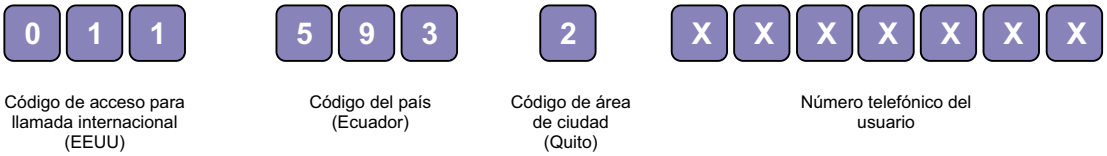


Figura 2.8. Elementos y etapas que intervienen en la llamada telefónica internacional normal

Proceso de establecimiento de la llamada telefónica internacional normal:

Etapa 1.

Desde Estados Unidos, el servicio telefónico automático permite al usuario comunicarse a través de un indicativo asignado, con diferentes países, que cuentan con marcación automática. Para realizar la llamada telefónica internacional se debe marcar el código de acceso para llamada internacional, código del país, código de área de la ciudad y el número telefónico del usuario a quien se desea realizar la llamada.



La llamada realizada ingresa a la central telefónica local legalmente establecida, la cual de acuerdo al código marcado identifica si se trata de una llamada local o internacional.

Etapa 2.

La central telefónica local recibe, procesa y enruta las llamadas, posee un conjunto de dispositivos de transporte de tráfico, etapas de conmutación, medios de control, señalización, y de otras unidades funcionales que permiten la interconexión de líneas de usuarios, circuitos de telecomunicaciones u otras unidades funcionales, tiene la habilidad de manejar un número considerable de llamadas en forma simultánea, monitorearlas y llevar registros.

La central telefónica local al identificar el código de acceso para llamada internacional enruta el tráfico hacia la central telefónica internacional legalmente establecida.

Etapa 3.

La transmisión de información vía satélite se la realiza utilizando infraestructura propia de la empresa telefónica por medio del telepuerto internacional o contratando los servicios de transmisión proporcionado por carriers.

Cada operador telefónico posee un código de identificación que se trasmite junto a la información, el cual permite al telepuerto internacional receptor reconocer datos correspondientes a tráfico telefónico y descartar cualquier otro ajeno al mismo. El enlace satelital entre los telepuertos internacionales utiliza la banda de frecuencia satelital[11] C, 6 GHz para transmisión y 4 GHz para recepción de datos.

Etapa 4.

El telepuerto internacional se encuentra situado en la superficie de la tierra y está destinado a establecer comunicación con una o varias estaciones espaciales; o, con uno o varios telepuertos de la misma naturaleza, mediante el empleo de uno o varios satélites reflectores u otros objetos situados en el espacio.

El telepuerto internacional situado en Ecuador envía el tráfico telefónico hacia la central de transito internacional legalmente establecida para que se realice la facturación y de acuerdo al código de área de la ciudad la llamada sea enrutada hacia la central local. Para efecto de la facturación se considera llamada completada únicamente las que contesta el número llamado.

Etapa 5 y 6.

La central telefónica local enruta el tráfico telefónico hacia el usuario y queda establecida la llamada telefónica internacional normal a través de la red pública de telefonía entre Estados Unidos y Ecuador.

---

11 **ANEXO D.** Banda de frecuencias satelitales

2.1.4.3.2 Call back

El Call back es un sistema, generalmente computarizado, que re-origina las llamadas, de tal forma que se tarifen y se facturen como si fueran llamadas telefónicas con origen o como si fueran hechas desde el extranjero, generalmente desde los Estados Unidos que mantiene tarifas telefónicas mucho más competitivas que los otros países.

Debido al costo menor que representa realizar las llamadas internacionales por medio de empresas que prestan el servicio de Call back en comparación a la tarifa establecida por las operadoras telefónicas legalmente establecidas, el usuario prefiere hacer uso del servicio de Call back para realizar llamadas internacionales.

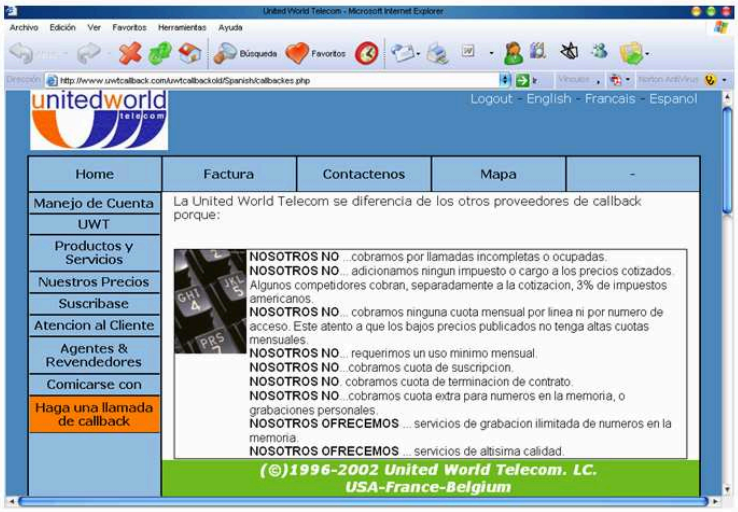
Para tener acceso al sistema se hace uso de canales o circuitos alquilados, a empresas de valor agregado con telepuertos y la red de telefonía ofreciendo un alto nivel de servicio gracias a los avances tecnológicos.

En Internet se puede encontrar varias empresas que ofrecen el servicio de llamadas telefónicas internacionales mediante sistema Call back, bastará con ingresar a la pagina de Internet y adquirir una cuenta, con la cual el usuario puede acceder al servicio de Call back desde el Internet.

Algunas de las empresas son:

- Unitedworld Telecom.
- Abacus Computer Services, Inc.
- net2secure.
- Satel.

Empresas que prestan servicio de Call Back



Empresa: Unitedworld Telecom

Dirección electrónica: http://www.uwtcallback.com/uwtcallbackold/Spanish/callbackes.php

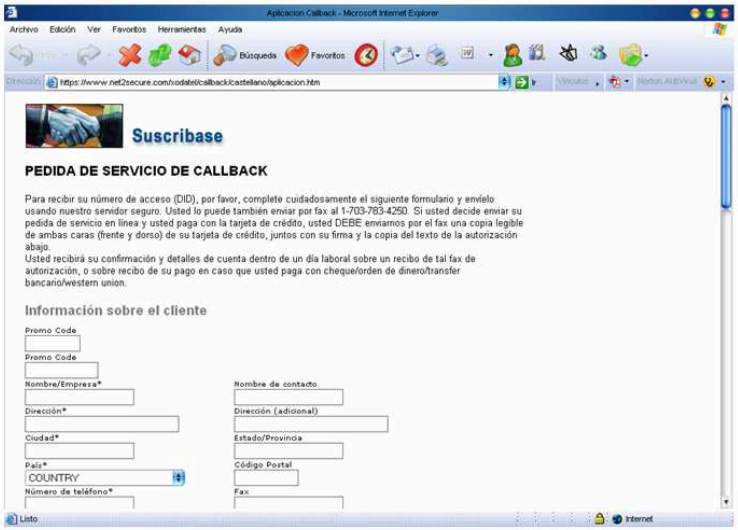
Empresas que prestan servicio de Call Back

Empresa: Abacus Computer Services, Inc.

Dirección electrónica: http://abacus-computer.net/abcb/intro.php?xlang=S&xres=1001

Figura 2.9. Páginas electrónicas de empresas que prestan servicio de Call Back

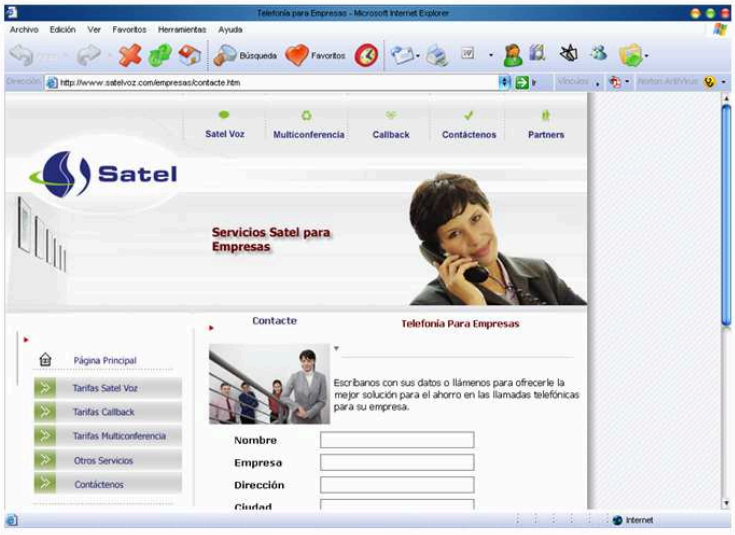
Empresas que prestan servicio de Call Back



Empresa: net2secure

Dirección electrónica:https://www.net2secure.com/xodatel/callback/castellano/aplicacion.htm

Empresas que prestan servicio de Call Back



Empresa: Satel

Dirección electrónica: http://www.satelvoz.com/empresas/contacte.htm

Figura 2.10. Cont. Páginas electrónicas de empresas que prestan servicio de Call Back

Forma de operar de la empresa Satel para la activación de llamadas internacionales mediante sistema Call back por Internet[12].

Para la activación de llamadas internacionales por Internet, no hay necesidad de configurar hardware, aplicar software ni cambiar proveedores de larga distancia. No hay costo de afiliación, ni tarifas mensuales o cargos ocultos. Los clientes pagan sólo una tarifa muy económica por minuto para las llamadas internacionales.

El servicio que se ofrece no es VoIP (Voz por Internet), sino que la llamada se establece introduciendo los teléfonos de origen y destino por Internet, pero se ejecuta sobre teléfonos fijos corrientes o celulares y de esta forma se aprovecha las tarifas telefónicas.

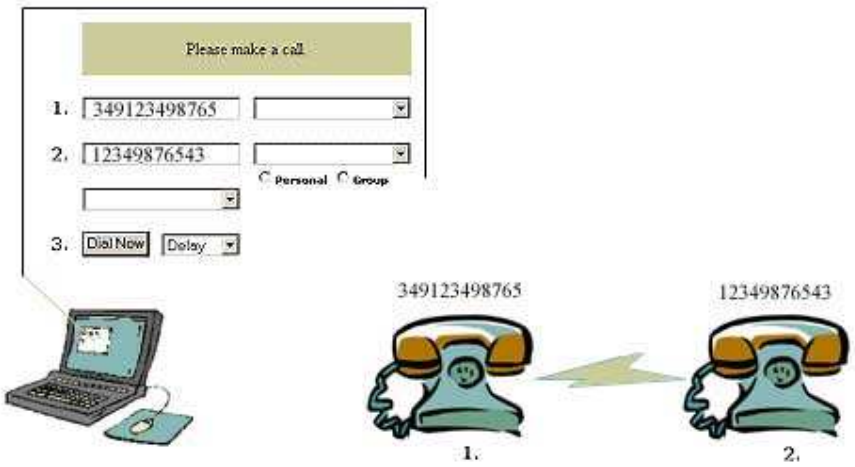


Figura 2.11. Activación de llamadas internacionales por Internet [18]

12 http://www.satelcard.com/activacion-llamada-telefonica.htm

Una vez conectado a Internet, se debe introducir el número telefónico origen (1) y el número telefónico destino (2) y pulsar el botón "Dial Now". Si el teléfono es compartido con la conexión a Internet, se podrá introducir un retardo (Delay) en la casilla correspondiente. Al pulsar "Dial Now" sonará el teléfono después del retardo que se haya introducido.

El usuario correspondiente al número telefónico origen, levanta el auricular hasta que de los tonos de llamada y contesten en el teléfono de destino.

Una vez que haya terminado la llamada, se podrá visualizar en la función billing el costo de las llamadas telefónicas realizadas, incluyendo esta última y cualquier otra función que el sistema proporcione.

Observaciones:

La forma de operar para la activación de llamadas internacionales mediante el sistema Call back por Internet no es considerada como fraude, ya que la llamada se establece introduciendo los teléfonos de origen y destino por Internet, pero se ejecuta sobre teléfonos fijos corrientes o celulares.

Forma ilícita de operar.

Empresas domiciliadas en el extranjero, generalmente en Estados Unidos, contactan a empresas nacionales que generan grandes volúmenes de tráfico internacional. Cuando un abonado en Ecuador realiza una llamada al exterior la llamada es enrutada hacia la empresa en Estados Unidos que presta el servicio de Call Back, en la cual un computador identifica y guarda el número telefónico desde el que se realizo la llamada y almacena el número telefónico destino, una vez que la persona que originó la llamada en Ecuador cuelga su teléfono recibe de vuelta una llamada internacional.

Forma de detección.

No se cuenta con un método específico para la detección del fraude de Call back, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica tiene en cuenta el comportamiento del uso de la línea telefónica en aspectos como son: facturación en la cual se detallan llamadas realizadas frecuentemente a un mismo número telefónico en el extranjero con poca duración y llamadas recibidas desde el número telefónico del exterior con larga duración, origen / destino, uso de otros servicios, comportamiento de la red.

- Al presentarse algún tipo de anomalías en los parámetros antes mencionados, el equipo antifraude de la operadora telefónica realiza las investigaciones necesarias para determinar si se está o no utilizando de manera indebida los servicios de telefonía para realizar fraude de Call back.

- En caso de confirmar el uso indebida los servicios de telefonía para realizar fraude de Call back, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante el fraude de Call back, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[13].

---

13 **ANEXO C.** Artículo 422 del Código Penal

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- La operadora telefónica debe Incorporar sistemas de alarmas que permitan realizar el monitoreo del tráfico telefónico para detectar, prevenir y evitar casos de llamadas telefónicas internacionales ilícitas realizadas mediante el sistema Call back.

- Debido a que la forma de operar para la activación de llamadas internacionales mediante el sistema Call back por Internet no es considerada como fraude, es necesario capacitar adecuadamente al personal encargado de realizar el control por parte de la operadora telefónica, para que sepa distinguir en que ocasiones se realizan llamadas telefónicas de manera ilícita.

- La Superintendencia de Telecomunicaciones en coordinación con las operadoras de telefonía, debe mantener un permanente combate a los servicios ilegales, velando para que frente a este moderno y tecnificado fraude se cuente con métodos de detección efectivos que permitan su eliminación.

2.1.4.3.2.1 Llamada telefónica internacional mediante sistema Call back

Para indicar el proceso ilícito de enrutamiento de tráfico telefónico internacional se ha tomado como ejemplo la realización de una llamada telefónica mediante sistema Call back desde Ecuador hacia Estados Unidos, teniendo en consideración que la facturación de la llamada telefónica es realizada en Estados Unidos.

En la figura 2.12 se muestran los elementos y etapas que intervienen en el establecimiento de la llamada internacional mediante sistema Call back.

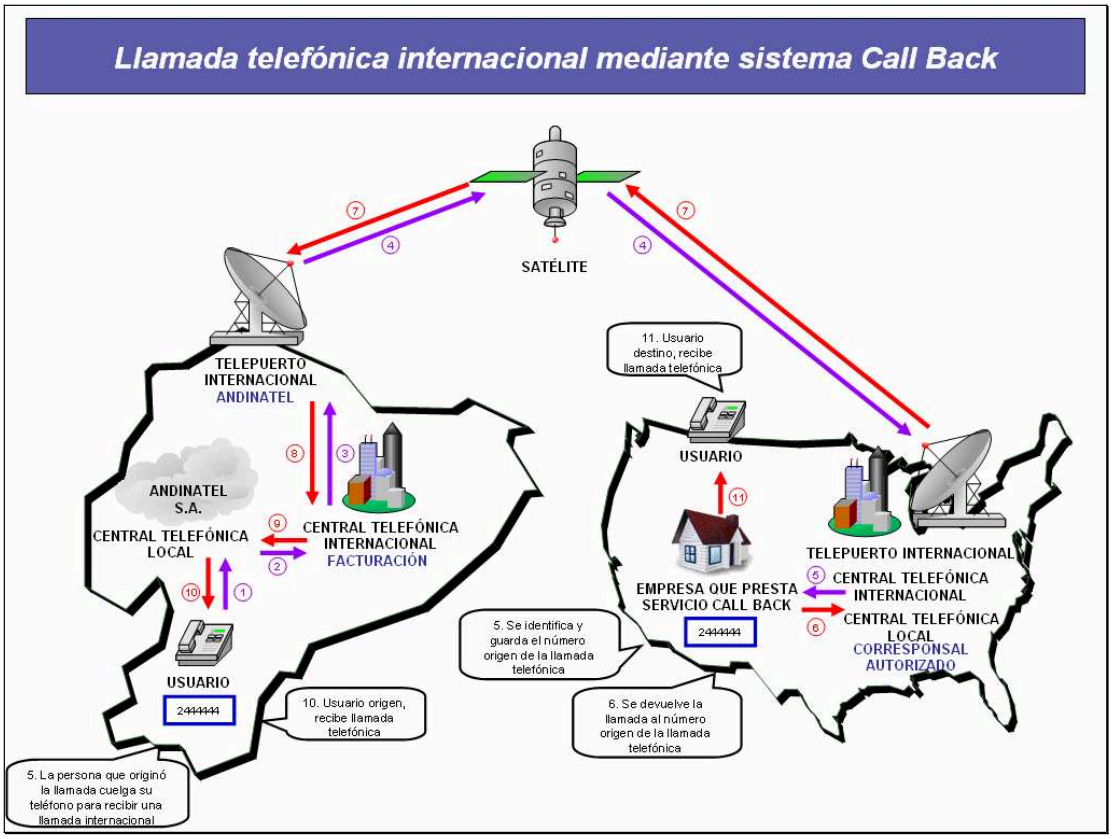
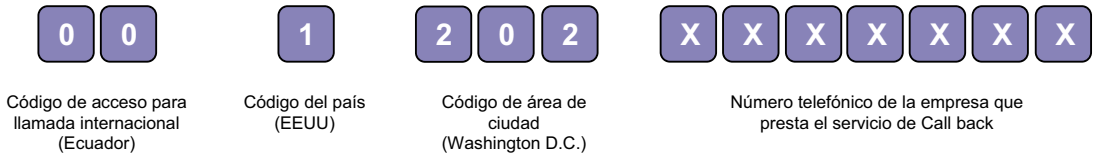


Figura 2.12. Elementos y etapas que intervienen en la llamada telefónica internacional mediante sistema Call back

Proceso de establecimiento de la llamada telefónica internacional mediante sistema Call back:

Etapa 1, 2, 3 y 4.

Desde Ecuador, para realizar la llamada telefónica internacional se debe marcar el código de acceso para llamada internacional, código del país, código de área de la ciudad y el número telefónico del usuario a quien se desea realizar la llamada, en este caso el número telefónico del usuario destino corresponde a la empresa que presta el servicio de Call back en los Estados Unidos.



El proceso de establecimiento de la llamada telefónica internacional desde Ecuador hacia Estados Unidos se realiza normalmente, hasta el momento en el que la llamada ingresa a la empresa que presta servicios de Call back.

Etapa 5.

La llamada telefónica realizada ingresa a la empresa que presta servicio de Call back, en la cual se la procesa y genera nuevamente la llamada telefónica.

Las empresas de reventa de servicios de larga distancia son quienes generalmente ofrecen realizar llamadas telefónicas internacionales a costos considerablemente bajos en comparación a los precios establecidos por las operadoras telefónicas legalmente establecidas.

Un computador es el encargado de identificar y guardar el número telefónico desde el cual se realizó la llamada, el usuario quien generó la llamada telefónica desde Ecuador escucha una grabación en la cual se le indica que marque el número telefónico de la persona a la cual se desea realizar la llamada, posteriormente se indica al usuario que cuelgue el teléfono y espere la llamada internacional.

Etapa 6.

El computador con los datos almacenados de los números telefónicos origen y destino, y teniendo en consideración que la persona que originó la llamada desde Ecuador a colgado el teléfono para esperar la llamada telefónica internacional, la computadora automáticamente realiza el discado tanto del número telefónico origen como el número telefónico destino.

Siendo Estados Unidos el país de origen de la llamada internacional hacia el destino en Ecuador.

Etapa 7, 8, 9, 10 y 11.

La empresa domiciliada en el extranjero que presta el servicio de Call back a realizado la inversión de la llamada que inicialmente tenía origen en Ecuador y destino Estados Unidos para evitar que la facturación sea realizada por la operadora telefónica en Ecuador.

Estableciéndose finalmente la llamada telefónica internacional con origen en Estados Unidos y destino Ecuador con la finalidad de que la facturación sea realizada por la operadora telefónica en Estados Unidos.

2.1.4.3.3 Refilling

Consiste en el procedimiento mediante el cual el país que origina el tráfico lo enruta a un tercer país, que no es el destino final. Ese tercer país re-enruta este tráfico hasta su último destino.

Debido a las diferencias tarifarias entre los países en el proceso, el país que origina el tráfico paga una tarifa más baja al tercero, el cual genera nuevos ingresos al obtener el tráfico adicional. Todo lo anterior a costa de menores ingresos para el país destino.

Forma ilícita de operar.

Empresas domiciliadas en el extranjero, generalmente en Estados Unidos, contactan a empresas nacionales que generan grandes volúmenes de tráfico internacional. Cuando un abonado en Estados Unidos realiza una llamada al exterior la llamada es enrutada hacia Ecuador al local que presta el servicio de Refilling, desde el cual se re-enruta la llamada telefónica internacional hacia el destino quedando establecido el enlace con el país origen.

Forma de detección.

No se cuenta con un método específico para la detección del fraude de Refilling, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica tiene en cuenta el comportamiento del uso de la línea telefónica en aspectos como son: llamadas de larga duración recibidas y realizadas frecuentemente al exterior, horario en el que se realiza las llamadas, uso de otros servicios, comportamiento de la red.

- Al presentarse algún tipo de anomalías en los parámetros antes mencionados, el equipo antifraude de la operadora telefónica realiza las investigaciones necesarias para determinar si se está o no utilizando de manera indebida los servicios de telefonía para realizar fraude de Refilling.

- En caso de confirmar el uso indebido de los servicios de telefonía para realizar fraude de Refilling, se procede a imponer las sanciones respectivas al defraudador.

Herramientas correctivas.

Como herramienta correctiva ante el fraude de Refilling, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[14].

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

- La operadora telefónica debe Incorporar sistemas de alarmas que permitan detectar casos de llamadas telefónicas internacionales ilícitas realizadas mediante el sistema Refilling.

- La Superintendencia de Telecomunicaciones en coordinación con las operadoras de telefonía, debe mantener un permanente combate a los servicios ilegales, velando para que frente a este moderno y tecnificado fraude se cuente con métodos de detección efectivos que permitan su eliminación.

---

14 **ANEXO C.** Artículo 422 del Código Penal

2.1.4.3.3.1 Llamada telefónica internacional mediante sistema Refilling

Para indicar el proceso ilícito de enrutamiento de tráfico telefónico internacional se ha tomado como ejemplo la realización de una llamada telefónica mediante sistema Refilling desde Estados Unidos hacia Cuba, siendo Ecuador el país intermediario para establecer la conexión.

En la figura 2.13 se muestran los elementos y etapas que intervienen en el establecimiento de la llamada internacional mediante sistema Refilling.

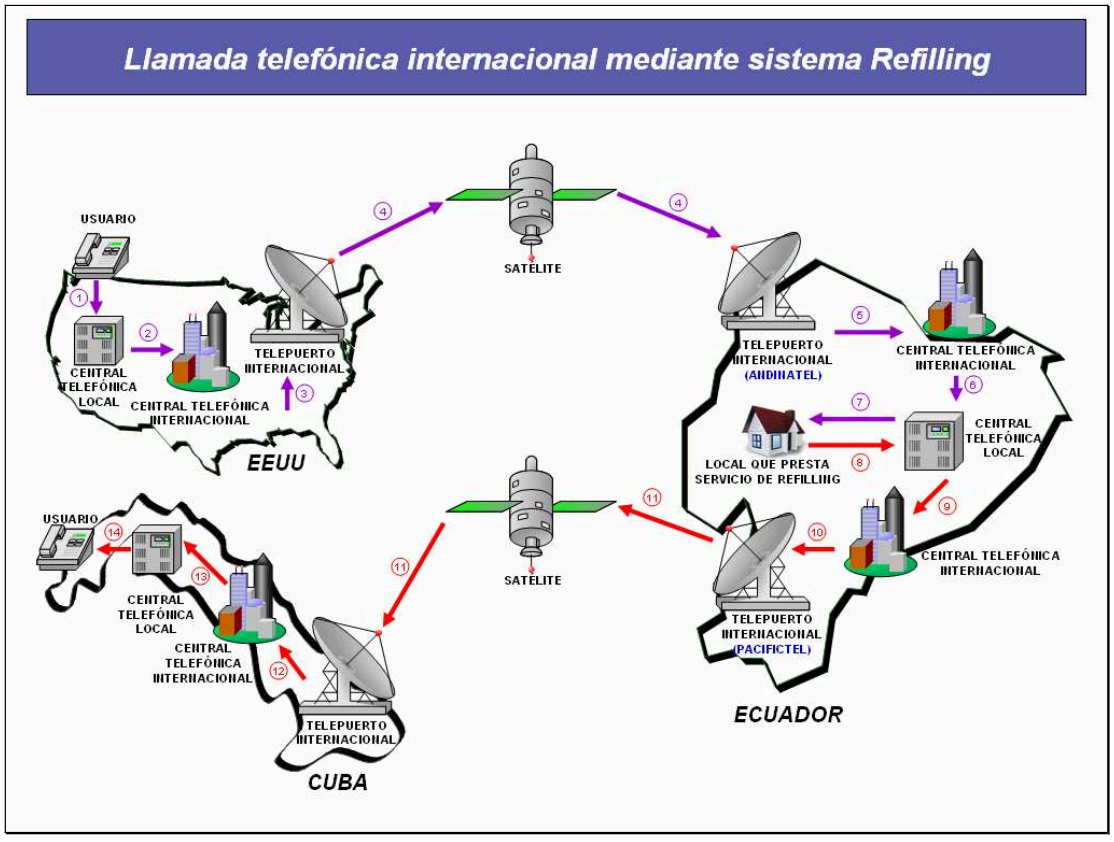
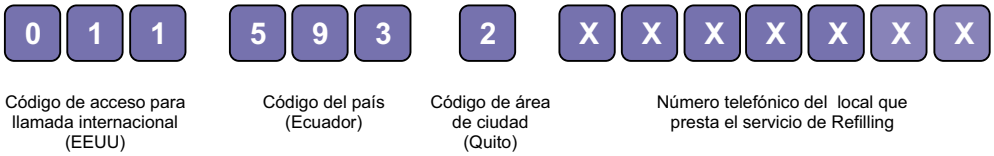


Figura 2.13. Elementos y etapas que intervienen en la llamada telefónica internacional mediante sistema Refilling

Proceso de establecimiento de la llamada telefónica internacional mediante sistema Refilling:

Etapa 1, 2, 3, 4, 5, 6 y 7.

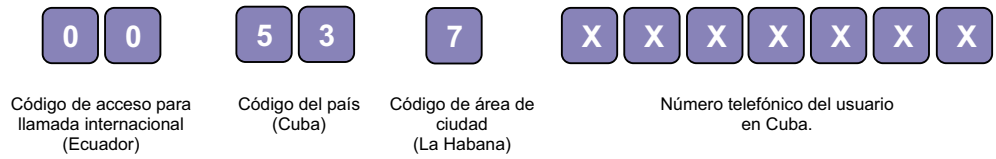
Desde Estados Unidos, para realizar la llamada telefónica internacional se debe marcar el código de acceso para llamada internacional, código del país, código de área de la ciudad y el número telefónico del usuario a quien se desea realizar la llamada, en este caso el número telefónico del usuario destino corresponde al local que presta el servicio de Refilling en Ecuador.



El proceso de establecimiento de la llamada telefónica internacional desde Estados Unidos hacia Ecuador se realiza normalmente, hasta el momento en el que la llamada ingresa al local que presta servicios de Refilling.

Etapa 8, 9, 10, 11, 12, 13 y 14.

Desde Ecuador, el servicio telefónico automático permite al usuario comunicarse a través de un indicativo asignado, con diferentes países, que cuentan con marcación automática. El número telefónico destino corresponde al usuario que se encuentra en Cuba.



El proceso de establecimiento de la llamada telefónica internacional desde Ecuador hacia Cuba se realiza normalmente, el local que presta el servicio de Refilling establece el enlace entre el Usuario en Estados Unidos y el usuario en Cuba estableciendo la llamada telefónica internacional.

2.1.4.3.4 By pass

El By pass encamina directamente el tráfico que viene del exterior hacia las centrales telefónicas locales, sin pasar por la central de tráfico internacional (es decir, se evita la tarifación de la llamada internacional y se la convierte en una llamada local).

Se hace uso de circuitos alquilados o instalados de manera ilegal para revender, a través de ellos, el tráfico telefónico internacional; para poder completar las comunicaciones, el operador irregular necesita utilizar la red nacional a través de la cual completa los servicios hasta cualquier usuario de sistema telefónico nacional y por tanto evitar el pago de interconexión al operador local legalmente establecido.

Para concretar el ilícito se establece un acuerdo entre un operador (por ejemplo un operador establecido en Ecuador) que no está legalmente habilitado para brindar el servicio de telefonía, y un operador extranjero (por ejemplo un operador establecido en Estados Unidos), ofreciéndole pagos por terminación de llamada más favorables que el operador legalmente establecido.

Los proveedores de este servicio ilícito se localizan principalmente en Estados Unidos y su forma de operar es a través de operadores locales, comercializadores de tarjetas telefónicas, carrier internacionales y operadores para la terminación de la llamada en el país de destino.

El costo del equipamiento para este tipo de operaciones ilícitas es significativamente menor al que invierte un operador legalmente establecido, que debe además cancelar el costo de la licencia de operación y la contribución al fondo de comunicaciones establecidos en todos los países.

2.1.4.3.4.1 Evolución tecnológica de los sistemas By pass

Un sistema de telefonía internacional ilegal denominado “By pass”, constituye una ruta alterna o paralela a las rutas autorizadas, por la cual, se cursa tráfico telefónico internacional ilegal, el mismo que es registrado por la operadora autorizada como si se tratase de tráfico telefónico generado local, regional o nacionalmente.

La estructura de un sistema tipo “By pass” esta formada básicamente por tres partes:

- Equipamiento para establecer el enlace internacional.
- Equipamiento de conmutación para enrutar las llamadas.
- Sistema operativo para evitar la detección de las líneas utilizadas.

Al analizar como se han estructurado los sistemas telefónicos tipo By pass, desde que se detectaron por primera vez en 1995, hasta los últimos intervenidos en el 2005[15], se pueden establecer tres etapas dentro de su evolución tecnológica, las mismas que pueden ser identificadas de acuerdo a los cambios producidos en sus componentes básicos y, que influyen principalmente en los procesos de detección de los números de las líneas telefónicas que se utilizan en estos sistemas ilegales.

En el Ecuador, para la detección de sistemas tipo By pass, se realiza el trabajo conjunto entre la operadora telefónica legalmente establecida y el ente regulador de telecomunicaciones.

---

15 http://www.supertel.gov.ec/no_autorizados/trafico.htm

Las operadoras de telefonía fija legalmente establecidas para cursar tráfico telefónico internacional, que han sido consideradas en la presente tesis son: ANDINATEL S.A., PACIFICTEL S.A. y ETAPA.

La Superintendencia de Telecomunicaciones como ente regulador, tiene como misión[16]: Controlar los servicios de telecomunicaciones[17] y el uso del espectro radioeléctrico, velando por el interés general para contribuir al desarrollo del sector y del país.

Las etapas que se han presentado en la evolución de los sistemas telefónicos tipo By pass, se describen a continuación:

➚ *Primer periodo de evolución tecnológica de los sistemas By pass*

El primer periodo de la evolución tecnológica de los sistemas de By pass está comprendido entre los años 1995 hasta principios de 1999[18], periodo en el cual las operadoras telefónicas y el ente regulador de telecomunicaciones evidencian los primeros casos de tráfico telefónico internacional ilegal.

Es importante mencionar que, antes de 1995 no se habían establecido procedimientos para combatir estos ilícitos, debido a que se presentaba como un nuevo tipo de fraude.

---

16 http://www.supertel.gov.ec/organizacion/organizacion1.htm#1

17 **ANEXO E.** Intervenciones realizadas por la Superintendencia de Telecomunicaciones a estaciones de radiodifusión, sistemas de televisión por cable, y sistemas de By pass, que operaban sin autorización

18 http://www.supertel.gov.ec/no_autorizados/trafico.htm

Equipo utilizado.

Los equipos son utilizados para realizar transmisión de datos y conmutación, este periodo se caracteriza por que los equipos son propiedad del defraudador o empresa que comete fraude, los mismos que deben realizar una inversión económica grande para adquirir esos equipos.

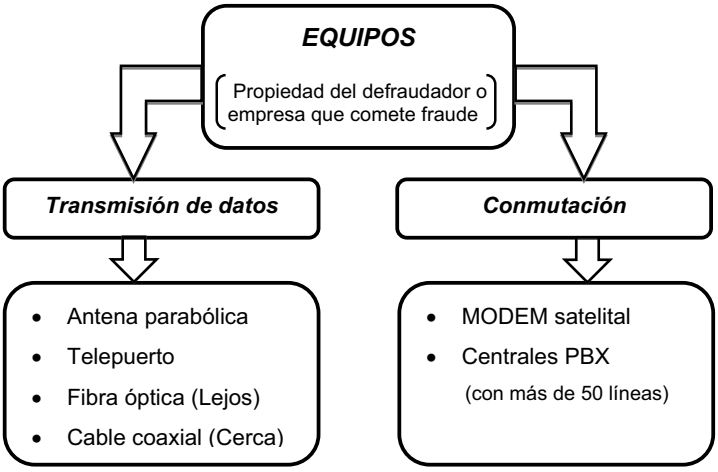


Figura 2.14. Equipos utilizados en el primer periodo de evolución tecnológica de los sistemas By pass

Transmisión de datos.

La transmisión de datos permite la comunicación de voz estableciendo la conversación entre usuarios. Generalmente se hace uso de antena parabólica, telepuerto, fibra óptica (cuando la transmisión de datos se realiza entre lugares distantes), cable coaxial (cuando la transmisión de datos se realiza entre lugares cercanos).

Conmutación.

La conmutación permite la interconexión de circuitos de telecomunicaciones por el tiempo necesario para transportar el tráfico telefónico. Generalmente los equipos usados son MODEM satelital y centrales PBX.

Observaciones:

- Durante este periodo, los sistemas telefónicos tipo By pass, se estructuran totalmente con infraestructura de propiedad de empresas o personas naturales, a cuyo nombre consta todo el equipamiento, incluso las líneas telefónicas.

  El gasto económico para adquirir los equipos es considerablemente alto, sin embargo las ganancias económicas obtenidas al cursar tráfico telefónico internacional de manera ilícita permite costear la inversión realizada por el defraudador o empresa que comete By pass, dejando una considerable ganancia económica.

- No se evidencia complicidad de los funcionarios ni manipulación de los registros de llamadas telefónicas internacionales almacenados en la base de datos de las operadoras telefónicas legalmente establecidas.

- Debido al tipo de equipo utilizado para realizar la transmisión y conmutación, se requiere de una persona presente supervisando, es decir, en el local clandestino se encuentran los equipos y el defraudador.

- Considerando la forma evidente de operar por parte del defraudador o empresa que comete el fraude, y con el trabajo conjunto entre la operadora telefónica y el ente regulador de telecomunicaciones, en este periodo, se detecta de manera fácil los sistemas tipo By pass.

- Las sanciones no se las impone de acuerdo al Código Penal, ya que en el mismo no se encuentra ningún artículo que sancione el acto de operar con sistemas tipo By pass para cursar tráfico telefónico de manera ilícita.

  Por lo tanto no se tiene un marco legal que permita tipificar este tipo de delito y penalizarlo adecuadamente, razón por la cual las sanciones impuestas son insignificantes frente a la ganancia económica que representa cursar tráfico telefónico internacional de manera ilícita.

↗ *Segundo periodo de evolución tecnológica de los sistemas By pass*

El segundo periodo de la evolución tecnológica de los sistemas de By pass está comprendido entre principios de 1999 hasta finales de 2002[19], periodo en el cual las operadoras telefónicas y el ente regulador de telecomunicaciones, tiene conocimientos más profundos acerca de los casos de tráfico telefónico internacional ilegal.

Equipo utilizado.

Los equipos son utilizados para realizar transmisión de datos y conmutación, este periodo se caracteriza por que el enlace satelital utilizado para la transmisión de datos es arrendado, y los equipos utilizados para realizar conmutación son propiedad del defraudador o empresa que comete fraude; lo cual implica que la inversión económica para adquirir los equipos es significativamente menor en comparación a la inversión que se realiza en el primer periodo.

---

19 http://www.supertel.gov.ec/no_autorizados/trafico.htm

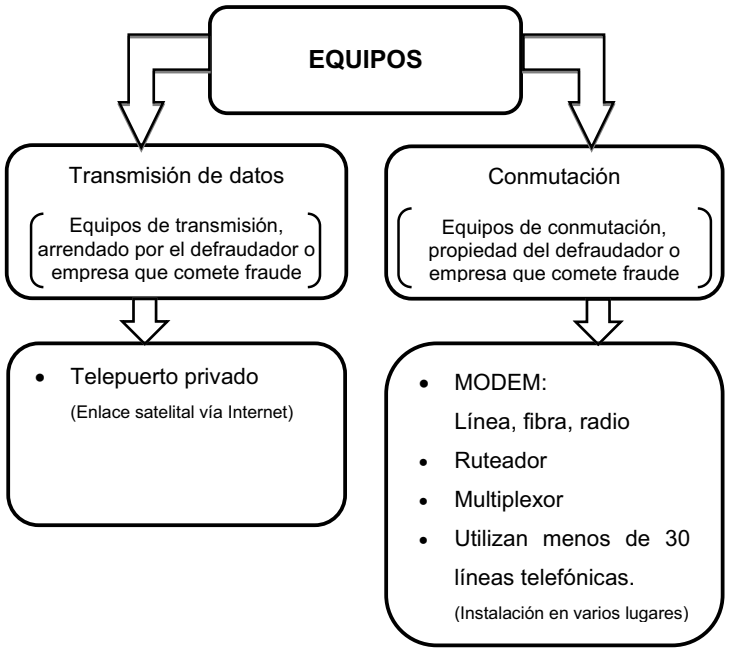


Figura 2.15. Equipos utilizados en el segundo periodo de evolución tecnológica de los sistemas By pass

Transmisión de datos.

La transmisión de datos permite la comunicación de voz estableciendo la conversación entre usuarios. Se hace uso del telepuerto privado para realizar el enlace satelital.

Conmutación.

La conmutación permite la interconexión de circuitos de telecomunicaciones por el tiempo necesario para transportar el tráfico telefónico. Se hace uso de las líneas telefónicas, y generalmente el equipo utilizado son MODEM, ruteadores, multiplexores.

Observaciones:

- En el segundo periodo se evidencia la complicidad de los funcionarios y manipulación de los registros de llamadas telefónicas internacionales de las operadoras telefónicas legalmente establecidas.

- Considerando los equipos utilizados y la forma de operar por parte del defraudador o empresa que comete el fraude, a pesar del trabajo conjunto entre la operadora telefónica y el ente regulador de telecomunicaciones, en este segundo periodo se detecta de manera difícil los sistemas tipo By pass.

- Los equipos de telecomunicaciones al ser configurados adecuadamente efectúan el trabajo continuamente sin necesidad de que haya una persona presente supervisando, es decir, en el local clandestino se encuentran los equipos más no el defraudador.

- Se tiene un marco legal que permite tipificar y penalizar adecuadamente el delito de operar con sistemas tipo By pass para cursar tráfico telefónico internacional de manera ilícita, las sanciones impuestas son de acuerdo al artículo 422 del Código Penal[20].

- En este periodo, el defraudador o empresa que opera con sistemas tipo By pass, utiliza los servicios de telepuertos privados legalmente autorizados para establecer enlaces satelitales, mediante el arrendamiento de estos servicios se establece el enlace internacional que permite el ingreso del tráfico telefónico internacional al Ecuador. Los telepuertos privados legalmente autorizados que prestan servicios de enlaces internacionales, técnicamente no pueden determinar la clase de información que su cliente está transportando a través de la infraestructura arrendada, por esta razón de estar cursando tráfico telefónico ilegal, no se sanciona al telepuerto privado.

---

20 **ANEXO C.** Artículo 422 del Código Penal

➚ *Tercer periodo de evolución tecnológica de los sistemas By pass*

El tercer periodo de la evolución tecnológica de los sistemas de By pass está comprendido a partir de finales de 2002 hasta los actuales momentos[21], periodo en el cual las operadoras telefónicas y el ente regulador de telecomunicaciones, cuentan con departamentos específicos para analizar las principales clases de fraude, su tendencia, desarrollo, técnicas de detección para proveer herramientas preventivas y correctivas en contra del fraude.

Los componentes básicos de un sistema telefónico tipo By pass se mantienen semejantes a los del segundo periodo, pero el vertiginoso avance de la tecnología hace que estos componentes estén ahora dotados de medios que hacen más difícil su detección.

Equipo utilizado.

Los equipos son utilizados para realizar transmisión de datos y conmutación, en este periodo el enlace satelital utilizado para la transmisión de datos es arrendado, y los equipos utilizados para realizar conmutación son propiedad del defraudador o empresa que comete fraude, al ser equipos actuales permiten efectuar diversas funciones a la vez evitando utilizar varios equipos que realicen estas funciones individualmente como se tenía en los periodos anteriores; lo cual implica que la inversión económica para adquirir los equipos es significativamente menor en comparación a la inversión que se realiza en el primer y segundo periodo.

---

21 http://www.supertel.gov.ec/no_autorizados/trafico.htm

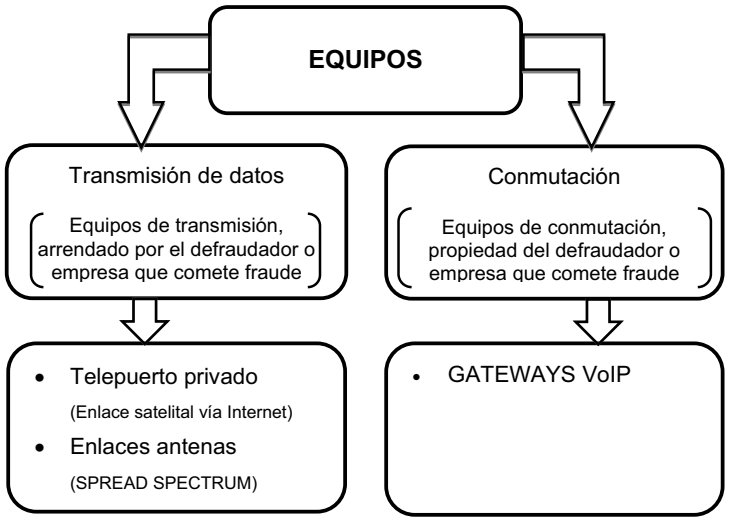


Figura 2.16. Equipos utilizados en el tercer periodo de evolución tecnológica de los sistemas By pass

Transmisión de datos.

La transmisión de datos permite la comunicación de voz estableciendo la conversación entre usuarios. Se hace uso del telepuerto privado para realizar el enlace satelital y antenas SPREAD SPECTRUM para enlaces locales.

Conmutación.

La conmutación permite la interconexión de los circuitos de telecomunicaciones por el tiempo necesario para transportar el tráfico telefónico. Se hace uso de equipos de telecomunicaciones entre los cuales se tiene GATEWAYS VoIP.

Observaciones:

- En este tercer periodo se evidencia complicidad de los funcionarios y manipulación de los registros de llamadas telefónicas internacionales de las operadoras telefónicas legalmente establecidas, llegando incluso al punto de impedir que esas líneas registren facturación, a pesar de que a través de ellas se genere tráfico telefónico, e incluso esas líneas no cuentan con ningún registro de abonado, es decir, son líneas aparentemente inexistentes.

- Considerando los equipos actualmente utilizados y la forma de operar por parte del defraudador o empresa que comete el fraude, y a pesar del trabajo conjunto entre la operadora telefónica y el ente regulador de telecomunicaciones, en este tercer periodo se detecta de manera muy difícil los sistemas tipo By pass.

- Los equipos de telecomunicaciones al ser configurados adecuadamente efectúan el trabajando continuamente, es decir, en el local clandestino se encuentran los equipos más no el defraudador.

  Al utilizarse equipos de telecomunicaciones denominados GATEWAYS los mismos que cuentan con aplicaciones específicas para procesar señales telefónicas, e incluso pueden manejar los parámetros de señalización de una red de telefonía, permiten que los sistemas tipo By pass sean fácilmente implementados.

- Al igual que en el segundo periodo se tiene un marco legal que permite tipificar y penalizar adecuadamente el delito de operar con sistemas tipo By pass, las sanciones impuestas son de acuerdo al artículo 422 del Código Penal[22].

---

22 **ANEXO C.** Artículo 422 del Código Penal

- Al igual que en el segundo periodo, el defraudador o empresa que opera con sistemas tipo By pass, arrienda los enlaces satelitales para establecer el enlace entre países que permite cursar tráfico telefónico internacional.

  Al estar cursando tráfico telefónico ilegal mediante el enlace satelital arrendado, el telepuerto privado legalmente autorizado que presta servicios de enlaces internacionales no es sancionado.

- Es en este tercer periodo de la evolución tecnológica de los sistemas tipo By pass cuando por primera vez se utilizan conectadas a estos sistemas ilegales líneas de telefonía móvil celular, a través de las cuales se cursa el tráfico internacional ilegal a las redes telefónicas del Ecuador.

  El uso de líneas de telefonía móvil celular en sistemas tipo By pass, dificulta considerablemente, la detección del sitio clandestino en donde se encuentra la instalación de los equipos de telecomunicaciones que procesa la señal telefónica internacional, esto debido a que en el caso de las líneas de telefonía móvil celular el medio de comunicación utilizado es una señal radioeléctrica que viaja en el espacio, mientras que en los sistemas que utilizan líneas físicas una vez identificados los números telefónicos se sigue la trayectoria del cable que contiene las líneas hasta identificar la ubicación de la instalación de los equipos de telecomunicaciones.

  Debido a que la presente tesis esta orientada al análisis de los diferentes tipos de fraude más frecuentes en la telefonía fija, únicamente se ha mencionado que los sistemas tipo By pass en este periodo están siendo implementados con líneas de telefonía móvil celular.

Al analizarse los diferentes tipos de fraude más frecuentes en la telefonía fija, se indica la forma ilícita de operar, forma de detección, herramientas correctivas y preventivas únicamente para el tercer periodo de evolución tecnológica de los sistemas By pass.

Forma ilícita de operar.

La forma ilícita de operar variara dependiendo de aspectos como son motivos, medios, modos, métodos, entre otros, es decir, no se cuenta con una forma específica para operar con sistemas tipo By pass, sin embargo los aspectos a considerarse comúnmente son:

- La persona o empresa que comete fraude prepara el local con equipos de telecomunicaciones con la finalidad de cursar tráfico telefónico internacional.

- Para evitar que los sistemas telefónicos tipo By pass sean detectados, físicamente las líneas telefónicas son manipuladas de tal manera que las redes clandestinas instaladas en diversos sectores, con varios kilómetros distantes entre ellos, mediante un tendido de cable las líneas telefónicas son llevadas hasta el local clandestino donde se encuentra la instalación de equipos de telecomunicaciones que procesa la señal telefónica internacional.

  Las líneas telefónicas (alrededor de 30 líneas en cada sector) están a nombre de varias personas o empresas para evitar que la operadora telefónica detecte una gran concentración de líneas telefónicas y no sospeche del uso fraudulento de las mismas.

- La mayoría de sistemas tipo By pass, utilizan los equipos denominados GATEWAYS, los mismos que permiten la convergencia entre una red de datos y una red telefónica pública conmutada, como la de las operadoras de telefonía fija del Ecuador.

- La persona que realiza este tipo de fraude vía Internet consigue el proveedor de tráfico telefónico internacional al cual se concede el costo de cada minuto telefónico a una tarifa menor a la establecida por las operadoras telefónicas legalmente establecidas, representando una ganancia económica para el proveedor extranjero de tráfico telefónico y para la persona o empresa que opera con sistemas tipo By pass en el Ecuador.

- El proveedor de tráfico telefónico internacional vende tarjetas telefónicas para establecer la llamada desde el exterior hacia el Ecuador. Debido al costo menor que representa realizar las llamadas internacionales por medio de las tarjetas telefónicas en comparación a la tarifa establecida por las operadoras telefónicas legalmente establecidas, el usuario prefiere adquirir las tarjetas para realizar llamadas internacionales.

- Haciendo uso de telepuertos privados (uno ubicado en el exterior y otro en el Ecuador) se realiza la transferencia de tráfico telefónico entre los países. Debido al tipo de equipos de telecomunicaciones utilizados para cometer el fraude, en el país extranjero mediante MODEM se digitaliza la señalización y la voz que son señales de origen analógico para ser encapsulados en paquetes IP, los mismos que son transmitidos vía satélite hacia el Ecuador, los paquetes IP ingresan al local clandestino en el cual se desencapsula la señalización y la voz para mediante MODEM convertir la señal digital en señal analógica.

Al trabajarse con paquetes IP, se tienen varios equipos de telecomunicaciones que requieren ser configurados como son: GATEWAYS y RUTEADORES.

- La mayoría de los sistemas tipo By pass utilizan la tecnología de espectro ensanchado, para establecer la comunicación entre el local clandestino donde se encuentra la instalación de equipos de telecomunicaciones, con el telepuerto privado al cual arrienda el enlace internacional.

- Con los equipos de transmisión arrendados, equipos de conmutación instalados en el local clandestino, y establecido el negocio para cursar tráfico telefónico, se realizan las llamadas internacionales tipo By pass.

- El defraudador o empresa que comete fraude para evitar ser descubierto trabaja en complicidad con los funcionarios de las operadoras telefónicas legalmente establecidas, quienes ayudan a conseguir fácilmente las líneas telefónicas que serán utilizadas ilícitamente y manipulan el sistema de registros de llamadas para realizar alteraciones ilícitas como son:

  - Enmascaramiento del número telefónico.

    El número telefónico del cual se realiza la llamada es identificado por la operadora telefónica y de acuerdo a la codificación de la misma se puede conocer si se trata de una llamada nacional o internacional, generalmente se altera dicha codificación para que la operadora telefónica no pueda conocer datos ciertos acerca del lugar origen de la llamada telefónica realizada.

- Alteración de datos del usuario.

  En los registros de la operadora telefónica se realizan alteraciones de los datos correspondientes a la persona o empresa que opera con sistemas tipo By pass, generalmente se modifican los datos personales y la dirección en el cual se instaló las líneas telefónicas.

- La principal preocupación del defraudador o empresa que comete el fraude es el de tener precaución de no ser descubierto por la operadora telefónica ni por el ente regulador de telecomunicaciones.

Forma de detección.

En el Ecuador, para la detección de sistemas tipo By pass, se realiza el trabajo conjunto entre la operadora telefónica legalmente establecida y el ente regulador de telecomunicaciones.

Los métodos para la detección de sistemas tipo By pass variaran dependiendo de aspectos como son el tipo y configuración de equipos, infraestructura del local clandestino, forma de cursar ilegalmente el tráfico telefónico, entre otros; es decir, no se cuenta con un método específico para la detección de sistemas tipo By pass, sin embargo los aspectos a considerarse comúnmente son:

- La operadora telefónica cuenta con el departamento de gerencia de fraude y aseguramiento de ingresos, departamento en el cual el equipo antifraude se encarga exclusivamente de la detección, control y gestión del fraude en telecomunicaciones.

- La operadora telefónica tiene funcionarios trabajando en los países extranjeros en los cuales se tiene un alto índice de habitantes ecuatorianos, los funcionarios en el exterior se encargan de adquirir tarjetas telefónicas y enviarlas al Ecuador para que el equipo antifraude de la operadora telefónica se encargue de hacer el control respectivo.

- Para adquirir las tarjetas telefónicas, los funcionarios consideran que el costo por llamada utilizando la tarjeta sea inferior al costo establecido por la operadora telefónica legalmente establecida para realizar llamadas internacionales, generalmente las tarjetas telefónicas sospechosas son las que tienen como tarifa el costo de llamada inferior a 10 centavos el minuto.

- El equipo antifraude haciendo uso de las tarjetas telefónicas realiza llamadas de prueba para confirmar si se está o no operando con sistemas tipo By pass en el Ecuador, la forma de operar que utiliza el equipo antifraude para detección de tráfico telefónico ilegal generalmente es:

    - El equipo antifraude trabaja esencialmente con dos teléfonos convencionales, un teléfono para realizar llamadas de prueba, y otro teléfono equipado con identificador de llamadas para recibir e identificar el origen de las llamadas entrantes.

    - Desde un teléfono convencional el equipo antifraude realiza la llamada a la operadora telefónica legalmente establecida solicitando el realizar una llamada internacional.

    - La operadora telefónica indica al equipo antifraude que le proporcione el código del país, código de área de la ciudad y número del usuario a quien se desea realizar la llamada telefónica internacional.

- El equipo antifraude proporciona los datos teniendo en cuenta el país y lugar en el cual se adquirió la tarjeta telefónica, el número al que se desea realizar la llamada es el que se indica en la tarjeta telefónica.

- La operadora telefónica establece la llamada internacional entre el equipo antifraude en el Ecuador y el país extranjero, en el país extranjero la llamada ingresa a un local en el cual está asignado el número telefónico que se indica en la tarjeta telefónica.

- En el Ecuador el equipo antifraude escucha una grabación proveniente del local en el país extranjero, la grabación solicita que se ingrese el código PIN de la tarjeta para escuchar el saldo y tiempo útil de la tarjeta para realizar llamadas telefónicas, posteriormente la grabación solicita que se ingrese el código del país, código de área de la ciudad y el número telefónico al que se desea realizar la llamada, el equipo antifraude ingresa el número telefónico correspondiente al teléfono equipado con identificador de llamada en el Ecuador.

- El equipo antifraude recibe la llamada telefónica de origen internacional y mediante el teléfono equipado con identificador de llamadas se verifica realmente el origen de la llamada entrante.

- Al estar operando de una manera normal para cursar tráfico telefónico internacional, en el identificador de llamada se observa el número telefónico internacional correspondiente al origen de la llamada telefónica.

- En algunas ocasiones en el identificador de llamada no se observan números telefónicos, se observan dígitos alfabéticos como puede ser una serie de letras, esto significa que funcionarios de la operadora legalmente establecida son

cómplices de la persona o empresa que comete fraude, los funcionarios corruptos manipulan el sistema alterando los registros de llamadas enmascarando el número telefónico del cual se ha realizado la llamada.

Frente a esta anomalía, la operadora telefónica detecta al funcionario corrupto y se le impone la sanción respectiva, se configura de manera correcta al sistema de registros de llamadas y se procede nuevamente a recibir llamadas del exterior.

- Al estar operando con sistemas tipo By pass para cursar tráfico telefónico internacional de manera ilícita, en el identificador de llamada no se observa el número telefónico internacional que es el verdadero origen de la llamada telefónica, se observa un número telefónico nacional correspondiente a las líneas telefónicas que han sido instaladas en el local clandestino.

  El equipo antifraude al conocer el número telefónico nacional correspondiente a las líneas telefónicas usadas para cursar tráfico telefónico internacional de manera ilícita, busca en la base de datos de los usuarios del servicio telefónico los datos de la persona o empresa y el lugar en el cual se instalaron las líneas telefónicas.

- La operadora telefónica ya con la prueba contundente que se esta cursando tráfico telefónico internacional de manera ilícita y la ubicación del local clandestino, pone en conocimiento de la anomalía a la Superintendencia de Telecomunicaciones.

- El departamento encargado de dicho tipo de anomalías es la “Unidad de investigaciones especiales de telecomunicaciones” de la Superintendencia de Telecomunicaciones, quien da conocimiento de este echo al ministerio público.

- Las autoridades ya en conocimiento de las anomalías en cuanto al tráfico telefónico internacional, realizan una inspección (visita técnica) al lugar que se opera con sistemas tipo By pass, intervienen:

  - Por parte de la Superintendencia de Telecomunicaciones, el departamento de Unidad de investigaciones especiales de telecomunicaciones.
  - Por parte del ministerio público, un fiscal.
  - Por parte de la operadora telefónica, el equipo antifraude.

  De ser necesario apoyo para realizar la inspección (visita técnica) al lugar que opera con sistemas tipo By pass, se pide la colaboración de la Policía.

  Estos funcionarios comprueban que se está operando con sistemas tipo By pass para cursar tráfico telefónico internacional de manera ilegal, luego se procede a imponer las sanciones respectivas.

Herramientas correctivas

Como herramienta correctiva ante la forma de operar con sistemas tipo By pass para cursar tráfico telefónico internacional de manera ilegal, la sanción es impuesta de acuerdo al artículo 422 del Código Penal[23].

Herramientas preventivas

Para una adecuada detección, control y gestión del fraude en telecomunicaciones por parte de la operadora telefónica y el ente regulador de telecomunicaciones, es necesario considerar aspectos como son:

---

23 **ANEXO C.** Artículo 422 del Código Penal

- En este periodo, las operadoras telefónicas cuentan con un departamento que se encarga de la gerencia de fraude y aseguramiento de ingresos, es decir, se cuenta con un equipo antifraude.

- El ente regulador de telecomunicaciones, Superintendencia de Telecomunicaciones, cuenta con la unidad de investigaciones especiales de telecomunicaciones.

- Debido a que los equipos de telecomunicaciones utilizados para operar como sistemas tipo By pass son de última tecnología, es necesario capacitar al personal que realiza las visitas técnicas para que sepa distinguir cuando la configuración y funcionamiento de los equipos permite cursar tráfico telefónico de manera ilícita.

- La Superintendencia de Telecomunicaciones, solicita que los usuarios de telefonía fija, previo a la instalación de cualquier servicio telefónico, suscriban un acta de compromiso en la que garanticen el correcto uso del servicio y la infraestructura proporcionada por la operadora de telefonía, a fin de que en caso de mal uso de los mismos, esa acta sirva como documento de apoyo en los procesos judiciales que en esos casos corresponde.

- La Superintendencia de Telecomunicaciones en coordinación con las operadoras de telefonía y el Ministerio Público, mantiene un permanente combate a estos servicios ilegales, velando para que frente a este moderno y tecnificado fraude se cuente con métodos de detección efectivos que permitan su eliminación.

2.1.4.3.4.2 Llamada telefónica internacional tipo By pass

Para indicar el proceso ilícito de enrutamiento de tráfico telefónico internacional se ha tomado como ejemplo la realización de una llamada telefónica tipo By pass desde los Estados Unidos hacia el Ecuador, teniendo como referencia el tercer periodo de la evolución tecnológica de los sistemas de By pass.

En la figura 2.17 se muestran los elementos y etapas que intervienen en el establecimiento de la llamada internacional tipo By pass.

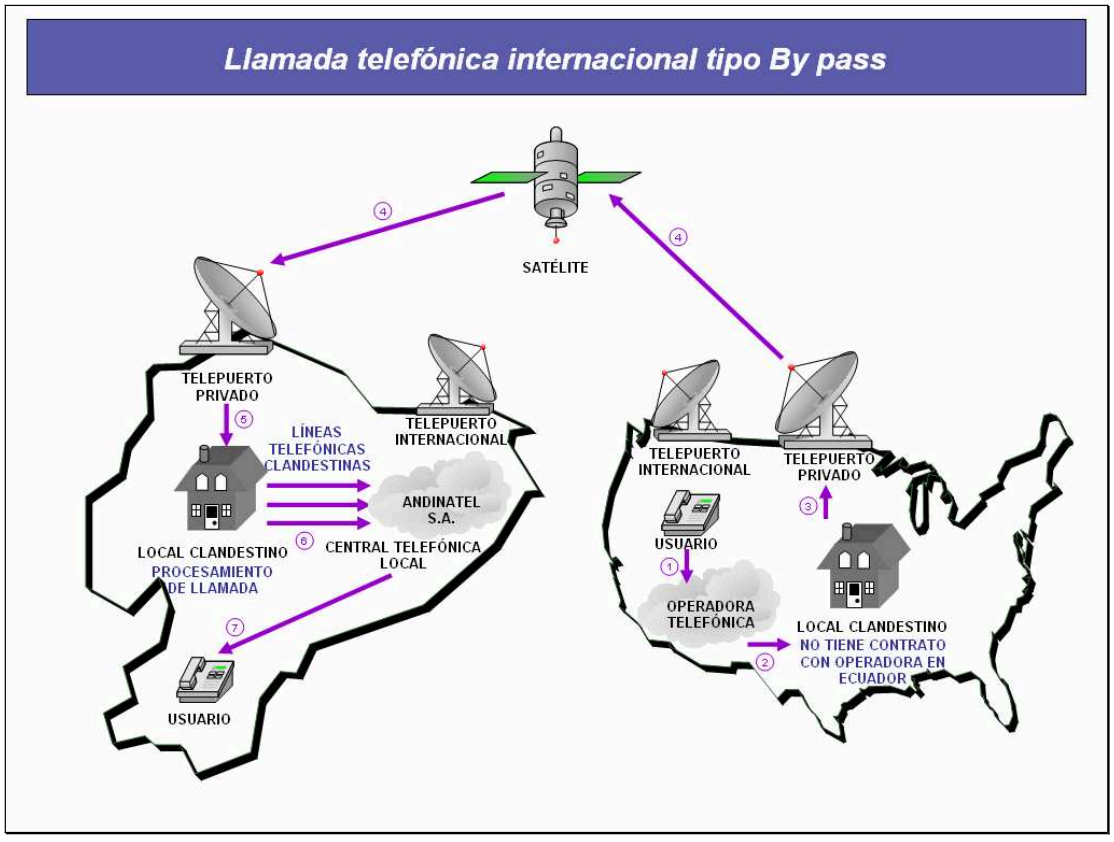


Figura 2.17. Elementos y etapas que intervienen en la llamada telefónica internacional tipo By pass

Proceso de establecimiento de la llamada telefónica internacional tipo By pass:

Etapa 1 y 2.

Generalmente se hace uso de tarjetas telefónicas para establecer la llamada desde el exterior hacia el Ecuador.

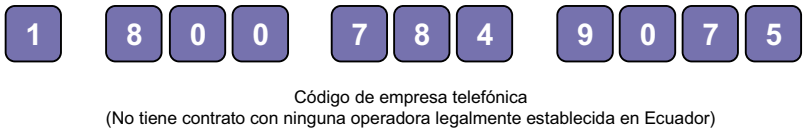
Debido al costo menor que representa realizar las llamadas internacionales por medio de las tarjetas telefónicas en comparación a la tarifa establecida por las operadoras telefónicas legalmente establecidas, el usuario prefiere adquirir las tarjetas para realizar llamadas internacionales, siendo éstas llamadas telefónicas internacionales tipo By pass.

En la tarjeta telefónica se indica el número telefónico para acceder a la empresa telefónica (no tiene contrato con la operadora en Ecuador), código PIN y pasos a seguir para establecer la llamada telefónica.

Figura 2.18. Tarjeta telefónica

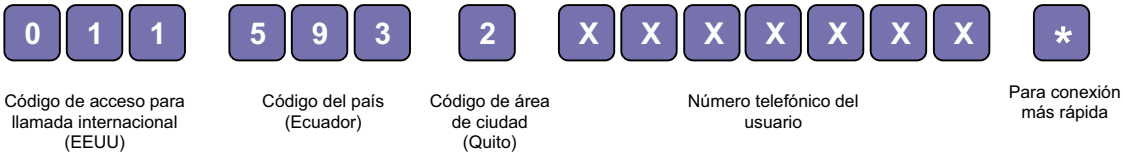
Desde Estados Unidos, para establecer la llamada telefónica internacional de acuerdo a la tarjeta telefónica de la figura 2.18, se tiene:

Se marca el número que figura en la tarjeta telefónica, el cual corresponde a la empresa telefónica que no tiene contrato con ninguna operadora legalmente establecida en Ecuador.



Se marca el número del código PIN, y el usuario escucha una grabación que le indica la cantidad de tiempo útil que le queda en la tarjeta telefónica; el tratamiento del código se realiza mediante software.

Luego, se marcar el código de acceso para llamada internacional, código del país, código de área de la ciudad y el número telefónico del usuario a quien se desea realizar la llamada.



El tiempo útil de la tarjeta telefónica no es deducido hasta que la llamada sea contestada, cuando se ha usado todo el tiempo útil, la tarjeta telefónica queda inactiva.

La llamada ingresa a la a la empresa telefónica en EEUU, en la cual haciendo uso de equipos de telecomunicaciones se encapsula la señalización y voz en paquetes IP, tratándose la información digitalmente durante todo el proceso de transmisión de datos hasta el local clandestino en Ecuador.

Etapa 3 y 4.

El tráfico telefónico internacional se enruta por telepuertos privados (sean estos autorizados o no) y no por telepuertos internacionales de las empresas telefónicas. Dependiendo de la magnitud del tráfico telefónico cursado de manera ilícita, la transmisión de información vía satélite se lo realiza por medio del telepuerto privado de la persona o empresa que comete fraude o contratando los servicios de transmisión proporcionado por carriers.

Debido a que el código de identificación que el telepuerto privado envía junto a la información no corresponde a ningún operador legalmente establecido, el telepuerto internacional receptor de la empresa telefónica toma la información y la descarta, siendo el código reconocido por el telepuerto privado receptor quién acepta la información.

Etapa 5.

Una vez que todo el volumen de tráfico telefónico ha ingresado al local clandestino, equipos de telecomunicaciones desencapsulan la señalización y voz que se encuentra en paquetes IP, para procesar automáticamente la información como una mini central telefónica.

Etapa 6 y 7.

Previamente, se debió equipar el local clandestino con numerosas líneas telefónicas, que dependiendo del tamaño del By pass suele bordear las 100 líneas.

Estas líneas son conseguidas a través de cómplices en la misma empresa telefónica o con documentación falsa, adulterada o robada.

Las llamadas procesadas por la mini central telefónica en el local clandestino generan llamadas locales hacia los abonados finales en el Ecuador, completando así la llamada que se generó desde cualquier parte del mundo hacia Ecuador.

Las empresas telefónicas locales sólo perciben una llamada local, mientras la porción internacional la cobra el defraudador o empresa que comete el fraude.

Enlaces entre el telepuerto y el local clandestino

Generalmente el telepuerto privado se encuentra a una distancia lejana del local clandestino, razón por la cual para realizar la transmisión de tráfico telefónico ilegal se hace uso de la tecnología de espectro ensanchado. La tecnología de espectro ensanchado, permite establecer enlaces microonda a través de antenas tipo rejilla, e incluso antenas omnidireccionales, que son aquellas que mantienen una cobertura geográfica circular, lo que dificulta determinar totalmente la infraestructura que conforma el sistema telefónico tipo By pass.

En el caso que el telepuerto privado se encuentre a una distancia cercana del local clandestino, la transmisión de tráfico telefónico ilegal se lo realiza mediante el uso de enlaces de última milla como son: fibra óptica, líneas dedicadas de cobre. Para este tipo de comunicación se utiliza un modem en el telepuerto privado y otro en el local clandestino, dependiendo del tipo de enlace se tendrá: modems de línea para cobre o modems de fibra óptica.

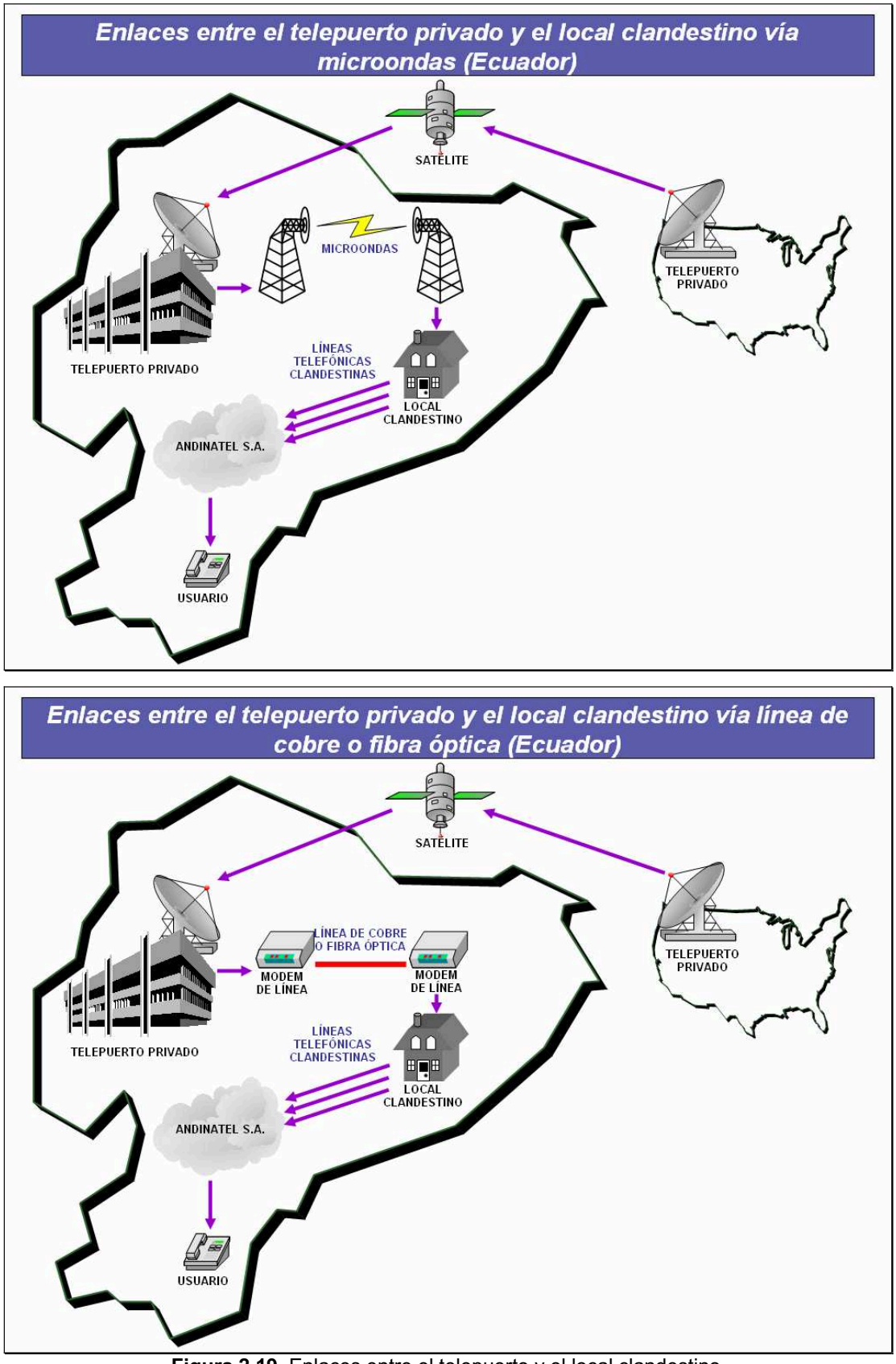


Figura 2.19. Enlaces entre el telepuerto y el local clandestino

Equipos de telecomunicaciones

Al trabajarse con equipos de telecomunicaciones, implica la configuración[24] de algunos de ellos como son los computadores, GATEWAYS y RUTEADORES. Los equipos generalmente utilizados en el establecimiento de la llamada telefónica internacional tipo By pass son:

- *GATEWAYS (MultiTech Systems modelo MVP800).* El GATEWAY es un sistema, hardware y software, que hace de puente entre las líneas telefónicas y la red de telecomunicaciones para que los datos puedan ser transferidos entre distintos ordenadores.
- *SWICH (CNet MultiTech Systems).* El SWICH permite conectar varios GATEWAYS lo que involucra el aumento de líneas telefónicas incrementando el volumen del tráfico telefónico ilegal.
- *RUTEADORES (CISCO 1600).* El RUTEADOR permite establecer el enlace entre las redes de telecomunicaciones, la del local clandestino con la del telepuerto privado.
- *MODEM SPREAD SPECTRUM (WESTERN Multiplex modelo Lynx.sc2).* Realiza la modulación y demodulación de información para su transmisión y recepción, permitiendo conectar las redes de telecomunicaciones, la del local clandestino con la del telepuerto privado.
- *MODEM SATELITAL (COMTECH SDM-300A).* Realiza la modulación y demodulación de información para su transmisión y recepción, permitiendo conectar vía satélite los telepuertos privados.

En la figura 2.20 se muestran los equipos que forman la red de telecomunicaciones, y etapas que intervienen en el enrutamiento del tráfico telefónico internacional tipo By pass.

---

24 **ANEXO F.** Configuración de equipos de telecomunicaciones

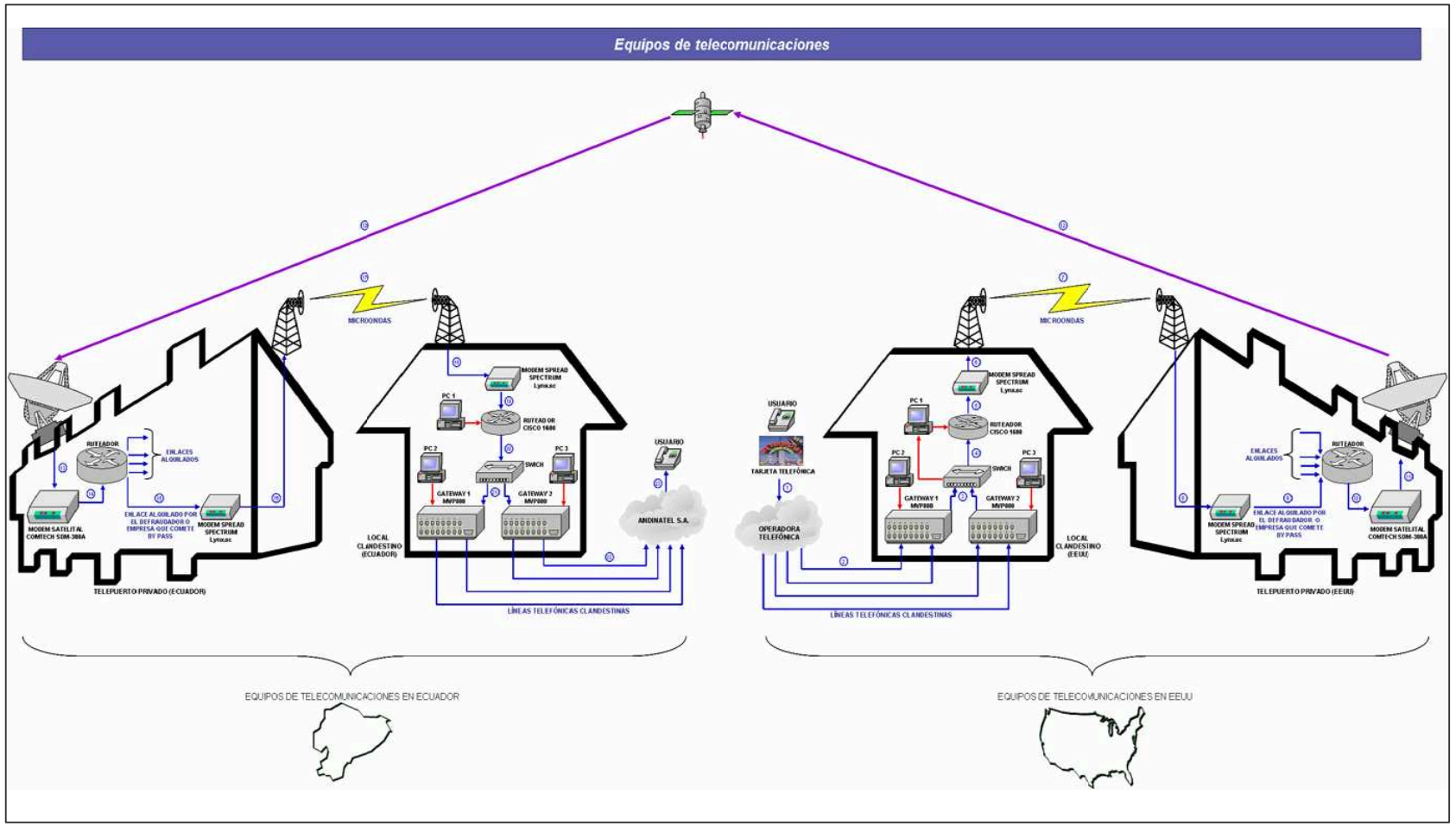


Figura 2.20. Equipos de telecomunicaciones y etapas que intervienen en el enrutamiento de tráfico telefónico internacional tipo By pass

- *Equipos de telecomunicaciones en EEUU*

El local clandestino ubicado en EEUU recibe llamadas telefónicas realizadas por usuarios que utilizan tarjetas telefónicas, para posteriormente la mini central telefónica por medio de equipos de telecomunicaciones encapsular la señalización y voz en paquetes IP (VoIP), y mediante software realizar el control del saldo y tiempo útil de la tarjeta telefónica.

El local clandestino vía microonda envía los paquetes IP al telepuerto privado, desde el cual son transportados vía satélite hasta el telepuerto privado en Ecuador.

- *Equipos de telecomunicaciones en Ecuador*

Los paquetes IP enviados desde el telepuerto privado de EEUU son recibidos por el telepuerto privado ubicado en Ecuador, desde el cual son transportados vía microonda hasta el local clandestino.

El local clandestino ubicado en Ecuador recibe la información enviada por el telepuerto privado, para posteriormente la mini central telefónica por medio de equipos de telecomunicaciones desencapsular la señalización y voz que se encuentra en paquetes IP (VoIP).

Con la señalización y voz desencapsuladas, desde el local clandestino se realizan las llamadas telefónicas, las cuales son enrutadas por la red de la operadora telefónica legalmente establecida hasta su destino.

2.1.4.3.4.3 Detección de números telefónicos usados para sistemas de By pass

El proceso de detección de números telefónicos usados para sistemas de By pass ha sido realizado teniendo como referencia el tercer periodo de la evolución tecnológica de los sistemas de By pass.

En la figura 2.21 se muestran los elementos y etapas que intervienen en la detección de números telefónicos usados para sistemas de By pass.

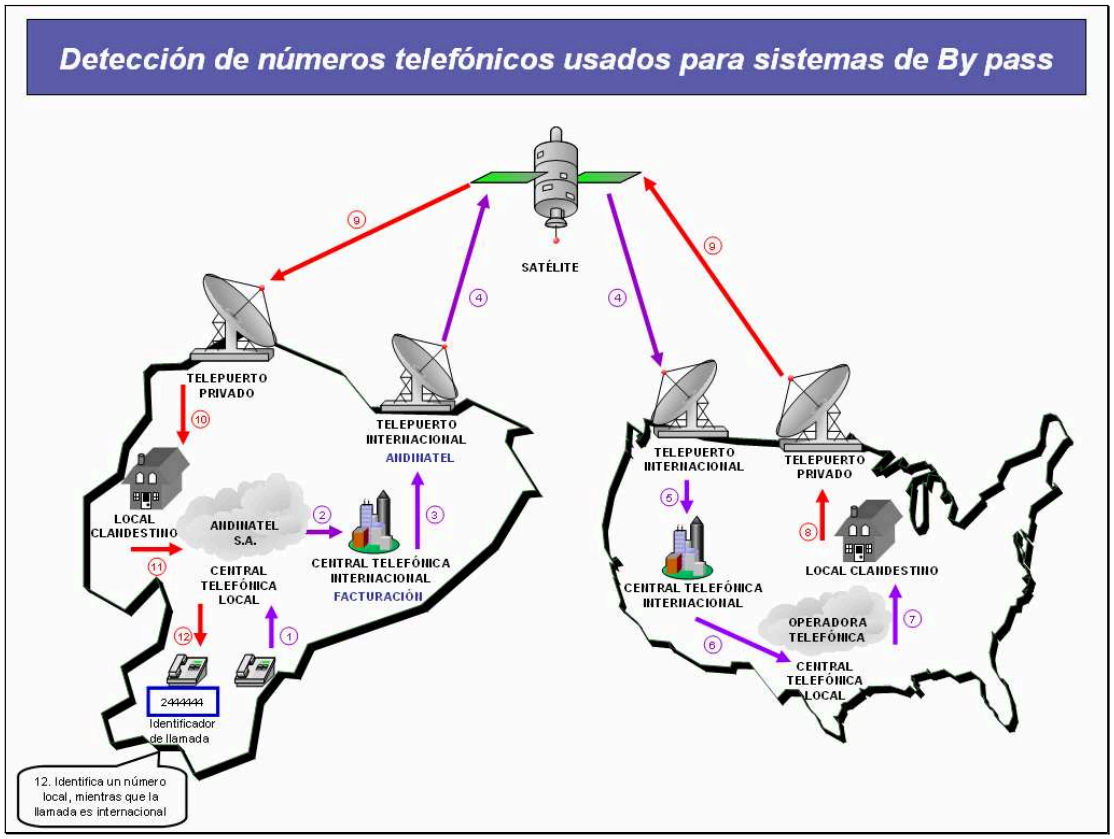


Figura 2.21. Elementos y etapas que intervienen en la detección de números telefónicos usados para sistemas de By pass

Proceso de detección de números telefónicos usados para sistemas de By pass:

Etapa 1.

En Ecuador, el equipo antifraude trabaja con dos teléfonos convencionales, uno para realizar llamadas de prueba, y otro equipado con identificador de llamadas para recibir e identificar el origen de las llamadas entrantes.

El equipo antifraude realiza la llamada a la central telefónica local solicitando realizar una llamada internacional.

Etapa 2, 3 y 4.

La central telefónica local enruta la llamada hacia la central telefónica internacional, a la que se proporciona los datos del código del país, código de área de la ciudad y número a quien se desea realizar la llamada telefónica internacional.

Mediante los telepuertos internacionales de Ecuador y EEUU se establece el enlace vía satélite.

Etapa 5, 6 y 7.

En EEUU, la llamada es enrutada desde el telepuerto internacional hacia la central telefónica internacional, en la cual de acuerdo a los datos de códigos la llamada es enrutada hacia la central telefónica local.

La llamada ingresa al local clandestino, se escucha una grabación solicitando que se ingrese el código PIN de la tarjeta, el código del país, código de área de la ciudad y el número telefónico al que se desea realizar la llamada, el equipo antifraude ingresa el número telefónico correspondiente al teléfono equipado con identificador de llamada en el Ecuador.

Etapa 8, 9, 10, 11 y 12.

Desde EEUU se realiza una llamada telefónica internacional tipo By pass hacia el Ecuador, finalmente la llamada ingresa al teléfono equipado con identificador de llamada en el cual no se observa el número telefónico internacional que es el verdadero origen de la llamada telefónica, se observa un número telefónico local correspondiente a las líneas telefónicas que han sido instaladas en el local clandestino en Ecuador.

Detectándose de esta manera los números telefónicos usados para sistemas de By pass.

CAPÍTULO

III

Estudio comparativo de curvas de tráfico y análisis de pérdidas económicas

CAPÍTULO III

ESTUDIO COMPARATIVO DE CURVAS DE TRÁFICO Y ANÁLISIS DE PÉRDIDAS ECONÓMICAS

3.1 SUPTEL (SUPERINTENDENCIA DE TELECOMUNICACIONES)

La Superintendencia de Telecomunicaciones es el organismo técnico, encargado de controlar el área de las telecomunicaciones en el país, procurando el desarrollo social en este amplio campo, por tal responsabilidad es de su competencia velar por la calidad y correcto uso de los servicios que empresas públicas y privadas brinden en este ámbito.

Las Funciones de la Superintendencia de Telecomunicaciones son[1]:

Según la ley reformatoria a la ley especial de telecomunicaciones.

1. Controlar y monitorear el uso del espectro radioeléctrico.
2. Controlar las actividades técnicas de los operadores de los servicios de telecomunicaciones.
3. Controlar la correcta aplicación de los pliegos tarifarios aprobados por el CONATEL.

---

1 http://www.supertel.gov.ec/organizacion/organizacion1.htm

4. Supervisar el cumplimiento de las concesiones y permisos otorgados para la explotación del servicio de telecomunicaciones.
5. Supervisar el cumplimiento de las normas de homologación y normalización aprobadas por el CONATEL.
6. Cumplir y hacer cumplir las resoluciones del CONATEL.
7. Aplicar las normas de protección del mercado y estimular la libre competencia; y,
8. Juzgar a las personas naturales y jurídicas que incurran en las infracciones señaladas en la Ley y aplicar las sanciones en los casos que corresponda.

Dentro de este Organismo de control, se ha creado la Dirección de Investigación Especial en Telecomunicaciones, la misma que tiene como misión principal, controlar y combatir los servicios de telecomunicaciones ilegales, como es el caso de TV cable no autorizado, radiodifusoras que operan sin autorización y principalmente lo que se refiere con el servicio de telefonía internacional ilegal denominado By pass.

De las diferentes infracciones que se cometen en el sector de las telecomunicaciones, y que esta dirección está encargada de combatir, el que más perjuicio origina a las operadoras de telefonía y al estado Ecuatoriano lo constituye el By pass[2], que en los últimos años ha causado perdidas millonarias. Como ya se menciono, se tiene tres periodos de evolución tecnológica de los sistemas de By pass.

---

2 Revista trimestral CIEEPI, Publicación: 07/24/2003.

3.1.1 ANÁLISIS DE TRÁFICO TELEFÓNICO INTERNACIONAL TOTAL (ENTRANTE Y SALIENTE) A ECUADOR

3.1.1.1 Tráfico telefónico internacional total (entrante y saliente) según datos publicados por la SUPTEL

Los datos publicados por la SUPTEL (Superintendencia de Telecomunicaciones) [3] indica la cantidad de tráfico telefónico internacional total anual (entrante y saliente) cursado por las operadoras telefónicas ANDINATEL S.A., PACIFICTEL S.A. Y ETAPA, expresado en minutos desde 1992 hasta noviembre del 2005, los datos se indican en la siguiente tabla.

Tráfico telefónico internacional total anual, cursado por ANDINATEL S.A., PACIFICTEL S.A. Y ETAPA	
Datos publicados por la SUPTEL	
Año	Cantidad (minutos)
1992	115917715
1993	136017117
1994	164013014
1995	192903092
1996	230128193
1997	241089010
1998	206239654
1999	317141521
2000	529574110
2001	649655252
2002	877228435
2003	1144001401
2004	1258413146
Nov. 2005	1216180236

Tabla 3.1. Tráfico telefónico internacional total anual publicado por la SUPTEL

3 http://www.supertel.gov.ec/no_autorizados/trafico.htm

3.1.1.2 Tendencia de crecimiento del tráfico telefónico internacional total (entrante y saliente) a Ecuador

La tendencia de crecimiento del tráfico telefónico internacional total (entrante y saliente) a Ecuador permite estimar el desarrollo que debió existir si no hubiera desviación de un importante volumen de tráfico telefónico que termina en rutas ilegales, como es el caso del By pass.

Para estimar la tendencia de crecimiento del tráfico telefónico internacional total se consideran aspectos como son:

- Entre los años 1992 y 1995, antes de que en Ecuador se introduzca el fraude telefónico con diversas modalidades como el Call back o el By pass, el tráfico telefónico internacional total tramitado por las operadoras telefónicas ANDINATEL S.A., PACIFICTEL S.A. y ETAPA presentó un crecimiento promedio anual normal del 19.09 %.

  Factor de proyección en el año 1994 respecto al año 1993.

$$Factor = \frac{|164013014\,Minutos - 136017117\,Minutos|}{136017117\,Minutos} = 0{,}2058 \rightarrow 20{,}58\%$$

  Factor de proyección en el año 1995 respecto al año 1994.

$$Factor = \frac{|192903092\,Minutos - 164013014\,Minutos|}{164013014\,Minutos} = 0{,}1761 \rightarrow 17{,}61\%$$

$$Factor\_promedio = \frac{0.2058 + 0.1761}{2} = 0{,}1909 \rightarrow 19.09\%$$

- Entre los años 1995 y 1997 la tendencia de crecimiento del 19.09 % se mantuvo al permanecer constante las condiciones generales en el Ecuador.

  Adicionalmente se debe mencionar que la tendencia mundial de crecimiento del tráfico telefónico internacional desde el año 1992 hasta el año 1997 se mantuvo prácticamente constante con una ligera tendencia a la baja.

- En el año 1998, existieron tres factores que modificaron el crecimiento del tráfico telefónico internacional en el Ecuador, dos de ellos favorecieron el crecimiento, y son:

  1. El gran volumen de migrantes del Ecuador hacia otros países, especialmente hacia España, el número de migrantes se duplicó respecto del año 1997, y en el 1999 se duplico respecto del año 1998, y en los años subsiguientes el número de migrantes se ha mantenido en altos niveles, estas personas potencialmente generan tráfico telefónico internacional por la necesidad de mantenerse comunicados con sus familiares.

  2. Fue notorio en Ecuador y en el mundo, la tendencia a la baja de las tasas de liquidación y tasa de terminación[4] a partir del año 1998.

  Uno de ellos por el contrario disminuyo su crecimiento:

  3. La tendencia mundial de crecimiento del tráfico telefónico internacional a partir del año 1998 ha decrecido significativamente, especialmente por la utilización de redes privadas y la utilización del Internet, que ha captado un importante segmento del volumen de tráfico telefónico internacional.

---

4 **ANEXO G.** Interconexión internacional

Por lo expuesto, entre los años 1997 y 1999, el tráfico telefónico internacional total tramitado por las operadoras telefónicas ANDINATEL S.A., PACIFICTEL S.A. y ETAPA presentó un crecimiento anual normal del 34,11 %.

Factor de proyección en el año 1998 respecto al año 1997.

$$Factor = \frac{|206239654\,Minutos - 241089010\,Minutos|}{241089010\,Minutos} = 0{,}1445 \rightarrow 14{,}45\%$$

Factor de proyección en el año 1999 respecto al año 1998.

$$Factor = \frac{|317141521\,Minutos - 206239654\,Minutos|}{206239654\,Minutos} = 0{,}5377 \rightarrow 53{,}77\%$$

$$Factor\_promedio = \frac{0{,}1445 + 0{,}5377}{2} = 0{,}3411 \rightarrow 34.11\%$$

- Entre los años 1999 y 2004 la tendencia de crecimiento del 34,11% se mantuvo al permanecer prácticamente constante las condiciones generales en el Ecuador.

Considerando el factor de crecimiento se obtiene la proyección de tráfico telefónico internacional total (entrante y saliente) a Ecuador, los datos se indican en la tabla 3.2.

3.1.1.3 Comparación de la curva de tráfico telefónico internacional total según datos publicados por la SUPTEL, y la curva de tendencia de crecimiento del tráfico telefónico internacional total.

Considerando el tráfico telefónico internacional total (entrante y saliente) cursado por las operadoras telefónicas ANDINATEL S.A. PACIFICTEL S.A. Y ETAPA obtenido según datos publicados por la SUPTEL (Superintendencia de Telecomunicaciones), y teniendo en cuenta su tendencia de crecimiento, se puede estimar la cantidad de minutos perdidos. Debido a que se está trabajando con el tráfico telefónico internacional total y la tasa de terminación de llamadas internacionales[5] es aplicado a llamadas entrantes a Ecuador, no se puede estimar el perjuicio económico.

Tráfico telefónico internacional total anual, cursado por ANDINATEL S.A., PACIFICTEL S.A. Y ETAPA			
Datos publicados por la SUPTEL		Proyección del tráfico telefónico internacional total anual	Pérdida del tráfico telefónico internacional total anual debido al fraude en telefonía
Año	Tráfico telefónico internacional total anual (minutos)	(minutos)	(minutos)
1992	115917715	115917715,00	0,00
1993	136017117	138046406,79	2029289,79
1994	164013014	164399465,85	386451,85
1995	192903092	195783323,88	2880231,88
1996	230128193	233158360,41	3030167,41
1997	241089010	277668291,41	36579281,41
1998	206239654	372392433,49	166152779,49
1999	317141521	499430899,41	182289378,41
2000	529574110	669807441,98	140233331,98
2001	649655252	898306472,14	248651220,14
2002	877228435	1204755975,11	327527540,11
2003	1144001401	1615748082,17	471746681,17
2004	1258413146	2166946600,77	908533454,77

Tabla 3.2. Cantidad, proyección y diferencia del tráfico telefónico internacional total anual, cursado por ANDINATEL S.A., PACIFICTEL S.A. Y ETAPA

5 **ANEXO G.** Interconexión internacional

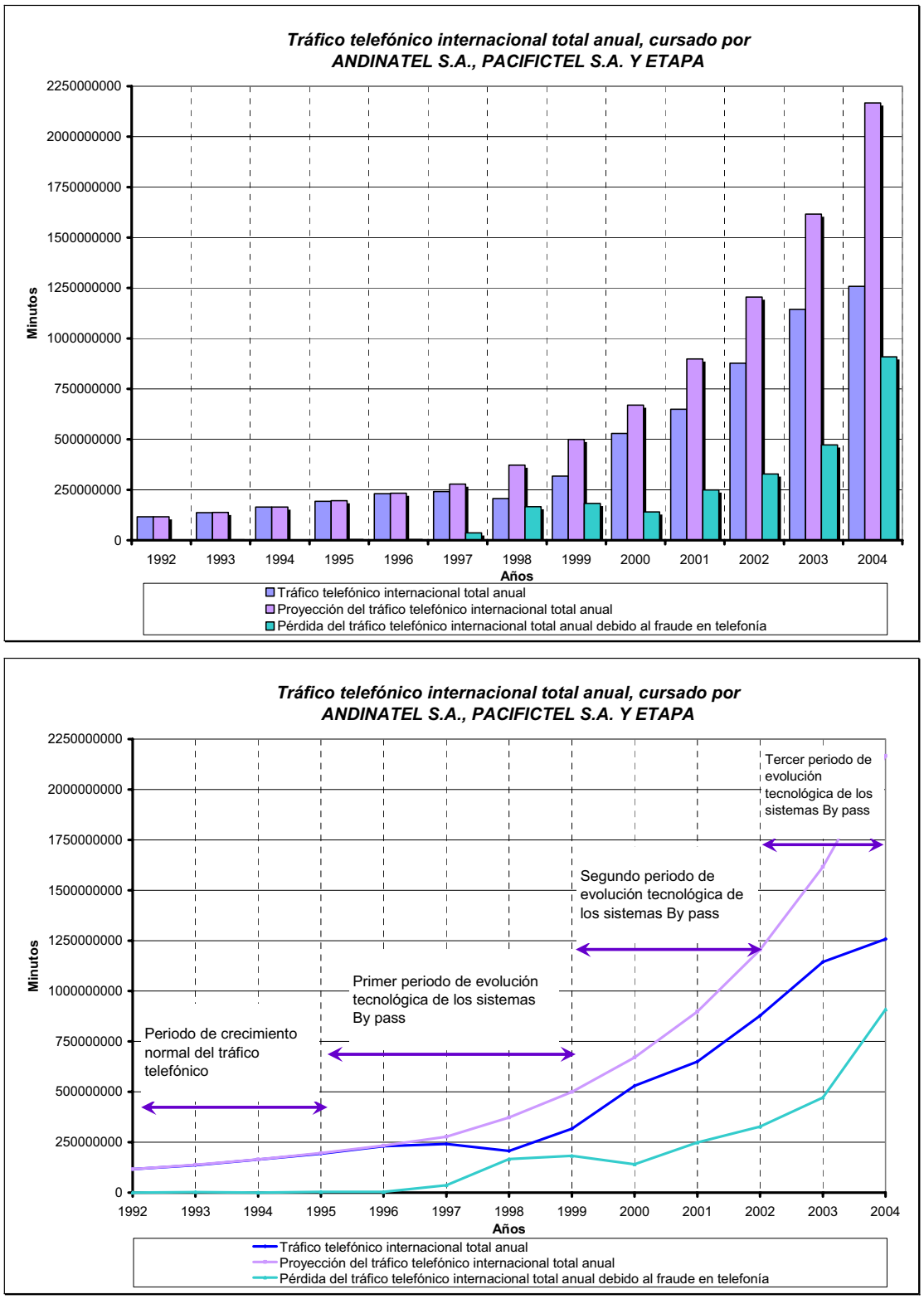


Figura 3.1. Comparación de curvas del tráfico telefónico internacional total

En la figura 3.1 correspondiente a la comparación de curvas del tráfico telefónico internacional total, tráfico que ha sido cursado por las operadoras telefónicas ANDINATEL S.A. PACIFICTEL S.A. Y ETAPA, se observa el decrecimiento de la cantidad de minutos en el año 1998 correspondiente al primer periodo de evolución tecnológica de los sistemas By pass, periodo en el cual las operadoras telefónicas y el ente regulador de telecomunicaciones no contaban con las herramientas adecuadas para contrarrestar dicho fraude telefónico. Evidenciándose una pérdida de tráfico telefónico considerable en comparación a los años anteriores.

De acuerdo a las curvas de tráfico mostradas se estima que el volumen de tráfico telefónico internacional total (entrante y saliente) perdido en 1998, año en el cual se tuvo el auge del fraude en la telefonía especialmente en cuanto a By pass se refiere, es de 166’152779,49 de minutos anuales.

La recuperación de tráfico telefónico internacional alcanzada en el año 2000 correspondiente al segundo periodo de evolución tecnológica de los sistemas By pass, es el resultado de la acción conjunta de la Superintendencia de Telecomunicaciones y las operadoras telefónicas en el combate al By pass. Evidenciándose el aumento de tráfico telefónico en comparación al primer periodo de evolución tecnológica de los sistemas By pass.

En el tercer periodo de evolución tecnológica de los sistemas By pass se observa un mínimo crecimiento del tráfico telefónico internacional resultado del incremento del By pass. Evidenciándose un aumento paulatino de minutos telefónicos en comparación a las del primer y segundo periodo de evolución tecnológica de los sistemas By pass.

3.2 FCC (FEDERAL COMMUNICATIONS COMMISSION)

La FCC se estableció en 1934 como una agencia gubernamental Norte americana independiente de la rama ejecutiva y directamente responsable ante el Congreso. La FCC regula las comunicaciones interestatales e internacionales por televisión, radio, alambre, satélite y cable en todos los 50 estados y los territorios Norte americanos [6].

El tráfico telefónico internacional entrante y saliente cursado por las operadoras que poseen concesión de servicios de telecomunicaciones[7] establecidas en el Ecuador, esta distribuido como tráfico FCC y tráfico restante.

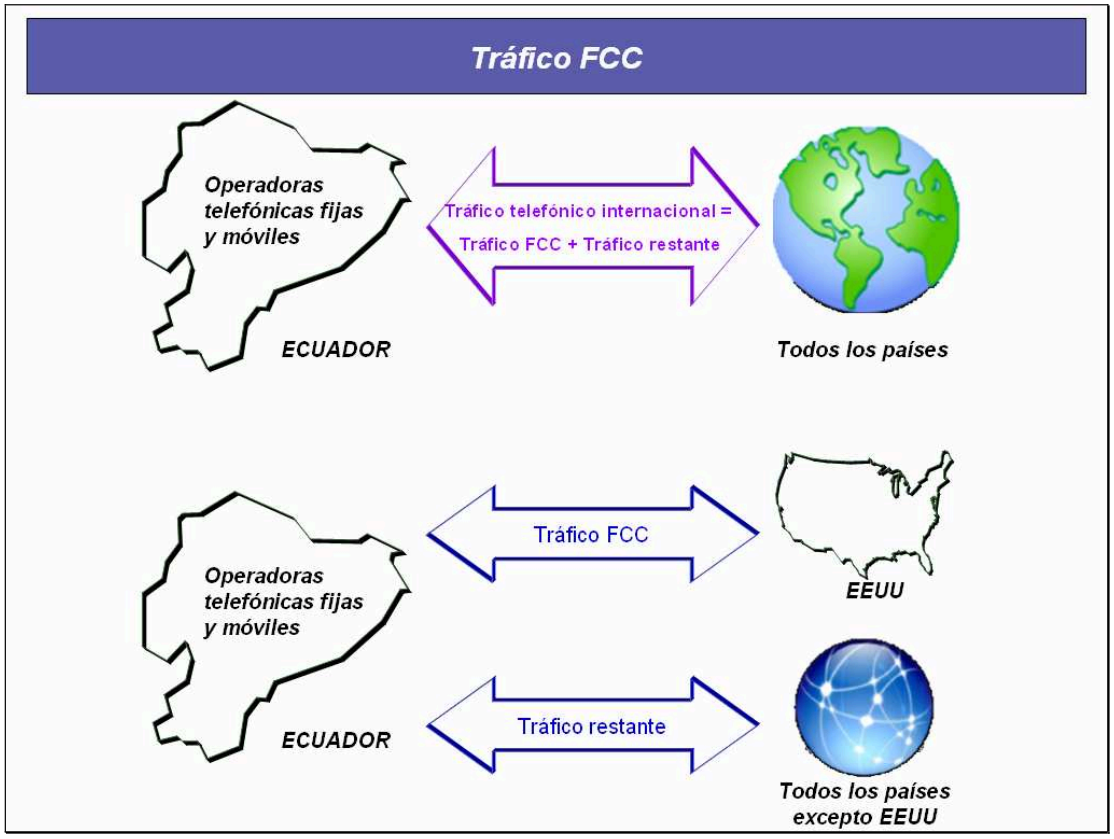


Figura 3.2. Tráfico FCC

6 www.fcc.gov

7 **ANEXO H.** Operadoras que poseen concesión de servicio de telecomunicaciones y están autorizadas a cursar tráfico telefónico internacional

Es decir, la distribución del tráfico telefónico internacional esta dada de la forma:

- Tráfico FCC. Tráfico telefónico internacional enviado desde Ecuador hacia Estados Unidos y desde Estados Unidos hacia Ecuador.

- Tráfico restante. Tráfico telefónico internacional enviado desde Ecuador hacia el resto de países y desde el resto de países hacia Ecuador, excepto Estados Unidos.

La FCC considera un solo tráfico telefónico internacional (tráfico FCC) enviado, desde Ecuador hacia Estados Unidos y desde Estados Unidos hacia Ecuador.

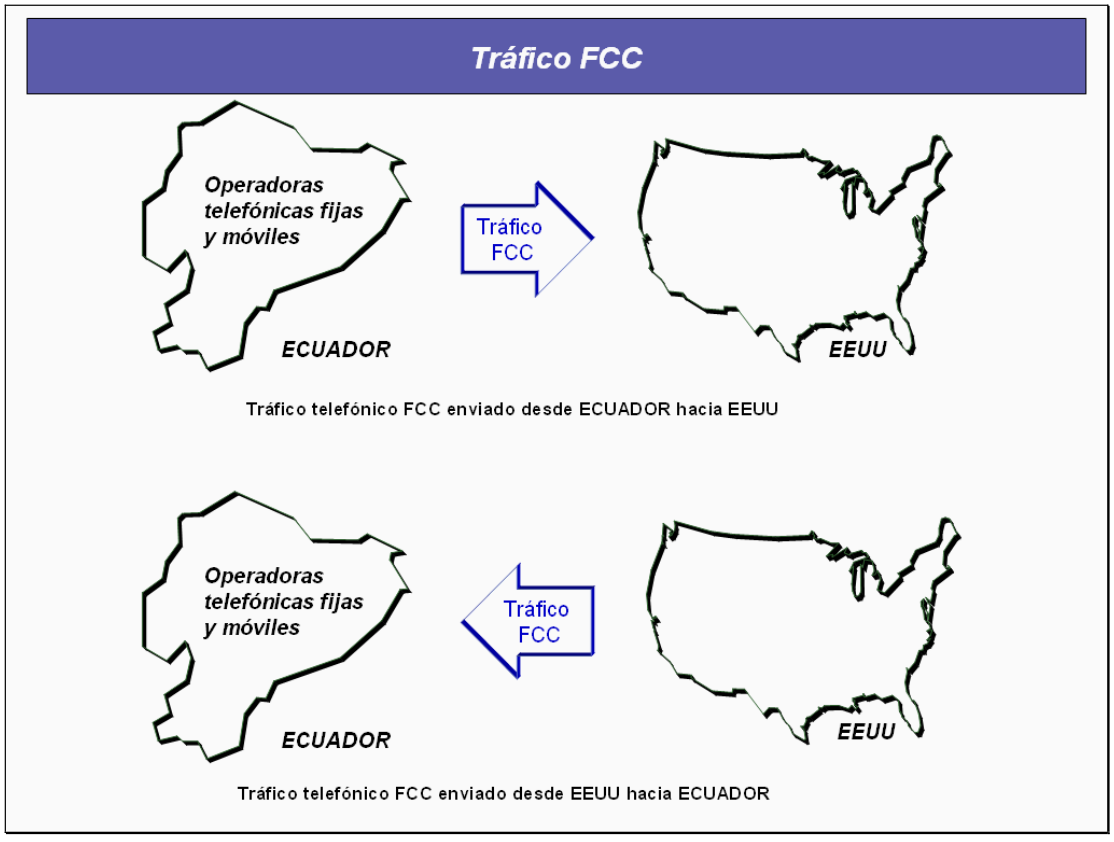


Figura 3.3. Cont. Tráfico FCC

3.2.1 ANÁLISIS DE TRÁFICO TELEFÓNICO FCC TOTAL (ENTRANTE Y SALIENTE) A ECUADOR

3.2.1.1 Tráfico telefónico FCC total (entrante y saliente) a Ecuador según datos publicados por la FCC.

Según datos publicados por la FCC[8], la cantidad de tráfico telefónico internacional enviado, desde Ecuador hacia Estados Unidos y desde Estados Unidos hacia Ecuador, expresado en minutos desde 1992 al 2003 es:

Year (Año)	Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) **Saliente de los Estados Unidos**				
	Number of Messages (número de llamadas)	Number of Minutes (Número de minutos)	U.S. Carriers Revenues (Ganancias de los Carriers de USA)	Payout to Foreingn Carriers (Pagos realizados a otros Carriers)	Retained Revenues (Ganancias Retenidas)
1992	7440306	73261608	83385139	58721086	24664053
1993	9464592	86366059	98419004	67069944	31349060
1994	12946873	108585707	119769625	81674158	38095467
1995	17783097	132893438	143158465	92802296	50356169
1996	21420429	156614864	136632027	96030416	40601611
1997	26576553	184854451	140975592	88810053	52165539
1998	16309744	111930104	96207653	50074040	46133613
1999	31219423	197980110	107297742	67571538	39726204
2000	51776946	303335545	130928057	75383274	55544783
2001	42883792	296758097	104692784	56143270	48449514
2002	40366053	323293619	60253979	44000360	16253619
2003	68181122	602202531	98048316	63813302	34235014

Year (Año)	Traffic Billed in Foreign Countries (Tráfico facturado en otros paises) **Entrante a los Estados Unidos**							Total U.S. Carriers Retained Revenues (Total de ganancias retenidas por Carriers de USA)
	Originating or Terminating in the United States (Originado o terminado en los Estados Unidos)			Transiting the United States (by Country of Origin) (Tránsito en los Estados Unidos, por pais de origen)				
	Number of Messages (número de llamadas)	Number of Minutes (Número de minutos)	Receipts from Foreign Carriers (Pagos de carriers extrangeros)	Number of Minutes	Receipts from Foreign Carriers	Payout to Foreingn Carriers	Retained Revenues	
1992	2460143	11628951	9414389		381736	292547	89189	34167631
1993	2642233	12131226	9388051		762807	410203	352604	41089715
1994	3039884	12918191	9530772		1480038	991798	488240	48114479
1995	3198970	12864995	9132272		1836723	1196973	639750	60128191
1996	3602222	15112971	9454113		4235166	2907662	1327504	51383228
1997	3776165	17413209	13602076		7404813	5415813	1989000	67756615
1998	2426354	13563630	8569039		25585623	22024513	3561110	58263762
1999	3281890	14269553	5174763		1401034	657121	743913	45644880
2000	3353036	15693507	3953666		7279969	5133724	2146245	61644694
2001	4918274	29350629	6053352		953217	224182	729035	55231901
2002	3912378	20643413	2243382		1298994	158378	1140616	19637617
2003	13141980	88691918	989244		137414	5	137409	35361667

Tabla 3.3. Tráfico telefónico internacional anual publicado por la FCC

8 http://www.fcc.gov/wcb/iatd/intl.html

De la tabla 3.3 correspondiente al tráfico telefónico internacional anual publicado por la FCC, considerando únicamente el tráfico telefónico FCC total (entrante y saliente) a Ecuador se tiene:

Tráfico telefónico FCC total anual (entrante y saliente) a Ecuador			
	Datos publicados por la FCC		
Year (Año)	**Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) Saliente de los Estados Unidos**	**Traffic Billed in Foreign Countries (Tráfico facturado en otros paises) Entrante a los Estados Unidos**	**Tráfico telefónico total entrante y saliente**
	Number of Minutes (Número de minutos)	Number of Minutes (Número de minutos)	(Número de minutos)
1992	73261608	11628951	84890559
1993	86366059	12131226	98497285
1994	108585707	12918191	121503898
1995	132893438	12864995	145758433
1996	156614864	15112971	171727835
1997	184854451	17413209	202267660
1998	111930104	13563630	125493734
1999	197980110	14269553	212249663
2000	303335545	15693507	319029052
2001	296758097	29350629	326108726
2002	323293619	20643413	343937032
2003	602202531	88691918	690894449

Tabla 3.4. Cantidad de tráfico telefónico FCC total anual reportado por la FCC

3.2.1.2 Tendencia de crecimiento del tráfico telefónico FCC total (entrante y saliente) a Ecuador

La tendencia de crecimiento del tráfico telefónico FCC total (entrante y saliente) a Ecuador permite estimar el desarrollo que debió existir si no hubiera desviación de un importante volumen de tráfico telefónico que termina en rutas ilegales.

Para estimar la tendencia de crecimiento del tráfico telefónico FCC total (entrante y saliente) a Ecuador se consideran aspectos como son:

- Entre los años 1992 y 1995, antes de que en Ecuador se introduzca el fraude telefónico, el tráfico telefónico internacional total tramitado por la FCC presentó un crecimiento promedio anual normal del 21,65 %.

  Factor de proyección en el año 1994 respecto al año 1993.

$$Factor = \frac{|121503898\,Minutos - 98497285\,Minutos|}{98497285\,Minutos} = 0{,}2336 \rightarrow 23{,}36\%$$

  Factor de proyección en el año 1995 respecto al año 1994.

$$Factor = \frac{|145758433\,Minutos - 121503898\,Minutos|}{121503898\,Minutos} = 0{,}1996 \rightarrow 19{,}96\%$$

$$Factor\_promedio = \frac{0.2336 + 0.1996}{2} = 0{,}2165 \rightarrow 21{,}65\%$$

- En el año 1998 se tiene un gran volumen de migrantes del Ecuador hacia otros países, estas personas eventualmente generan tráfico telefónico internacional, sin embargo debido a que el tráfico telefónico FCC es reportado por Estados Unidos y la gran cantidad de migrantes ha sido hacia España, se considera que el factor de crecimiento para el tráfico telefónico FCC se mantiene en el 21,65 % entre los años 1992 y 2003.

Considerando el factor de crecimiento se obtiene la proyección de tráfico telefónico FCC total, los datos se indican en la tabla 3.5.

3.2.1.3 Comparación de la curva de tráfico telefónico FCC total según datos publicados por la FCC, y la curva de tendencia de crecimiento del tráfico telefónico FCC total.

Considerando el tráfico telefónico FCC total (entrante y saliente) a Ecuador, obtenido según datos publicados por la FCC (Federal Communications Commission), y teniendo en cuenta su tendencia de crecimiento, se puede estimar la cantidad de minutos perdidos. Debido a que se está trabajando con el tráfico telefónico FCC total y la tasa de terminación de llamadas internacionales[9] es aplicado a llamadas entrantes a Ecuador, no se puede estimar el perjuicio económico.

Tráfico telefónico FCC total anual (entrante y saliente) a Ecuador					
Datos publicados por la FCC			**Tráfico telefónico total entrante y saliente**	**Proyección del tráfico telefónico total entrante y saliente**	**Pérdida del tráfico telefónico total entrante y saliente debido al fraude en telefonía**
Year (Año)	**Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) Saliente de los Estados Unidos**	**Traffic Billed in Foreign Countries (Tráfico facturado en otros paises) Entrante a los Estados Unidos**			
	Number of Minutes (Número de minutos)	Number of Minutes (Número de minutos)	(Número de minutos)	(Número de minutos)	(Número de minutos perdidos)
1992	73261608	11628951	84890559	84890559,00	0,00
1993	86366059	12131226	98497285	103277663,56	4780378,56
1994	108585707	12918191	121503898	125647373,71	4143475,71
1995	132893438	12864995	145758433	152862312,87	7103879,87
1996	156614864	15112971	171727835	185971946,78	14244111,78
1997	184854451	17413209	202267660	226253053,09	23985393,09
1998	111930104	13563630	125493734	275258956,62	149765222,62
1999	197980110	14269553	212249663	334879428,88	122629765,88
2000	303335545	15693507	319029052	407413561,62	88384509,62
2001	296758097	29350629	326108726	495658424,73	169549698,73
2002	323293619	20643413	343937032	603016927,15	259079895,15
2003	602202531	88691918	690894449	733629040,25	42734591,25

Tabla 3.5. Cantidad, proyección y diferencia del tráfico telefónico FCC total anual, reportado por la FCC

9 **ANEXO G.** Interconexión internacional

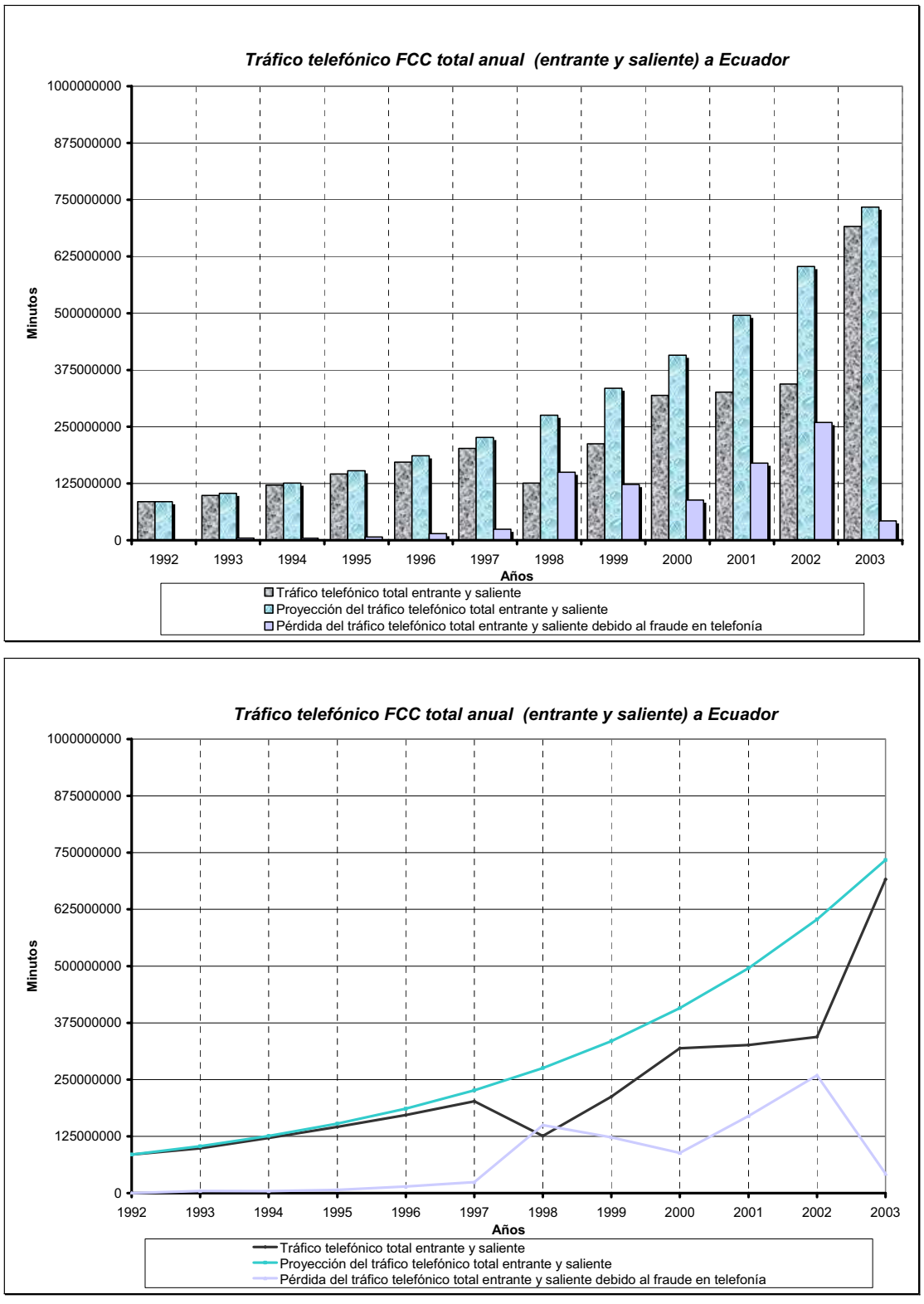


Figura 3.4. Comparación de curvas del tráfico telefónico FCC total

De acuerdo a las curvas de tráfico mostradas se estima que el volumen de tráfico telefónico FCC total (entrante y saliente) perdido en 1998, año en el cual se tuvo el auge del fraude en la telefonía especialmente en cuanto a By pass se refiere, es de 149'765222,62 de minutos anuales.

3.2.2 ANÁLISIS DE TRÁFICO TELEFÓNICO FCC ENTRANTE A ECUADOR

3.2.2.1 Tráfico telefónico FCC entrante a Ecuador según datos publicados por la FCC.

De la tabla 3.3 correspondiente al tráfico telefónico internacional anual publicado por la FCC, considerando únicamente el tráfico telefónico FCC entrante a Ecuador (saliente de los Estados Unidos) se tiene:

Tráfico telefónico FCC anual entrante a Ecuador	
Datos publicados por la FCC	
Year (Año)	**Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) Saliente de los Estados Unidos**
	Number of Minutes (Número de minutos)
1992	73261608
1993	86366059
1994	108585707
1995	132893438
1996	156614864
1997	184854451
1998	111930104
1999	197980110
2000	303335545
2001	296758097
2002	323293619
2003	602202531

Tabla 3.6. Cantidad de tráfico telefónico FCC anual entrante a Ecuador reportado por la FCC

3.2.2.2 Tendencia de crecimiento del tráfico telefónico FCC entrante a Ecuador

La tendencia de crecimiento del tráfico telefónico FCC entrante a Ecuador permite estimar el desarrollo que debió existir si no hubiera desviación de un importante volumen de tráfico telefónico que termina en rutas ilegales.

Para estimar la tendencia de crecimiento del tráfico telefónico FCC entrante a Ecuador se consideran aspectos como son:

- Entre los años 1992 y 1995, antes de que en Ecuador se introduzca el fraude telefónico, el tráfico telefónico FCC entrante a Ecuador presentó un crecimiento promedio anual normal del 24,06 %.

  Factor de proyección en el año 1994 respecto al año 1993.

$$Factor = \frac{|108585707\,Minutos - 86366059\,Minutos|}{86366059\,Minutos} = 0{,}2573 \rightarrow 25{,}73\%$$

  Factor de proyección en el año 1995 respecto al año 1994.

$$Factor = \frac{|132893438\,Minutos - 108585707\,Minutos|}{108585707\,Minutos} = 0{,}2239 \rightarrow 22{,}39\%$$

$$Factor\_promedio = \frac{0.2573 + 0.2239}{2} = 0{,}2406 \rightarrow 24{,}06\%$$

- Al igual que en el análisis realizado para el tráfico telefónico FCC total, en el año 1998 se tiene un gran volumen de migrantes del Ecuador y debido a que el tráfico telefónico FCC es reportado por Estados Unidos y la gran cantidad de migrantes a sido hacia España, se considera que el factor de crecimiento para el tráfico telefónico FCC entrante a Ecuador se mantiene en el 24,06 % entre los años 1992 y 2003.

Considerando el factor de crecimiento se obtiene la proyección de tráfico telefónico FCC entrante a Ecuador, los datos se indican en la tabla 3.7.

3.2.2.3 Comparación de la curva de tráfico telefónico FCC entrante a Ecuador según datos publicados por la FCC y la curva de tendencia de crecimiento del tráfico telefónico FCC entrante a Ecuador.

Considerando el tráfico telefónico FCC entrante a Ecuador, obtenido según datos publicados por la FCC (Federal Communications Commission), y teniendo en cuenta su tendencia de crecimiento, se puede estimar la cantidad de minutos perdidos debido al fraude en telefonía y el perjuicio económico considerando un valor de referencia para la tasa de terminación de llamadas internacionales[10] de 11.8 centavos el minuto.

Tráfico telefónico FCC anual entrante a Ecuador				
Datos publicados por la FCC		**Proyección. Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) Saliente de los Estados Unidos**	**Pérdida. Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) Saliente de los Estados Unidos**	**Pérdida económica**
Year (Año)	**Traffic Billed in the United States (Tráfico facturado en los Estados Unidos) Saliente de los Estados Unidos**			
	Number of Minutes (Número de minutos)	Number of Minutes (Número de minutos)	(Número de minutos perdidos)	(Dólares)
1992	73261608	73261608,00	0,00	$ 0,00
1993	86366059	90885804,09	4519745,09	$ 533.329,92
1994	108585707	112749769,09	4164062,09	$ 491.359,33
1995	132893438	139873444,01	6980006,01	$ 823.640,71
1996	156614864	173522132,21	16907268,21	$ 1.995.057,65
1997	184854451	215265525,07	30411074,07	$ 3.588.506,74
1998	111930104	267050927,12	155120823,12	$ 18.304.257,13
1999	197980110	331294096,69	133313986,69	$ 15.731.050,43
2000	303335545	410991939,57	107656394,57	$ 12.703.454,56
2001	296758097	509862312,91	213104215,91	$ 25.146.297,48
2002	323293619	632517461,05	309223842,05	$ 36.488.413,36
2003	602202531	784679173,96	182476642,96	$ 21.532.243,87

Tabla 3.7. Cantidad, proyección y diferencia del tráfico telefónico FCC entrante a Ecuador, reportado por la FCC

10 **ANEXO G.** Interconexión internacional

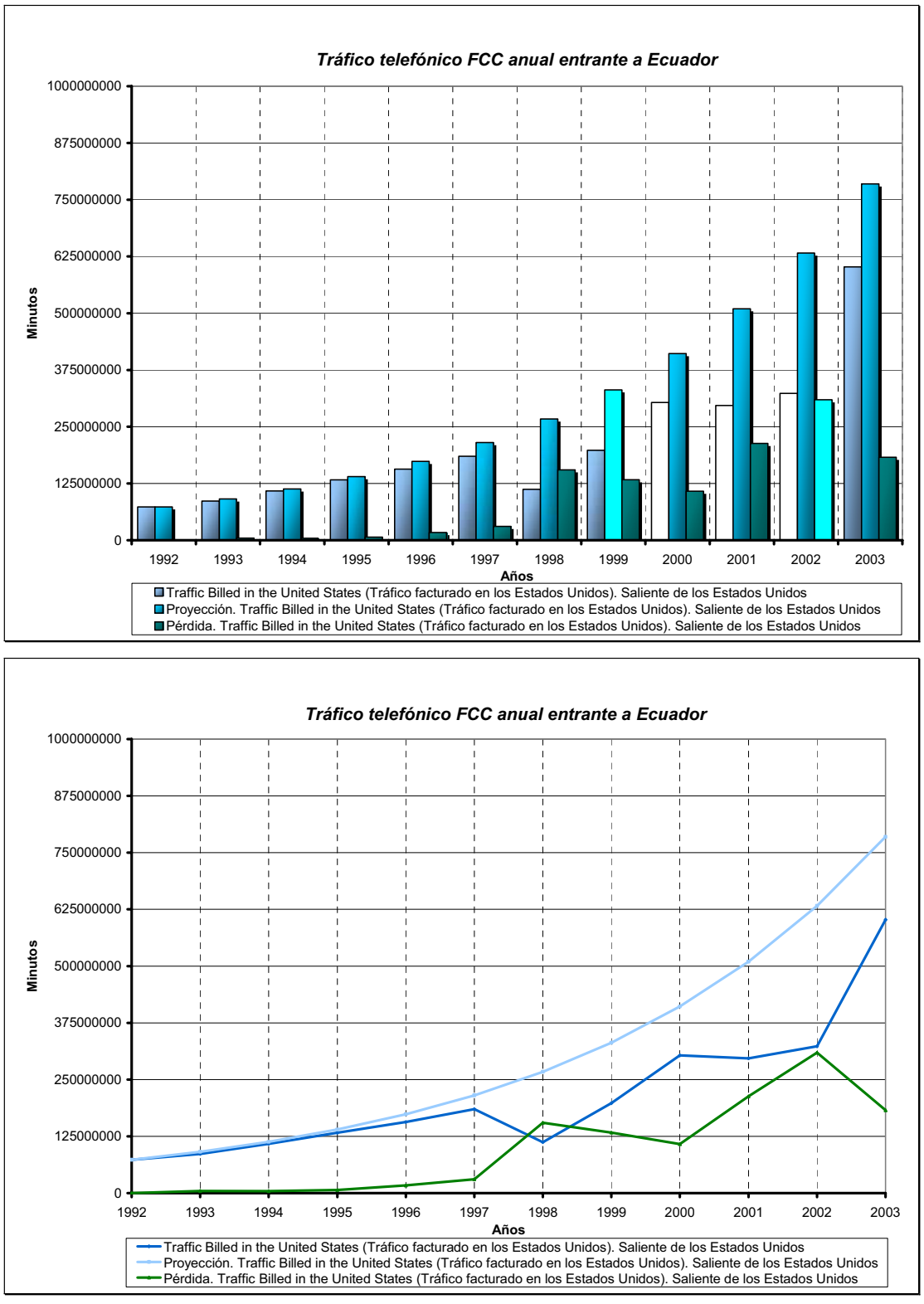


Figura 3.5. Comparación de curvas del tráfico telefónico FCC entrante a Ecuador

En la figura 3.5 correspondiente a la Comparación de curvas del tráfico telefónico FCC entrante a Ecuador, tráfico que ha sido reportado por la FCC, se observa el decrecimiento de la cantidad de minutos cursado por la FCC en el año 1998, dicho año corresponde al primer periodo de evolución tecnológica de los sistemas By pass en el Ecuador. Evidenciándose una pérdida de tráfico telefónico considerable en comparación a los años anteriores.

De acuerdo a las curvas de tráfico mostradas se estima que el volumen de tráfico telefónico FCC entrante al Ecuador perdido en 1998, año en el cual se tuvo el auge del fraude en la telefonía especialmente en cuanto a By pass se refiere, es de 155'120823,12 de minutos anuales, lo cual representa un perjuicio económico de $18.304.257,13 considerando un valor de referencia para la tasa de terminación de llamadas internacionales[11] de 11.8 centavos el minuto.

Otro factor que ha ocasionado el decrecimiento del tráfico telefónico FCC en el primer periodo de evolución tecnológica de los sistemas By pass en el Ecuador, es la exagerada oferta de tarjetas, que permiten realizar llamadas telefónicas, que en el mercado se denominan: "International Phone Card & International Calling Card", estas se expenden libremente en países como Estados Unidos, también se las promocionan y venden a través del Internet.

La gran cantidad de oferta de tarjetas con costos exageradamente bajos, demuestra el crecimiento que el By pass adquirió durante el año 1998. Los valores de estas tarjetas van desde los 4 centavos de dólar el minuto de llamadas telefónicas a Ecuador.

La recuperación de tráfico telefónico FCC alcanzada en el año 2000 es el resultado de la acción conjunta del ente regulador de las Telecomunicaciones y las operadoras telefónicas en Ecuador. Evidenciándose la disminución de pérdidas económicas en comparación a las de años anteriores.

---

11 **ANEXO G.** Interconexión internacional

3.3 COMPARACIÓN DE LA CURVA DE TRÁFICO TELEFÓNICO INTERNACIONAL SEGÚN DATOS PUBLICADOS POR LA SUPTEL Y LA CURVA DE TRÁFICO TELEFÓNICO INTERNACIONAL SEGÚN DATOS PUBLICADOS POR LA FCC

Considerando el tráfico telefónico internacional total anual (entrante y saliente) cursado por las operadoras telefónicas ANDINATEL S.A. PACIFICTE S.A. Y ETAPA según datos publicados por la SUPTEL (Superintendencia de Telecomunicaciones) indicados en la tabla 3.1, y teniendo en cuenta el tráfico telefónico FCC total anual (entrante y saliente) según datos publicados por la FCC (Federal Communications Commission) indicados en la tabla 3.4, se realiza la comparación de las curvas lo cual permite observar el progreso que ha tenido el tráfico telefónico desde el año 1992 hasta el año 2003.

De las tablas indicadas anteriormente, considerando únicamente el tráfico telefónico total (entrante y saliente) a Ecuador se tiene:

Tráfico telefónico total anual (entrante y saliente) a Ecuador		
Year (Año)	*Datos publicados por la SUPTEL*	*Datos publicados por la FCC*
	Tráfico telefónico total (entrante y saliente)	Tráfico telefónico total (entrante y saliente)
	(Número de minutos)	(Número de minutos)
1992	115917715	84890559
1993	136017117	98497285
1994	164013014	121503898
1995	192903092	145758433
1996	230128193	171727835
1997	241089010	202267660
1998	206239654	125493734
1999	317141521	212249663
2000	529574110	319029052
2001	649655252	326108726
2002	877228435	343937032
2003	1144001401	690894449

Tabla 3.8. Cantidad de tráfico telefónico internacional anual reportado por la SUPTEL y la FCC

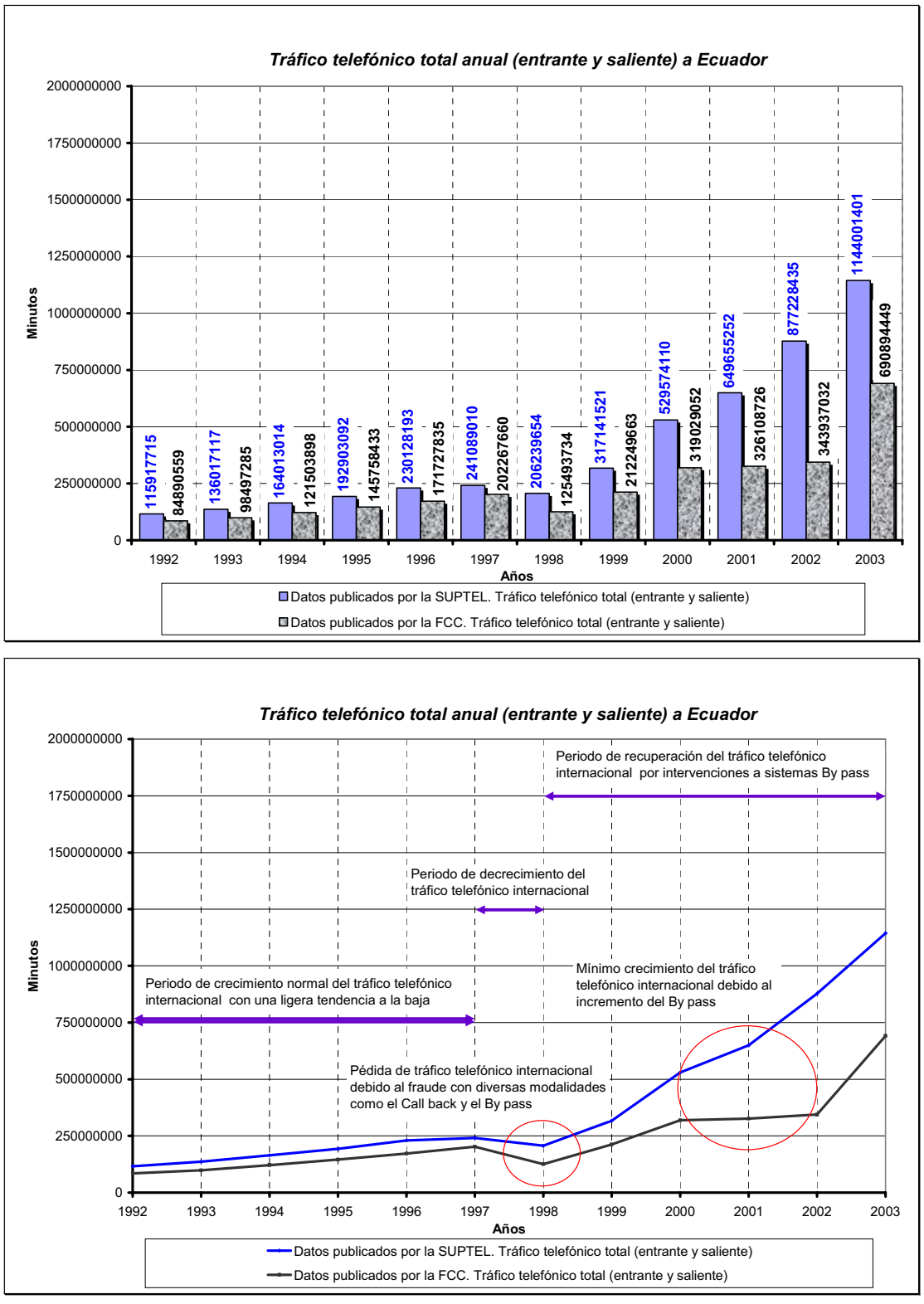


Figura 3.6. Comparación de curvas del tráfico telefónico según datos publicados por la SUPTEL y la FCC

Al analizar el tráfico telefónico internacional total cursado por las operadoras telefónicas fijas ANDINATEL S.A. PACIFICTEL S.A. Y ETAPA, y al compararlo con el tráfico FCC total no se puede realizar estimaciones de minutos perdidos ni perdidas económicas por fraude, debido a que:

- La SUPTEL considera el tráfico telefónico cursado solo por las operadoras telefónicas fijas, mientras que la FCC considera el tráfico telefónico cursado por operadoras fijas y móviles establecidas en Ecuador.

- El tráfico telefónico internacional cursado por las operadoras telefónicas fijas está considerado como el tráfico FCC más tráfico restante.

Sin embargo, tanto en la curva de tráfico telefónico internacional según datos publicados por la SUPTEL y la curva de tráfico telefónico internacional según datos publicados por la FCC se observa:

- La disminución de tráfico telefónico internacional entre los años 1997 y 1998 es el resultado del auge que en dicho periodo tuvo el fraude a la telefonía con diversas modalidades como el Call back y el By pass, periodo en el cual se evidencia la pérdida considerable de minutos en comparación a los años anteriores.

- El mínimo crecimiento del tráfico telefónico internacional comprendido entre los años 2000 y 2002 se debe al incremento del By pass, que para dicho periodo maneja una tecnología de punta que imposibilita su detección sin la asistencia de equipos especializados en el control del fraude telefónico.

CAPÍTULO

IV

Conclusiones y recomendaciones

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El fraude telefónico nunca podrá ser eliminado pues el problema evoluciona al ritmo de la tecnología, sin embargo puede ser reducido significativamente con un adecuado sistema de detección, control y gestión del fraude en Telecomunicaciones.

- El fraude en telecomunicaciones se produce en todos los países del mundo, incluyendo a Ecuador, produciendo pérdidas económicas millonarias a las operadoras locales de cada país. Este fraude no solo involucra a las empresas de telefonía fija, sino también a las celulares.

- Un adecuado sistema de detección, control y gestión del fraude en telecomunicaciones requiere por parte de las operadoras telefónicas el desarrollo de una estructura funcional y operativa que debidamente organizada de cómo resultado la conformación de un equipo de trabajo que responda de manera pro activa para combatir el fraude.

- A pesar de que cada tipo de fraude implica diversos motivos, medios, modos y métodos, se considera la adopción de determinadas acciones de detección comunes, entre las actividades y mecanismos utilizados para realizarla se tiene en cuenta principalmente la adquisición de la tecnología apropiada que administre adecuadamente los sistemas de información destinados al monitoreo y control de los patrones del uso de la red telefónica tanto fija como móvil.

- Es importante establecer el intercambio de información entre las operadoras telefónicas y el ente regulador de las Telecomunicaciones para constatar si hay o no anomalías en cuanto al tráfico telefónico cursado.

- Frente al estudio de un caso fraudulento, se debe tener en cuenta la adecuada discriminación de la información que será analizada para evitar el uso innecesario de recursos.

  Un elemento importante a tener en cuanta es el análisis de los CDR`s (Call Detail Record) los cuales permiten obtener el registro detallado de llamadas tanto entrantes como salientes.

- Por parte de las operadoras telefónicas es necesario realizar una investigación post facturación continua para monitorear, detectar y referir casos sospechosos e identificar patrones de alto uso y/o anomalías en cuanto al tráfico telefónico se refiere.

- Al tratar acerca de aspectos fraudulentos el tiempo es valioso, por ello se considera que un equipo opera eficientemente cuando empieza a actuar antes que los defraudadores cometan los errores que hacen que los sistemas de detección activen las alarmas y los identifiquen, es decir, detectar, evitar y contrarrestar oportunamente cualquier indicio de fraude.

- El recurso tanto humano como tecnológico invertido para contrarrestar el fraude en telecomunicaciones, se torna en vano mientras las leyes no sean aplicadas rigurosamente para imponer sanciones.

- El Call back, Refilling y By pass son los tipos de fraude que ocasionan mayores pérdidas económicas a las operadoras telefónicas legalmente establecidas, debido a que el fraude cometido en dichas modalidades implica cursar ilícitamente tráfico telefónico internacional.

- Las empresas que se dedican a cometer acciones ilegales como el By pass, son empresas muy bien organizadas con un gran respaldo a sus gestiones.

  Los trámites para traer tráfico de By pass a nuestro país son realizados en su mayoría en los Estados Unidos donde esta modalidad está permitida, y donde incluso se facilitan los equipos que permiten ingresar este tráfico como local en nuestro país.

- Es importante que las empresas encargadas de realizar la detección, control y gestión del fraude en telecomunicaciones en la región de América Latina se unan en la lucha contra los estafadores que operan muy organizadamente en todos los países.

- Se ha realizado el estudio de las curvas de tráfico telefónico internacional según datos publicados por la SUPTEL y la FCC, y su tendencia de crecimiento que debió existir si no hubiera desviación de un importante volumen de tráfico que termina en rutas ilegales, los resultados obtenidos del análisis individual y en conjunto de las curvas son similares, el fraude en la telefonía esta creciendo con diversas modalidades como el Call back y el By pass.

- De acuerdo a la comparación de la curva de tráfico telefónico internacional según datos publicados por la SUPTEL y la curva de tráfico telefónico internacional según datos publicados por la FCC, se observa:

  En el año 1998 se tuvo el auge del fraude al cursar tráfico telefónico internacional que termina en rutas ilegales de By pass, año que corresponde al primer periodo de evolución tecnológica de los sistemas By pass, periodo en el cual las operadoras telefónicas y el ente regulador de telecomunicaciones no contaban con las herramientas adecuadas para contrarrestar dicho fraude telefónico.

  En el periodo comprendido entre los años 2000 y 2002 se observa:

  - La recuperación de tráfico telefónico, resultado de la acción conjunta de la Superintendencia de Telecomunicaciones y las operadoras telefónicas ANDINATEL S.A. PACIFICTEL S.A. Y ETAPA en el combate al By pass, sin embargo el crecimiento del tráfico telefónico es mínimo debido al incremento del By pass, que para dicho periodo maneja una tecnología de punta que imposibilita su detección sin la asistencia de equipos especializados en el control del fraude telefónico.

  - La gran cantidad de oferta de tarjetas, que permiten realizar llamadas telefónicas que en el mercado se denominan: “International Phone Card & International Calling Card”, con costos exageradamente bajos en comparación a los precios establecidos por las operadoras telefónicas legalmente establecidas, también nos demuestra el crecimiento que el By pass adquirió durante dicho periodo.

  - El advenimiento del Internet, y en este sentido el auge de la telefonía por Internet (VoIP), ha sido otro factor que ha ocasionado pérdidas de tráfico telefónico.

- De acuerdo al análisis realizado con los datos de tráfico FCC entrante al Ecuador, se ha estimado que en 1998 debido al fraude en telefonía Ecuador ha perdido un volumen de tráfico de 155'120823,12 minutos anuales los cuales representan una perdida anual de $18.304.257,13 de dólares, teniendo en cuenta una tasa de terminación de llamadas internacionales de 11.8 centavos el minuto.

- El proyecto "Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones" ha sido puesto a consideración de la Dirección General de Investigación Especial en Telecomunicaciones de la Superintendencia de Telecomunicaciones, la cual a manifestado[1] que el documento en mención es considerado como importante, ya que debido a su contenido aporta dentro de la comprensión del alcance con que dichos ilícitos afectan tanto técnica como económicamente a las empresas operadoras de telecomunicaciones debidamente autorizadas.

---

1 **ANEXO K.** Análisis realizado por la Dirección General de Investigación Especial en Telecomunicaciones de la SUPTEL del documento "Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones"

4.2 RECOMENDACIONES

- Las operadoras telefónicas deben contar con un departamento de gerencia de fraude y aseguramiento de ingresos, con su respectivo equipamiento para la detección, control y gestión del fraude que le permita evitar y prevenir pérdidas económicas.

  Es decir todo servicio que sea factible de prestar sea prestado, que todo servicio prestado sea facturado, que todo lo facturado sea cobrado.

- El departamento de gerencia de fraude y aseguramiento de ingresos debe contar con un equipo de trabajo debidamente capacitado y conciente de las actividades y funciones que se deben cumplir.

  Entre las principales aptitudes que debe poseer el equipo de trabajo se tiene el uso correcto de software y hardware utilizado por el departamento para combatir el fraude, tener conocimiento de conceptos relacionados a telecomunicaciones y fraudes, ser capaz de desarrollar técnicas de investigación de acuerdo a los diferentes perfiles de fraude.

- Las posibilidades tecnológicas para realizar fraude son inmensas lo que ha ocasionado el incremento de estafas en el ámbito de las telecomunicaciones, por lo que es recomendable que el personal de las operadoras telefónicas, ANDINATEL S.A., PACIFICTEL S.A, ETAPA, y el ente regulador de las Telecomunicaciones, Superintendencia de Telecomunicaciones, esté muy bien capacitado en el campo del desarrollo tecnológico.

- Continuamente se debe dar soporte técnico tanto preventivo como correctivo al equipo utilizado por el departamento de gerencia de fraude y aseguramiento de ingresos, actualizar e integrar nuevas tecnologías para la detección, control y gestión del fraude en telecomunicaciones, lo cual permitirá administrar eficientemente los procesos informáticos en contra del fraude.

- Las operadoras telefónicas deben contar con un sistema de adquisición de datos, redes neuronales, capaz de establecer perfiles de comportamiento de la red de telefonía, tráfico telefónico y comparar dicho comportamiento con patrones normales y fraudulentos, así el sistema puede generar alarmas cuando se detectan comportamientos que salen fuera del patrón normal.

  Al momento de seleccionar un sistema de adquisición de datos, este debe ser independiente del proveedor, del tipo de redes ya sean fijas móviles o redes basadas en IP, debe ser adaptable a la adquisición de datos provenientes de cualquier dispositivo, debe ser flexible y escalable para pequeños o grandes volúmenes de tráfico telefónico.

- Por parte de las operadoras telefónicas y el ente regulador de las Telecomunicaciones, mediante los centros de atención al usuario se debe informar constantemente al usuario del servicio telefónico, los tipos de fraude a los cuales está expuesto, dar a conocer las precauciones y cuidados para evitar ser perjudicado.

- Las operadoras telefónicas y el ente regulador de las Telecomunicaciones, continuamente deben estar capacitando al personal laboral mediante cursos[2], seminarios, proyectos, etc. para en caso de presentarse un ataque fraudulento, el personal sepa reconocer el tipo de fraude y actuar debidamente ante el ilícito.

- Las técnicas utilizadas para ingresar el tráfico telefónico internacional por rutas de By pass han cambiado desde el inicio del año 2003, por lo que los métodos tradicionales utilizados para detectar posibles By pass han quedado caducos, las operadoras telefónicas y el ente regulador de las Telecomunicaciones deberán implementar nuevos métodos que con la ayuda de la tecnología permitan efectividad en el combate al By pass y otros tipos de fraudes telefónicos.

---

2 **ANEXO I.** Ejercicios prácticos referentes a fraudes en Telecomunicaciones

Referencias bibliográficas

REFERENCIAS BIBLIOGRÁFICAS

Textos

- CIEEPI, **Revista trimestral**, Publicación: 07/24/2003.

- FML SECURING BUSINESS, **Curso: Detección, Control y Gestión del Fraude en Telecomunicaciones**, 2005.

- FML SECURING BUSINESS, **Ejercicios prácticos y respuestas sugeridas: Detección, Control y Gestión del Fraude en Telecomunicaciones**, FML Americas Inc. 2002.

- IBC. INTERNATIONAL BUSINESS COMMUNICATIONS, **Curso: Renueve Assurance & Fraud Management Americas**, 2002.

- CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES, **Código penal, legislación conexa**, Edición: Décima quinta 2004.

- SUPERINTENDENCIA DE TELECOMUNICACIONES, **Intervenciones realizadas por la Superintendencia de Telecomunicaciones a estaciones de radiodifusión, sistemas de televisión por cable, y sistemas de By pass, que operaban sin autorización,** 09 JUN 2006.

- SUPERINTENDENCIA DE TELECOMUNICACIONES, **Interconexión internacional,** 2003.

- SUPERINTENDENCIA DE TELECOMUNICACIONES, **Análisis realizado por la Dirección General de Investigación Especial en Telecomunicaciones de la SUPTEL del documento "Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones",** 08 AGO 2006

- SECRETARIA NACIONAL DE TELECOMUNICACIONES, **Operadoras que poseen concesión de servicio de telecomunicaciones y están autorizadas a cursar tráfico telefónico internacional,** 18 MAY 2006.

Tesis

- Vaca Guaicha Estuardo, **"Estudio del fraude tecnológico en el sistema de telefonía móvil celular"**, 2000**.**

Páginas WEB

[1] http://www.supertel.gov.ec

[2] http://www.fmlsolutions.com

[3] http://www.fmlsolutions.com/span/bvaconcept/bva.html

[4] http://www.fcc.gov

[5] http://www.fcc.gov/wcb/iatd/intl.html

[6] http://www.fraudmanagement.com/

[7] http://www.conatel.gov.ec/espanol/glosario/contenido_glosario.htm

[8] http://www.unisys.com.ar/

[9] http://www.unisys.com.ar/telecomunicaciones/default.asp
[10] http://www.grupoice.com/esp/cencon/gral/infocom/glosario_telecom.htm
[11] http://www.netmedia.info/netmedia/articulos.php?id_sec=30&id_art=2109
[12] http://fraudtechnologies.cl/analisiseinvestigacion.html
[13] http://www.plus-ti.com/Espanhol/Aseguramiento_del_Ingreso.htm
[14] http://www.delitoselectronicos.com
[15] http://www.spss.com/es/soluciones/telecomunicaciones/fraude.htm
[16] http://www.andinatel.com/segmentos/comercial/disdir.htm
[17] http://www.cieepi.org/pages1/revista.asp?num=72
[18] http://www.satelcard.com/activacion-llamada-telefonica.htm
[19] http://www.uwtcallback.com/uwtcallbackold/Spanish/callbackes.php
[20] http://abacus-computer.net/abcb/intro.php?xlang=S&xres=1001
[21] http://www.net2secure.com/xodatel/callback/castellano/aplicacion.htm
[22] http://www.satelvoz.com/empresas/contacte.htm
[23] http://www.i-media.com/es/VOICE-6.HTML
[24] http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm
[25] http://www.rompecadenas.com.ar/ingsocial.htm
[26] http://lestertheteacher.cjb.net/
[27] http://virusattack.xnetwork.com.ar/articulos/VerArticulo.php3?idarticulo=4
[28] http://www.iec.csic.es/criptonomicon/articulos/expertos72.html
[29] http://www6.gratisweb.com/disidents/ascii/ezine/nocionesis.html
[30] http://rr.sans.org/social/social.php
[31] http://www.nitecrest.co.uk/spanish/plastic.htm
[32] http://www.conatel.gov.ec/website/baselegal/leyes.php?cod_cont=21&nomb_grupo=leyes&cod_nivel=n1

ANEXO

A

Glosario

GLOSARIO

Antenas omnidireccionales

Son aquellas que propagan o reciben ondas de radio o electromagnéticas, mantienen una cobertura geográfica circular.

Carriers

Operadores de telecomunicaciones propietarios de las redes troncales de Internet y responsables del transporte de los datos. Proporciona una conexión a Internet de alto nivel.

Central telefónica

Conjunto de dispositivos de transporte de tráfico, de etapas de conmutación, de medios de control y señalización, y de otras unidades funcionales de un nodo de la red, que permite la interconexión de líneas de abonados, circuitos de telecomunicaciones u otras unidades funcionales, según lo requieran los usuarios individuales.

Concesión

Contrato mediante el cual se otorga a una persona natural o jurídica el derecho a explotar servicios de Telecomunicaciones.

CDR. (Call Detail Record)

Registro de detalle de llamada. Listado cronológico de todas las llamadas realizadas en un sistema telefónico.

Dirección IP

Dirección única de un dispositivo en una red TCP/IP. Consiste de cuatro números entre 0 y 255 separados por puntos. Por ejemplo 200.132.5.45.

Enlace

Medio de transmisión con características específicas entre dos puntos. Esto puede ser mediante canal o circuito.

Enlace por satélite

Enlace radioeléctrico efectuado entre una estación terrena transmisora y una estación terrena receptora por medio de un satélite. Un enlace por satélite está formado por un enlace ascendente y un enlace descendente.

FCC

Federal Communications Commission.

GATEWAY

El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles. GATEWAY o pasarela es un dispositivo, con frecuencia un ordenador, que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, un GATEWAY de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

Hacker

Persona con conocimientos de sistemas operativos, redes, protocolos, seguridad informática y programación entre otras cosas, capaz de entrar en sistemas cuyo acceso es restringido.

Hacking

Es el conjunto de acciones por los cuales una persona vulnera la seguridad de los sistemas informáticos ajenos.

IP (Internet Protocol)

Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132.248.53.10.

MODEM

Es una contracción de Modulador y Demodulador, lo cual representa las operaciones de transmisión y recepción, respectivamente, en un sistema de transmisión punto a punto. La rata de símbolos enviada por unidad de tiempo se denomina baudio; deben operar con varias limitaciones características del canal de voz.

PBX

Es una central de conmutación privada que está operada por un abonado de servicio de telecomunicaciones, la cual puede conectarse a una red pública como equipo terminal o a una red privada.

Planta externa

Conjunto de redes troncales, primarias, secundarias, armarios, cajas, regletas, distribuidores (por lo general todo lo que involucre cobre).

Phreaking

Es el conjunto de acciones por los cuales una persona vulnera la seguridad de los sistemas telefónicos ajenos para evitar pagar llamadas a larga distancia. Con la voz sobre IP (VoIP), entre otras tecnologías.

Red de telecomunicaciones

Conjunto de elementos que permite el transporte de señales de voz, sonidos, datos, textos, márgenes u otras señales de cualquier naturaleza entre dos o más puntos de terminación definidos forman parte de esta red los equipos de, conmutación, transmisión y control, los cables, soportes lógicos y otros elementos físicos, así como el uso del espectro radioeléctrico asignado para integrar la red, si es el caso.

Red pública de telefonía

La cual es compartida entre muchos usuarios, y cualquier usuario puede establecer comunicación con cualquier otro usuario, incluyendo servicios de larga distancia.

Redes neuronales

Son un paradigma de aprendizaje y procesamiento automático. Consiste en simular propiedades a través de modelos matemáticos recreados mediante mecanismos artificiales como un circuito integrado, un ordenador o conjunto de válvulas.

ROUTER

Computadores especializados que toman los paquetes entrantes y comparan sus direcciones de destino con tablas de encaminamiento interno y, en función de la política de encaminamiento del caso, envían los paquetes a la interfaz idónea. Este proceso puede repetirse muchas veces hasta que el paquete llega al destino previsto.

Satélite

Cuerpo que gira alrededor de otro cuerpo de masa preponderante y cuyo movimiento está principalmente determinado, de modo permanente, por la fuerza de atracción de este último.

SENATEL

Secretaria Nacional de Telecomunicaciones.

SUPTEL

Superintendencia de Telecomunicaciones.

SWITCH

Dispositivo de red capaz de buscar y seleccionar el camino correcto para enviar una serie de datos a su próximo destino. De acuerdo al modelo ISO/OSI, el SWITCH opera en el nivel de enlace de datos (nivel 2) y ocasionalmente en el nivel de red (nivel 3).

Telepuerto

Uno o más transmisores o receptores, o una combinación de transmisores y receptores, incluyendo las instalaciones accesorias, necesarios para asegurar un servicio de radiocomunicación, o el servicio de radioastronomía en un lugar determinado. Las estaciones se clasificarán según el servicio en el que participen de una manera permanente o temporal.

Troyano

Tipo de virus que se camufla dentro de un programa que parece inofensivo para que el usuario lo ejecute. Una ves instalado pretende sacar al exterior información del ordenador, como son contraseñas y otros tipos de datos que pudieran ser valiosos.

Usuario

Es toda aquella persona física o moral que en forma eventual o permanente tiene acceso a algún servicio público o privado de telecomunicaciones.

VoIP (VoIP, Voice over IP)

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways, teléfonos IP y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

VSAT (Very Small Aperture Satellite Terminal)

En comunicaciones vía satélite, estaciones receptoras de diámetro pequeño típicamente operadas en la banda Ku.

ANEXO

B

Ley Especial de Telecomunicaciones Reformada

ANEXO B

LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA

La Ley Especial de Telecomunicaciones Reformada que rige en Ecuador sirve de marco jurídico para combatir el fraude.

Los artículos relacionados a prohibiciones o restricciones del uso indebido o no autorizado de los servicios de telecomunicaciones considerados para imponer sanciones, se encuentran resaltados.

LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA[1]

(Ley No. 184)

CONGRESO NACIONAL
EL PLENARIO DE LAS COMISIONES LEGISLATIVAS

Considerando:

Que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud, tecnología y especialidad de dichos servicios, de suerte que se pueda desarrollar esta actividad con criterios de gestión empresarial y beneficio social;

Que es indispensable asegurar una adecuada regulación y expansión de los sistemas radioeléctricos y servicios de telecomunicaciones a la comunidad y mejorar permanentemente la prestación de los servicios existentes, de acuerdo a las necesidades del desarrollo social y económico del país; y,

En ejercicio de sus atribuciones constitucionales, expide la siguiente:

LEY ESPECIAL DE TELECOMUNICACIONES
Capítulo I
DISPOSICIONES FUNDAMENTALES

Art. 1.- Ámbito de la Ley.- La presente Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

---

1 http://www.conatel.gov.ec/website/baselegal/leyes.php?cod_cont=21&nomb_grupo=leyes&cod_nivel=n1

Los términos técnicos de telecomunicaciones no definidos en la presente Ley, serán utilizados con los significados establecidos por la Unión Internacional de Telecomunicaciones.

Art. 2.- Espectro radioeléctrico.- El espectro radioeléctrico es un recurso natural de propiedad exclusiva del Estado y como tal constituye un bien de dominio público, inalienable e imprescriptible, cuya gestión, administración y control corresponde al Estado.

Art. 3.- Administración del espectro.- Las facultades de gestión, administración y control del espectro radioeléctrico comprenden, entre otras, las actividades de planificación y coordinación, la atribución del cuadro de frecuencias, la asignación y verificación de frecuencias, el otorgamiento de autorizaciones para su utilización, la protección y defensa del espectro, la comprobación técnica de emisiones radioeléctricas, la identificación, localización y eliminación de interferencias perjudiciales, el establecimiento de condiciones técnicas de equipos terminales y redes que utilicen en cualquier forma el espectro, la detección de infracciones, irregularidades y perturbaciones, y la adopción de medidas tendientes a establecer el correcto y racional uso del espectro, y a reestablecerlo en caso de perturbación o irregularidades.

Art. 4.- Uso de frecuencias.- El uso de frecuencias radioeléctricas para los servicios de radiodifusión y televisión requieren de una concesión previa otorgada por el Estado y dará lugar al pago de los derechos que corresponda. Cualquier ampliación, extensión, renovación o modificación de las condiciones, requiere de nueva concesión previa y expresa.

El uso de frecuencias radioeléctricas para otros fines diferentes de los servicios de radiodifusión y televisión requieren de una autorización previa otorgada por el Estado y dará lugar al pago de los derechos que corresponda. Cualquier ampliación, extensión, renovación o modificación de las condiciones, requiere de nueva autorización, previa y expresa.

La concesión y la autorización para el uso de frecuencias radioeléctricas tendrá un plazo definido que no podrá exceder de cinco años, renovables por períodos iguales.

Art. 5.- Normalización y homologación.- El Estado formulará, dictará y promulgará reglamentos de normalización de uso de frecuencias, explotación de servicios, industrialización de equipos y comercialización de servicios, en el área de telecomunicaciones, así como normas de homologación de equipos terminales y otros equipos que se considere conveniente acordes con los avances tecnológicos, que aseguren la interconexión entre las redes y el desarrollo armónico de los servicios de telecomunicaciones.

Art. 6.- Naturaleza del servicio.- Las telecomunicaciones constituyen un servicio de necesidad, utilidad y seguridad públicas y son de atribución privativa y de responsabilidad del Estado.

Las telecomunicaciones relacionadas con la defensa y seguridad nacionales son de responsabilidad de los Ministerios de Defensa Nacional y de Gobierno.

Los servicios de radiodifusión y de televisión se sujetarán a la Ley de Radiodifusión y Televisión y a las disposiciones pertinentes de la presente Ley.

Art. 7.- Función básica.- Es atribución del Estado dirigir, regular y controlar todas las actividades de telecomunicaciones.

Art. 8.- Servicios finales y servicios portadores.- Para efectos de la presente Ley, los servicios abiertos a la correspondencia pública se dividen en servicios finales y servicios portadores, los que se definen a continuación y se prestan a los usuarios en las siguientes condiciones:

a) Servicios finales de telecomunicaciones son aquellos servicios de telecomunicación que proporcionan la capacidad completa para la comunicación entre usuarios, incluidas las funciones del equipo terminal y que generalmente requieren elementos de conmutación.

Forman parte de estos servicios, inicialmente, los siguientes: telefónico rural, urbano, interurbano e internacional; videotelefónico; telefax; burofax; datafax; videotex, telefónico móvil automático, telefónico móvil marítimo o aeronáutico de correspondencia pública; telegráfico; radiotelegráfico; de télex y de teletextos.

También se podrán incluir entre los servicios finales de telecomunicación los que sean definidos por los organismos internacionales competentes, para ser prestados con carácter universal.

El régimen de prestación de servicios finales será:

1. (Numeral derogado por el lit. p) del Art. 100 de la Ley 2000-4, R.O. 34-S, 13-III-2000);
2. El Reglamento Técnico de cada servicio final de telecomunicación deberá definir los puntos de conexión a los cuales se conecten los equipos terminales del mismo. Esta definición deberá contener las especificaciones completas de las características técnicas y operacionales y las normas de homologación que deberán cumplir los equipos terminales; y,
3. Los equipos terminales, con certificado de homologación, podrán ser libremente adquiridos a la empresa estatal o a empresas privadas;

b) Servicios portadores son los servicios de telecomunicación que proporcionan la capacidad necesaria para la transmisión de señales entre puntos de terminación de red definidos.

El régimen de prestación de servicios portadores se sujeta a las siguientes normas:

1. En este tipo de servicios existen dos modalidades:

   a. Servicios que utilizan redes de telecomunicaciones conmutadas para enlazar los puntos de terminación, tales como la transmisión de datos por redes de conmutación de paquetes, por redes de conmutación de circuitos, por la red conmutada o por la red télex; y,

b. Servicios que utilizan redes de telecomunicación no conmutadas. Pertenecen a este grupo, entre otros, el servicio de alquiler de circuitos;

2. Los puntos de terminación de red a que hace referencia la definición de servicios portadores deberán estar completamente especificados en todas sus características técnicas y operacionales en los correspondientes Reglamentos Técnicos.

3. (Numeral derogado por el lit. p) del Art. 100 de la Ley 2000-4, R.O. 34-S, 13-III-2000).

Art. 9.- Autorizaciones.- El Estado regulará, vigilará y contratará los servicios de telecomunicaciones en el País.

Art. 10.- Intercomunicaciones internas.- No será necesaria autorización alguna para el establecimiento o utilización de instalaciones destinadas a intercomunicaciones dentro de residencias, edificaciones e inmuebles públicos o privados, siempre que para el efecto no se intercepten o interfieran los sistemas de telecomunicaciones públicos. Si lo hicieran, sus propietarios o usuarios estarán obligados a realizar, a su costo, las modificaciones necesarias para evitar dichas interferencias o intercepciones, sin perjuicio de la aplicación de las sanciones previstas en esta Ley. En todo caso, también estas instalaciones estarán sujetas a la regulación y control por parte del Estado.

Art. 11.- Uso prohibido.- Es prohibido usar los medios de telecomunicación contra la seguridad del Estado, el orden público, la moral y las buenas costumbres. La contravención a esta disposición será sancionada de conformidad con el Código Penal y más leyes pertinentes.

Art. 12.- Sistemas móviles.- Compete al Estado la regulación de todos los sistemas radioeléctricos de las naves aéreas o marítimas y cualquier otro vehículo, nacional o extranjero, que operen habitualmente en el país o se encuentre en tránsito en el territorio nacional.

La Armada Nacional prestará, explotará y controlará el Servicio Móvil Marítimo que incluye las estaciones costeras, tanto en el aspecto Militar como en el abierto a la correspondencia pública, concertando para este último los convenios operativos de interconexión con la operadora de los servicios finales de telefonía, telegrafía y télex con sujeción a los reglamentos de Radiocomunicaciones acordados por la Unión Internacional de Telecomunicaciones, de la cual el Ecuador es país signatario.

Art. 13.- Regulación del espectro radioeléctrico.- Es facultad privativa del Estado el aprovechamiento pleno de los recursos naturales como el espectro de frecuencias radioeléctricas, y le corresponde administrar, regular y controlar la utilización del espectro radioeléctrico en sistemas de telecomunicaciones en todo el territorio ecuatoriano, de acuerdo con los intereses nacionales.

Art. 14.- Derecho al secreto de las telecomunicaciones.- El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones.

Art. 15.- Control en casos de emergencia.- En caso de guerra o conmoción interna, así como de emergencia nacional, regional o local, declarada por el Presidente de la República, el Comando Conjunto de las Fuerzas Armadas, en coordinación con la operadora de los servicios finales, tomará el control directo e inmediato de los servicios de telecomunicaciones. Este control cesará al desaparecer la causa que lo originó.

Art. 16.- Coordinación con obras viales.- El Ministerio de Obras Públicas realizará la coordinación que sea indispensable, a pedido de la operadora de servicios finales o del Comando Conjunto de las Fuerzas Armadas, para la ejecución o supresión de obras relacionadas con líneas físicas de telecomunicaciones en las carreteras que sean construidas o modificadas por el Ministerio de Obras Públicas o por entidades municipales y provinciales.

Art. 17.- Protección contra interferencias.- INECEL, las Empresas Eléctricas y cualquier otra persona natural o jurídica que establezcan líneas de transmisión o de distribución de energía eléctrica o instalaciones radioeléctricas de cualquier tipo, están obligadas a evitar, a su costo, cualquier interferencia que pudiera producirse por efecto de dichas instalaciones sobre el sistema de telecomunicaciones, ya sea adoptando normas apropiadas para el trazado y construcción de las mismas o instalando los implementos o equipos necesarios para el efecto.

Nota:
La Ley 98-14 (R.O. 37-S, 30-IX-98), reformatoria a la Ley de Régimen del Sector Eléctrico, establece el proceso de liquidación de INECEL y el plazo extintivo de su personalidad jurídica al 31 de marzo de 1999.

Art. 18.- Daños a instalaciones.- Cuando las instalaciones de telecomunicaciones pertenecientes a la red pública o las instalaciones de radio comunicaciones que forman parte del servicio público, sufran interferencias, daños o deterioros causados por el uso de equipos eléctricos, vehículos, construcciones o cualquier otra causa, corresponderá al causante del daño pagar los costos de las modificaciones o reparaciones necesarias, inclusive por la vía coactiva.

Capítulo II
DE LAS TASAS Y TARIFAS

Art. 19.- Retribución de Servicios.- (Sustituido por el Art. 3 de la Ley 94, R.O. 770, 30-VIII-95).- La prestación de cualquier servicio de telecomunicaciones por medio de empresas legalmente autorizadas, está sujeta al pago de tarifas que serán reguladas en los respectivos contratos de concesión, de conformidad con lo dispuesto en el artículo 22 de esta Ley.

Art. 20.- Tarifas populares.- (Sustituido por el Art. 4 de la Ley 94, R.O. 770, 30-VIII-95).- En los pliegos tarifarios correspondientes se establecerán tarifas

especiales o diferenciadas para el servicio residencial popular, marginal y rural, orientales, de Galápagos y fronterizas, en función de escalas de bajo consumo.

EMETEL S.A. y las compañías resultantes de su escisión establecerán anualmente un fondo de hasta el 4% de las utilidades netas que será empleado exclusivamente para subsidiar la parte no rentable de proyectos específicos de desarrollo rural de las telecomunicaciones.

Art. 21.- Criterios para la fijación de tarifas.- (Sustituido por el Art. 5 de la Ley 94, R.O. 770, 30-VIII-95).- Los pliegos tarifarios de cada uno de los servicios de telecomunicaciones serán establecidos por el ente regulador.

Los criterios para la fijación de los pliegos tarifarios podrán determinarse sobre las bases de las fórmulas de tasa interna de retorno y tope de precio aplicadas en la industria telefónica, por los diferentes servicios efectuados por las operadoras. El ente regulador podrá, así mismo, utilizar combinaciones de estas fórmulas en salvaguarda de la eficiencia y del interés de los usuarios, con el objeto de promover la competencia leal entre los operadores.

En los contratos de concesión se establecerán los pliegos tarifarios iniciales y el régimen para su modificación. El CONATEL aprobará el respectivo pliego tarifario en función del cumplimiento por parte del operador u operadores de las siguientes condiciones:

a) La ejecución del Plan de Expansión del servicio de telecomunicaciones acordado en los contratos de concesión a que se hace referencia en esta Ley;

b) Que en la ejecución del referido plan se hayan respetado las exigencias de calidad determinadas en los contratos de concesión, y de venta de acciones. Dentro de las exigencias de calidad se verificará obligatoriamente las siguientes:

1. Porcentaje de digitalización de la red;
2. Tasa de llamadas completadas a niveles local, nacional e internacional;
3. Tiempo en el tono de discar;

4. Tiempo de atención promedio de los servicios con operadores;
5. Porcentaje de averías reportadas por 100 lineas en servicio por mes;
6. Porcentaje de averías reparadas en 24 horas;
7. Porcentaje de averías reparadas en 48 horas;
8. Porcentaje de cumplimiento de visitas de reparación;
9. Peticiones de servicio satisfechas en cinco días;
10. Reclamos por facturación por cada 100 facturas;
11. Satisfacción de los usuarios; y,
12. Otras que sean utilizadas por la Unión Internacional de Telecomunicaciones (UIT) para la medición de la calidad de servicio.

Se prohíbe los subsidios excepto aquellos contemplados en el artículo 4 de esta Ley.

Bajo ningún concepto el Estado garantizará la rentabilidad de las empresas, ni otorgará ninguna garantía especial, salvo las determinadas en la Ley.

Art. 22.- Aprobación y vigencia de las tarifas.- (Sustituido por el Art. 6 de la Ley 94, R.O. 770, 30-VIII-95).- Los pliegos tarifarios entrarán en vigencia una vez que hayan sido aprobados por el ente regulador de las telecomunicaciones.

El ente de regulación de las telecomunicaciones aprobará los pliegos tarifarios siempre y cuando el o los operadores justifiquen satisfactoriamente que han dado cumplimiento a las obligaciones establecidas en los correspondientes contratos de concesión.

Art. 23.- Tasas y tarifas por concesiones y autorizaciones.- Las tasas y tarifas por concesiones y autorizaciones para instalar y explotar los servicios radioeléctricos se fijarán por el Estado conforme a lo dispuesto en la Ley de Radiodifusión y Televisión y en los contratos de concesión o de autorización correspondientes.

Capítulo III
DEL PLAN DE DESARROLLO DE LAS TELECOMUNICACIONES

Art. 24.- Plan de desarrollo.- (Sustituido inc. 2 por el Art. 7 de la Ley 94, R.O. 770, 30-VIII-95).- El Plan de Desarrollo de las Telecomunicaciones tiene por finalidad dotar al país de un sistema de telecomunicaciones capaz de satisfacer las necesidades de desarrollo, para establecer sistemas de comunicaciones eficientes, económicas y seguras.

Las empresas legalmente autorizadas para prestar al público servicios de telecomunicaciones deberán presentar, para aprobación del Consejo Nacional de Telecomunicaciones (CONATEL), un plan de inversiones a ser ejecutado durante el período de exclusividad.

Capítulo IV
DE LOS USUARIOS

Art. 25.- Derecho al servicio.- Todas las personas naturales o jurídicas, ecuatorianas o extranjeras, tienen el derecho a utilizar los servicios públicos de telecomunicaciones condicionado a las normas establecidas en los reglamentos y al pago de las tasas y tarifas respectivas.

Las empresas legalmente autorizadas establecerán los mecanismos necesarios para garantizar el ejercicio de los derechos de los usuarios.

Art. 26.- Prohibición de conceder exoneraciones.- (Reformado por el Art. 8 de la Ley 94, R.O. 770, 30-VIII-95).- Prohíbese conceder exoneraciones del pago de tasas y tarifas por el uso de los servicios públicos de telecomunicaciones o por el otorgamiento de concesiones o autorizaciones.

En los presupuestos de cada uno de los organismos y entidades del sector público, constarán obligatoriamente partidas destinadas al pago de los servicios de telecomunicaciones.

Capítulo V
DE LAS SANCIONES

Art. 27.- Delitos contra las telecomunicaciones.- Los delitos cometidos contra los medios y servicios de telecomunicaciones serán los tipificados en el Código Penal y serán sancionados de conformidad con lo dispuesto en dicho código.

Art. 28.- Infracciones.- Constituyen infracciones a la presente Ley, las siguientes:

a. El ejercicio de actividades o la prestación de servicios sin la correspondiente concesión o autorización, así como la utilización de frecuencias radioeléctricas sin permiso o en forma distinta de la permitida;
b. El ejercicio de actividades o la prestación de servicios que no correspondan al objeto o al contenido de las concesiones o autorizaciones;
c. La conexión de otras redes a la red de telecomunicaciones sin autorización o en forma distinta a la autorizada o a lo previsto en esta Ley y sus Reglamentos;
d. La instalación, la utilización o la conexión a la red de telecomunicaciones de equipos que no se ajusten a las normas correspondientes;
e. La producción de daños a la red de telecomunicaciones como consecuencia de conexiones o instalaciones no autorizadas;
f. La importación, fabricación, distribución, venta o exposición para la venta de equipos o aparatos que no dispongan de los certificados de homologación y de cumplimiento de las especificaciones técnicas que se establezcan en los Reglamentos;
g. La competencia desleal en la prestación de los servicios de telecomunicaciones; y,
h. Cualquiera otra forma de incumplimiento o violación de las disposiciones legales, reglamentarias o contractuales en materia de telecomunicaciones.

Se consideran infracciones graves las siguientes:

1. La conducta culposa o negligente que ocasione daños, interferencias o perturbaciones en la red de telecomunicaciones en cualquiera de sus elementos o en su funcionamiento;
2. La alteración o manipulación de las características técnicas de los equipos, aparatos o de terminales homologados o la de sus marcas, etiquetas o signos de identificación;
3. La producción deliberada de interferencias definidas como perjudiciales en el Convenio Internacional de Telecomunicaciones; y,
4. La violación a la prohibición constante en el artículo 14 de la presente Ley.

Art. 29.- Sanciones.- La persona natural o jurídica que incurra en cualquiera de las infracciones señaladas en el artículo anterior sin perjuicio de la reparación de los daños ocasionados será sancionada por las autoridades indicadas en el artículo 30 con una de las siguientes sanciones según la gravedad de la falta, el daño producido y la reincidencia en su comisión:

a. Amonestación escrita;
b. Sanción pecuniaria de uno hasta cincuenta salarios mínimos vitales generales;
c. Suspensión temporal de los servicios;
d. Suspensión definitiva de los servicios; y,
e. Cancelación de la concesión o autorización y negativa al otorgamiento de nuevas.

Art. 30.- Juzgamiento.- Corresponde al Superintendente de Telecomunicaciones juzgar al presunto infractor, graduando la aplicación de la sanción según las circunstancias, mediante resolución motivada y notificada al infractor.

Art. 31.- Notificación.- La notificación de la presunta infracción se hará por una boleta, en el domicilio mercantil o civil del infractor o por correo certificado.

Cuando no se conociera el domicilio o se trate de notificar a los herederos del infractor, la notificación se hará mediante una publicación en un periódico de la capital de provincia de su domicilio, cuando hubiera, y además en uno de los

periódicos de la capital de la República. Las notificaciones por la prensa podrán hacerse individual o colectivamente, cuando fueran varios los presuntos infractores.

Art. 32.- Contestación.- El presunto infractor tendrá el término de ocho días contados desde el día hábil siguiente al de la notificación respectiva para contestarla y ejercer plenamente su derecho de defensa.

Art. 33.- Resolución.- El Superintendente dictará resolución en el término de quince días contados desde el vencimiento del término para contestar, haya o no recibido la contestación.

Las resoluciones contendrán la referencia expresa a las disposiciones legales y reglamentarias aplicadas y a la documentación y actuaciones que las fundamenten; decidirán sobre todas las cuestiones planteadas en la notificación y su contestación y en las alegaciones pertinentes de los interesados.

La resolución que dicte el Superintendente causará ejecutoria en la vía administrativa, pero podrá contradecirse en la vía jurisdiccional ante el Tribunal de lo Contencioso Administrativo, conforme a la Ley.

Nota:
El Tribunal de lo Contencioso Administrativo fue suprimido por las reformas constitucionales del 23-XII-92, que crearon los Tribunales Distritales de lo Contencioso Administrativo. De presentarse recurso de casación lo conocerá la Sala especializada de la Corte Suprema de Justicia en esta materia.

Capítulo VI
DEL CONSEJO NACIONAL DE TELECOMUNICACIONES, DE LA SECRETARÍA NACIONAL DE TELECOMUNICACIONES Y DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES

(Capítulo redenominado por el Art. 9 de la Ley 94, R.O. 770, 30-VIII-95)

Título I (Ley 94)

EL CONSEJO NACIONAL DE TELECOMUNICACIONES (CONATEL)

(Título agregado por el Art. 10 de la Ley 94, R.O. 770, 30-VIII-95)

Art. ... (1).- Del Consejo Nacional de Telecomunicaciones (CONATEL).- Créase el Consejo Nacional de Telecomunicaciones (CONATEL) como ente de administración y regulación de las telecomunicaciones en el país, con domicilio en la ciudad de Quito.

El Consejo Nacional de Telecomunicaciones tendrá la representación del Estado para ejercer, a su nombre, las funciones de administración y regulación de los servicios de telecomunicaciones, y es la Administración de Telecomunicaciones del Ecuador ante la Unión Internacional de Telecomunicaciones (UIT).

Sesionará ordinariamente una vez al mes y extraordinariamente cuando lo convoque el Presidente o a solicitud de tres de sus miembros. Sus resoluciones se adoptarán por mayoría de votos.

Art. ... (2).- El CONATEL estará integrado por:

a. Un representante del Presidente de la República, quien lo presidirá;
b. El Jefe del Comando de las Fuerzas Armadas;
c. El Secretario General del Consejo Nacional de Desarrollo (CONADE);
d. El Secretario Nacional de Telecomunicaciones;
e. El Superintendente de Telecomunicaciones;
f. Un representante designado conjuntamente por las Cámaras de Producción; y,
g. El representante legal del Comité Central Único Nacional de los Trabajadores de EMETEL (CONAUTEL).

El representante al que se refiere el literal f), durará 2 años en sus funciones; el Reglamento a la Ley normará la calificación que deberá tener este representante,

tanto en el ámbito profesional, como en experiencia y conocimiento en los temas relacionados a las funciones del CONATEL.

Nota:

- Por disposición del Art. 255 de la Constitución Política vigente, el Sistema Nacional de Planificación estará a cargo de un organismo técnico dependiente de la Presidencia de la República, por lo que desaparece el CONADE. Hasta que se expida su ley regulatoria y en virtud de lo dispuesto por la trigésima novena disposición transitoria de la Constitución, ha sido creada la Oficina de Planificación (D.E. 120, R.O. 27, 16-IX-98).

- El Art. 3 del D.E. 120 (R.O. 27, 16-IX-98) reformado por el Art. 3 del D.E. 103 (R.O. 23, 23-II-2000) dispone que en todas las normas en las que se establezca cuerpos colegiados de los que forme parte el CONADE, su Presidente o el Secretario General de Planificación, se entenderá que se habla del Vicepresidente de la República como Director General de la Oficina de Planificación.

Art. ... (3).-Compete al Consejo Nacional de Telecomunicaciones (CONATEL):

a. Dictar las políticas del Estado con relación a las Telecomunicaciones;
b. Aprobar el Plan Nacional de Desarrollo de las Telecomunicaciones;
c. Aprobar el plan de frecuencias y de uso del espectro radioeléctrico;
d. Aprobar las normas de homologación, regulación y control de equipos y servicios de telecomunicaciones;
e. Aprobar los pliegos tarifarios de los servicios de telecomunicaciones abiertos a la correspondencia pública, así como los cargos de interconexión que deban pagar obligatoriamente los concesionarios de servicios portadores, incluyendo los alquileres de circuitos;
f. Establecer términos, condiciones y plazos para otorgar las concesiones y autorizaciones del uso de frecuencias así como la autorización de la explotación de los servicios finales y portadores de telecomunicaciones;
g. Designar al Secretario del CONATEL;

h. Autorizar a la Secretaría Nacional de Telecomunicaciones la suscripción de contratos de concesión para la explotación de servicios de telecomunicaciones;
i. Autorizar a la Secretaría Nacional de Telecomunicaciones la suscripción de contratos de concesión para el uso del espectro radioeléctrico;
j. Expedir los reglamentos necesarios para la interconexión de las redes;
k. Aprobar el plan de trabajo de la Secretaría Nacional de Telecomunicaciones;
l. Aprobar los presupuestos de la Secretaría Nacional de Telecomunicaciones y de la Superintendencia de Telecomunicaciones;
m. Conocer y aprobar el informe de labores de la Secretaría Nacional de Telecomunicaciones así como de sus estados financieros auditados;
n. Promover la investigación científica y tecnológica en el área de las telecomunicaciones;
o. Aprobar los porcentajes provenientes de la aplicación de las tarifas por el uso de frecuencias radioeléctricas que se destinarán a los presupuestos del CONATEL, de la Secretaría Nacional de Telecomunicaciones y de la Superintendencia de Telecomunicaciones;
p. Expedir los reglamentos operativos necesarios para el cumplimiento de sus funciones;
q. Declarar de utilidad pública con fines de expropiación, los bienes indispensables para el normal funcionamiento del sector de las telecomunicaciones;
r. En general, realizar todo acto que sea necesario para el mejor cumplimiento de sus funciones y de los fines de esta Ley y su Reglamentación; y,
s. Las demás previstas en esta ley y sus reglamentos.

Título II
DE LA SECRETARÍA NACIONAL DE TELECOMUNICACIONES

(Título agregado por el Art. 10 de la Ley 94, R.O. 770, 30-VIII-95)

Art. ... (1).- De la Secretaría Nacional de Telecomunicaciones.- Créase la Secretaría Nacional de Telecomunicaciones, como ente encargado de la ejecución de la política de telecomunicaciones en el país, con domicilio en la ciudad de Quito.

La Secretaría Nacional de Telecomunicaciones estará a cargo del Secretario Nacional de Telecomunicaciones que será nombrado por el Presidente de la República; tendrá dedicación exclusiva en sus funciones y será designado para un período de 4 años.

El Secretario Nacional de Telecomunicaciones, para su designación, deberá reunir los requisitos de profesionalidad y experiencia que se determine en el Reglamento de esta Ley.

El régimen de contrataciones, administración financiera y contable y administración de recursos humanos de la Secretaría Nacional de Telecomunicaciones será autónomo. En consecuencia, la Secretaría Nacional de Telecomunicaciones no estará sujeta a las leyes de Contratación Pública, de Servicio Civil y Carrera Administrativa, de Consultoría. Para tales efectos, se regirá por los reglamentos que expida el Presidente de la República.

Art. ... (2).- Compete al Secretario Nacional de Telecomunicaciones:

a. Ejercer la representación legal de la Secretaría Nacional de Telecomunicaciones;
b. Cumplir y hacer cumplir las resoluciones del CONATEL;
c. Ejercer la gestión y administración del espectro radioeléctrico;
d. Elaborar el Plan Nacional de Desarrollo de las Telecomunicaciones y someterlo a consideración y aprobación del CONATEL;
e. Elaborar el Plan de Frecuencias y de uso del espectro Radioeléctrico y ponerlo a consideración y aprobación del CONATEL;
f. Elaborar las normas de homologación, regulación y control de equipos y servicios de telecomunicaciones, que serán conocidas y aprobadas por el CONATEL;

g. Conocer los pliegos tarifarios de los servicios de telecomunicaciones abiertos a la correspondencia pública propuestos por los operadores y presentar el correspondiente informe al CONATEL;
h. Suscribir los contratos de concesión para la explotación de servicios de telecomunicaciones autorizados por el CONATEL;
i. Suscribir los contratos de autorización y/o concesión para el uso del espectro radioeléctrico autorizados por el CONATEL;
j. Otorgar la autorización necesaria para la interconexión de las redes;
k. Presentar para aprobación del CONATEL, el plan de trabajo y la proforma presupuestaria de la Secretaría Nacional de Telecomunicaciones;
l. Presentar para aprobación del CONATEL, el informe de Labores de la Secretaría Nacional de Telecomunicaciones, así como sus estados financieros auditados;
m. Resolver los asuntos relativos a la administración general de la Secretaría Nacional de Telecomunicaciones;
n. Promover la investigación científica y tecnológica en el campo de las telecomunicaciones;
o. Delegar una o más atribuciones específicas a los funcionarios de la Secretaría Nacional de Telecomunicaciones; y,
p. Las demás que le asignen esta Ley y su Reglamento.

Título III
DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES

Art. 34.- (Sustituido por el Art. 11 de la Ley 94, R.O. 770, 30-VIII-95).- Créase la Superintendencia de Telecomunicaciones, que tendrá su domicilio en la ciudad de Quito para el ejercicio de las funciones asignadas a ella en la presente Ley.

La Superintendencia estará dirigida por un Superintendente nombrado por el Congreso Nacional para un período de cuatro años, de una terna enviada por el Presidente de la República. En caso de ausencia definitiva del titular, se designará un nuevo superintendente que durará en sus funciones hasta completar el período del anterior.

Los requisitos para ser designado Superintendente constarán en el reglamento respectivo.

El régimen de contrataciones, administración financiera y contable y administración de recursos humanos de la Superintendencia de Telecomunicaciones será autónomo. En consecuencia, la Superintendencia no estará sujeta a las leyes de contratación pública, de servicio civil y carrera administrativa, de consultoría. Para tales efectos, se regirá por los reglamentos que expida el Presidente de la República.

Art. 35.- (Sustituido por el Art. 12 de la Ley 94, R.O. 770, 30-VIII-95).- Las funciones de la Superintendencia de Telecomunicaciones, son:

a. Cumplir y hacer cumplir las resoluciones del CONATEL;
b. El control y monitoreo del espectro radioeléctrico;
c. El control de los operadores que exploten servicios de telecomunicaciones;
d. Supervisar el cumplimiento de los contratos de concesión para la explotación de los servicios de telecomunicaciones;
e. Supervisar el cumplimiento de las normas de homologación y regulación que apruebe el CONATEL;
f. Controlar la correcta aplicación de los pliegos tarifarios aprobados por el CONATEL;
g. Controlar que el mercado de las telecomunicaciones se desarrolle en un marco de libre competencia, con las excepciones señaladas en esta Ley,
h. Juzgar a las personas naturales y jurídicas que incurran en las infracciones señaladas en esta Ley y aplicar las sanciones en los casos que correspondan; e,
i. Las demás que le asigne la Ley y el Reglamento.

Art. 36.- Funciones del Superintendente.- Son funciones del Superintendente de Telecomunicaciones las siguientes:

a. Ejercer la representación legal de la Superintendencia en los actos y contratos que sean de su competencia;

b. Nombrar y remover al personal de la Superintendencia, conforme al Orgánico Funcional que dicte;
c. (Sustituido por el Art. 13 de la Ley 94, R.O. 770, 30-VIII-95) Solicitar al CONATEL la aprobación del presupuesto anual;
d. (Sustituido por el Art. 13 de la Ley 94, R.O. 770, 30-VIII-95) Expedir los reglamentos internos necesarios para el cumplimiento de sus funciones.
e. Delegar una o más atribuciones específicas a los funcionarios de la Superintendencia;
f. Ejercer la jurisdicción coactiva de acuerdo con el Código de Procedimiento Civil;
g. Presentar al Congreso Nacional un informe de labores;
h. Juzgar de las infracciones previstas en esta Ley y en la Ley de Radiodifusión y Televisión;
i. Declarar de utilidad pública con fines de expropiación, los bienes que sean indispensables para su normal funcionamiento; y,
j. Las demás previstas en esta Ley.

Art. 37.- Recursos del CONATEL, de la Secretaría Nacional de Telecomunicaciones y de la Superintendencia de Telecomunicaciones.- (Sustituido por el Art. 14 de la Ley 94, R.O. 770, 30-VIII-95).- Sin perjuicio de lo dispuesto en otras leyes generales o especiales, los presupuestos del CONATEL, de la Secretaría Nacional de Telecomunicaciones y de la Superintendencia de Telecomunicaciones se financiarán con los recursos provenientes de la aplicación de las tasas y tarifas por el uso de frecuencias radioeléctricas, así como con los siguientes ingresos:

a. Las herencias, legados, donaciones o transferencias bajo cualquier título que reciban;
b. Los demás fondos, bienes o recursos que le puedan ser asignados en virtud de las leyes y reglamentos aplicables; y,
c. Los intereses, beneficios y rendimientos resultantes de la gestión de sus propios fondos.

Capítulo VII
RÉGIMEN DE LIBRE COMPETENCIA

(Sustituido por el Art. 58 de la Ley 2000-4, R.O. 34-S, 13-III-2000)

Art. 38.- Régimen de libre competencia.- Todos los servicios de telecomunicaciones se brindarán en régimen de libre competencia, evitando los monopolios, prácticas restrictivas o de abuso de posición dominante, y la competencia desleal, garantizando la seguridad nacional, y promoviendo la eficiencia, universalidad, accesibilidad, continuidad y la calidad del servicio. El Consejo Nacional de Telecomunicaciones CONATEL, en uso de sus facultades, expedirá en un plazo no mayor de 180 días, contados a partir de la publicación de la presente Ley en el Registro Oficial, el reglamento que se aplicará para otorgar las concesiones de los servicios de telecomunicaciones que se brindarán en régimen de libre competencia, como consecuencia de la aplicación de la presente Ley. Dicho reglamento deberá contener las disposiciones necesarias para la creación de un Fondo para el desarrollo de las telecomunicaciones en las áreas rurales y urbano-marginales, el cual será financiado por las empresas operadoras de telecomunicaciones, con aportes que se determinen en función de sus ingresos.

Se reconoce a favor de la I. Municipalidad del cantón Cuenca, provincia del Azuay, la titularidad del servicio público de telecomunicaciones, para operar en conexión con el resto del país y el extranjero, pudiendo prestar servicios en forma directa o a través de concesiones.

Art. 39.- (Sustituido por el Art. 58 de la Ley 2000-4, R.O. 34-S, 13-III-2000).- Protección de los derechos de los usuarios.- Todo usuario tiene derecho a recibir el servicio en las condiciones contractuales estipuladas con el proveedor del servicio, y a que dichas condiciones no sean modificadas unilateralmente sin su consentimiento, salvo por fuerza mayor a ser indemnizados por el incumplimiento a dichos términos contractuales por parte del proveedor del servicio.

El Estado garantiza el derecho al secreto y a la privacidad del contenido de las telecomunicaciones. Queda prohibido interceptar, interferir, publicar o divulgar sin consentimiento previo de las partes la información cursada mediante los servicios de telecomunicaciones, bajo las sanciones previstas en la ley para la violación de correspondencia. Los operadores de redes y proveedores de servicios deberán adoptar las medidas necesarias, técnica y económicamente aceptables, para garantizar la inviolabilidad de las telecomunicaciones.

El Estado determinará, a través del reglamento de la presente ley, los mecanismos para que los derechos de los usuarios sean garantizados y satisfechos, incluyendo las modalidades para la solución de los reclamos, mediante procedimientos arbitrales o de mediación, sin perjuicio de lo establecido en la Ley de Defensa del Consumidor y el Usuario.

Las tarifas reflejarán los costos de eficiencia basados en los parámetros internacionales y se facturarán por tiempo efectivo de uso, establecido en horas, minutos y segundos, según corresponda. Los ajustes tarifarios se realizarán de manera gradual.

DISPOSICIONES TRANSITORIAS

(Agregadas por el Art. 59 de la Ley 2000-4, R.O. 34-S, 13-III-2000)

Art. ... (1) .- La participación accionaria del sector privado en el capital de las compañías de telecomunicaciones en las que el Fondo de Solidaridad fuese accionista, se podrá realizar mediante la venta de acciones, atendiendo a la naturaleza de la empresa y el mayor beneficio para el Estado y los usuarios.

Art. ... (2) .- La transferencia de acciones de propiedad del Fondo de Solidaridad a compañías de telecomunicaciones, o del derecho preferente para suscribirlas, se llevará a cabo mediante procedimientos públicos competitivos, en igualdad de condiciones para todos los interesados. Para este propósito, el Fondo de

Solidaridad pondrá a disposición de los interesados un porcentaje de hasta el 51% de acciones con derecho a voto o de suscripción de acciones con derecho a voto en el capital de la empresa. El precio base de la venta será el valor proporcional que resulte de la valoración de las empresas como negocio en marcha, para cuyo efecto se considerará el conjunto de derechos y obligaciones de contenido económico, así como valores intangibles que sean técnicamente admisibles. La valoración será realizada por consultores que acrediten experiencia, solvencia, y serán seleccionados mediante licitación pública internacional.

Art. ... (3) .- Los funcionarios, empleados y trabajadores de ANDINATEL S.A., PACIFICTEL S.A. y EMETEL S.A., Y LA SECRETARÍA NACIONAL DE TELECOMUNICACIONES así como los ex-funcionarios, ex-empleados y ex-trabajadores de las mismas empresas y de la Ex-Empresa Estatal de Telecomunicaciones EMETEL, que hubiesen dejado de prestar sus servicios a las mencionadas entidades a partir del 30 de agosto de 1995, tendrán derecho a adquirir, dentro del plazo de cinco años contados a partir de la fecha de adquisición de acciones por parte de un operador del sector privado, acciones en el capital de cada una de las compañías que resultaron de la escisión de EMETEL S.A. (ANDINATEL S.A. y PACIFICTEL S.A.), en un porcentaje de hasta el diez por ciento (10%) del capital suscrito, al valor que estas acciones tengan en el mercado al momento de pago. Los ex-funcionarios, ex-empleados, ex-trabajadores y jubilados del sector de las telecomunicaciones estatales, que hubieren adquirido esta categoría antes del 30 de agosto de 1995, tendrán derecho a adquirir acciones en las empresas antes mencionadas, dentro del plazo señalado, en un porcentaje de hasta el dos punto cinco por ciento (2.5%) del capital suscrito de cada una de las compañías, al valor que estas acciones tengan en el mercado al momento de pago. En los casos previstos en este párrafo, si la compra se realizare dentro del plazo de un año, el precio de las acciones no será superior al que hubiere pagado el operador del sector privado.

Si vencido el plazo de cinco años no se hubieren adquirido las acciones referidas en el párrafo anterior, el Fondo de Solidaridad estará en libertad de resolver sobre

la venta total o parcial de la parte no adquirida de las acciones representativas del capital social de cada una de las compañías escindidas.

Capítulo VIII
REFORMAS A LA LEY DE RADIODIFUSIÓN Y TELEVISIÓN

(Derogado por el artículo innumerado sexto de las Disposiciones Generales del Título VIII, de la Ley de Radiodifusión y Televisión, agregado por Ley s/n, R.O. 691, 9-V-95)

Dado en la ciudad de Quito, en la Sala de Sesiones del Plenario de las Comisiones Legislativas, a los treinta días del mes de julio de mil novecientos noventa y dos.

FUENTES DE LA PRESENTE EDICIÓN DE LA LEY ESPECIAL DE TELECOMUNICACIONES

1.- Ley 184 (Registro Oficial 996, 10-VIII-92)
2.- Ley s/n (Registro Oficial 691, 9-V-95)
3.- Ley 94 (Registro Oficial 770, 30-VIII-95)
4.- Ley s/n (Suplemento del Registro Oficial 15, 30-VIII-96)
5.- Ley 15 (Suplemento del Registro Oficial 120, 31-VII-97)
6.- Ley 17 (Suplemento del Registro Oficial 134, 20-VIII-97)
7.- Ley 2000-4 (Suplemento del Registro Oficial 34, 13-III-2000).

ANEXO

C

Artículo 422 del Código Penal

ARTÍCULO 422 DEL CÓDIGO PENAL[1]

"**Art. 422 [Interrupción de comunicaciones].-** Será reprimido con prisión de seis meses a dos años el que interrumpiere la comunicación postal, telegráfica, telefónica, radiofónica o de otro sistema, o resistiere violentamente al restablecimiento de la comunicación interrumpida.

Si el acto se realizare en reunión o en pandilla, o la interrupción fuere por medios violentos, vías de hecho o amenazas, la pena será de prisión de tres a cinco años.

Quienes ofrezcan, presten o comercialicen servicios de telecomunicaciones, sin estar legalmente facultados, mediante concesión, autorización, licencia, permiso, convenios o cualquier otra forma de la contratación administrativa, salvo la utilización de servicios de internet, serán reprimidos con prisión de dos a cinco años.

Estarán comprendidos en esta disposición, quienes se encuentren en posesión clandestina de instalaciones que, por su configuración y demás datos técnicos, hagan presumir que entre sus finalidades está la de destinarlos a ofrecer los servicios señalados en el inciso anterior, aún cuando no estén siendo utilizados.

Las sanciones indicadas en este artículo, se aplicarán sin perjuicio de las responsabilidades administrativas y civiles previstas en la Ley Especial de Telecomunicaciones y sus reglamentos."

Nota: La letra cursiva corresponde a los incisos añadidos el 12 de agosto de 1999.

---

1 CÓDIGO PENAL, LEGISLACIÓN CONEXA. LIBRO II, De los delitos en particular. TÍTULO V, De los delitos contra la seguridad pública. CAPÍTULO VIII, De los delitos contra los medios de transporte y de comunicación, Art. 422.

ANEXO

D

Bandas de frecuencias satelitales

BANDAS DE FRECUENCIAS SATELITALES[1]

Bandas de frecuencias satelitales		
Banda	**Designación (GHz)**	**Servicio Típico**
L	1 – 2	BSS (sonido), MSS
S	2 – 4	MSS, BSS (sonido)
C	(6 / 4)	FSS, BSS (TV)
X	7 – 8	Militar, FSS
Ku	(14/11), (14,12),(17/12)	FSS, BSS (TV)
Ka	(30 / 20)	FSS, BSS, MSS

1 http://www.emp-centauri.cz

ANEXO
E

Intervenciones realizadas por la Superintendencia de Telecomunicaciones a estaciones de radiodifusión, sistemas de televisión por cable, y sistemas de By pass, que operaban sin autorización.

(Documento proporcionado por la SUPTEL)

SUPERINTENDENCIA DE TELECOMUNICACIONES

Oficio No. ITG.2006. 1600

Quito, 09 JUN. 2006

Señor
Christian Gallardo
Quito

De mi consideración:

Me refiero a su comunicación ingresada a esta Superintendencia con hoja de trámite No. 03336, en la cual usted manifiesta que, en razón de que se encuentra desarrollando su proyecto de titulación, previa obtención del título de Ingeniero en Electrónica y Telecomunicaciones, ante lo cual manifiesto lo siguiente:

- En el Anexo 1 de este documento encontrará el Cuadro de Intervenciones realizadas por esta Superintendencia a estaciones y sistemas de telecomunicaciones que operaban sin autorización, actualizado a la fecha de emisión de este oficio.
- En el Anexo 2 se incluye el documento denominado: "Interconexión Internacional", solicitado en su comunicación.
- Al respecto del valor promedio aproximado en cuanto a la tasa de terminación para llamadas telefónicas internacionales entrantes a Ecuador, considero que para efectos de un cálculo aproximado se puede considerar un valor de promedio de 11.8 centavos de dólar.

Atentamente,

Ing. Nelson Peñafiel Barrezueta
INTENDENTE GENERAL DE TELECOMUNICACIONES

ANEXO 1

SUPERINTENDENCIA DE TELECOMUNICACIONES
DIRECCIÓN DE INVESTIGACIÓN ESPECIAL

INTERVENCIONES

INTERVENCIONES REALIZADAS POR LA SUPERINTENDENCIA DE TELECOMUNICACIONES A ESTACIONES DE RADIODIFUSIÓN, SISTEMAS DE TELEVISION POR CABLE, Y SISTEMAS DE BY PASS, QUE OPERABAN SIN AUTORIZACIÓN.

PERIODO I : DESDE AGOSTO DE 1992 (CREACION DE LA SUPTEL) HASTA EL 23 DE SEPTIEMBRE DE 1998

INTERVENCIÓN A:	NUMERO DE INTERVENCIONES (EN EL PERIODO I)
ESTACIONES DE RADIODIFUSION	21
SISTEMAS DE TV POR CABLE	1
SISTEMAS DE BY PASS	1
TOTAL GENERAL	23

PERIODO II : DESDE EL 24 DE SEPTIEMBRE DE 1998 HASTA EL 6 DE JUNIO DE 2006

INTERVENCIÓN A:	NUMERO DE INTERVENCIONES									
	1998 desde 24 sept	1999	2000	2001	2002	2003	2004	2005	2006	TOTAL POR SERVICIO
ESTACIONES DE RADIODIFUSION	13	21	8	_	11	4	1	2	_	60
SISTEMAS DE TV	_	3	35	15	1	8	7	7	1	77
SISTEMAS DE BY PASS	_	24	30	33	21	10	18	13	13	162
TOTAL GENERAL										299

NÚMERO TOTAL DE INTERVENCIONES
EN EL PERIODO I : **23**

NÚMERO TOTAL DE INTERVENCIONES
EN EL PERIODO II : **299**

ANEXO

F

Configuración de equipos de telecomunicaciones

CONFIGURACIÓN DE EQUIPOS DE TELECOMUNICACIONES

ASIGNACIÓN DE DIRECCIONES IP, NÚMEROS TELEFÓNICOS Y CONFIGURACIÓN DEL EQUIPO EN EL LOCAL CLANDESTINO (EEUU)

El número telefónico correspondiente a las líneas telefónicas instaladas en el local clandestino en Estados Unidos, ha sido asignado tomando como referencia los datos que se indica en el CAPÍTULO II “Fraude en telefonía fija”, Figura 2.18. Tarjeta telefónica.

Las direcciones IP de los equipos de telecomunicaciones instalados en el local clandestino en Estados Unidos son asignadas por el defraudador, la dirección IP correspondiente al enlace proporcionado por el telepuerto privado es asignada por el proveedor del servicio.

Consideraciones:

En el ejemplo de configuración de los equipos de telecomunicaciones se considera varios aspectos como son:

- El número telefónico asignado a las líneas telefónicas es el que consta en la tarjeta telefónica que se indica en el CAPÍTULO II “Fraude en telefonía fija”, Figura 2.18. Tarjeta telefónica.
- Para la asignación de direcciones IP a los equipos de telecomunicaciones instalados en el local clandestino, se ha considerado la utilización de direcciones IP privadas clase C con máscara por defecto.

Una propuesta válida de asignación de direcciones IP y números telefónicos en el local clandestino en Estados Unidos, es la que se indica en la figura a continuación.

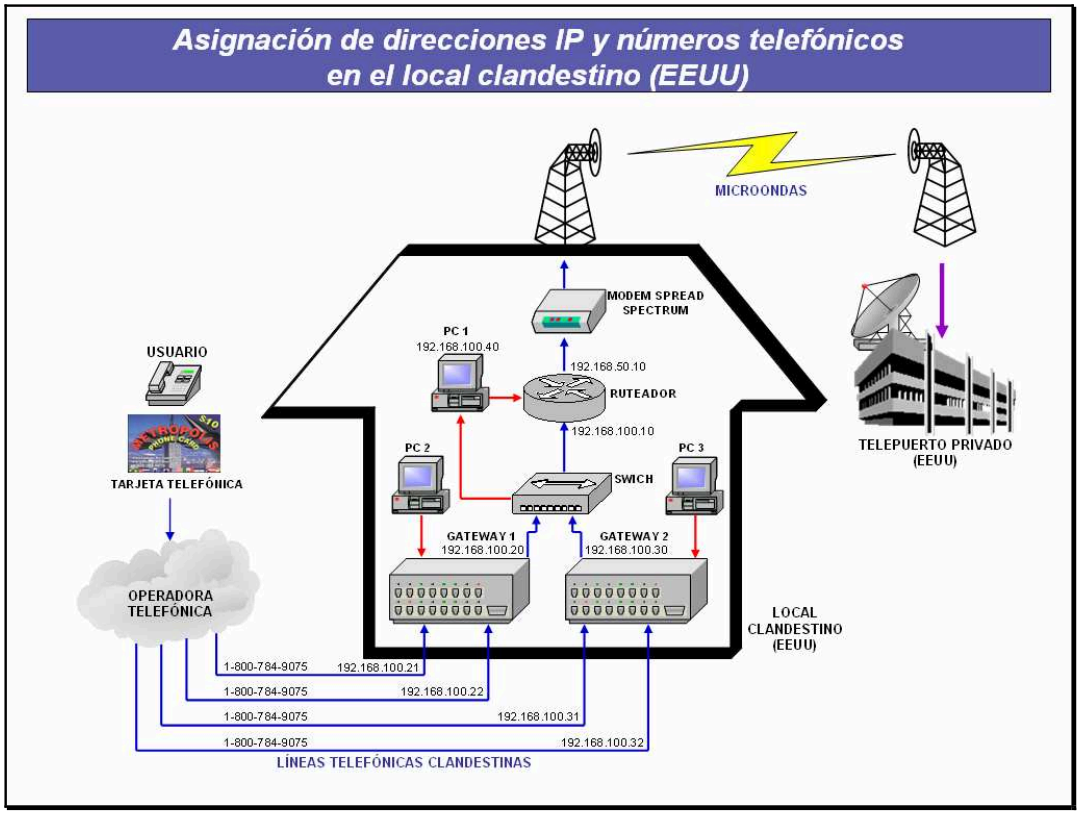


Figura E.1. (EEUU) Asignación de direcciones IP y números telefónicos en el local clandestino

Como se observa en la figura, los equipos que requieren ser configurados son:

PC1 (Sistema operativo Windows XP)

Mediante un software instalado en la computadora se realiza el control del saldo y tiempo útil de la tarjeta telefónica.

RUTEADOR (CISCO 1600)

Permite establecer el enlace entre la red de telecomunicaciones del local clandestino y la red del telepuerto privado.

GATEWAYS (MVP 800)

Permiten la convergencia entre una red de datos y una red telefónica pública conmutada.

Configuración del PC1 (Sistema operativo Windows XP)

- *Paso 1. Ingresar a Conexión de área local*

En la barra de tareas de Windows XP:
Inicio > Panel de control > Conexiones de red > Conexión de área local

- *Paso 2. Configurar propiedades de protocolo Internet (TCP/IP)*

En la ventana emergente “Propiedades de Conexión de área local” se escoge “Protocolo Internet (TCP/IP)” y se selecciona Propiedades.
En la ventana emergente “Propiedades de Protocolo Internet (TCP/IP)” se Configuran los parámetros necesarios.

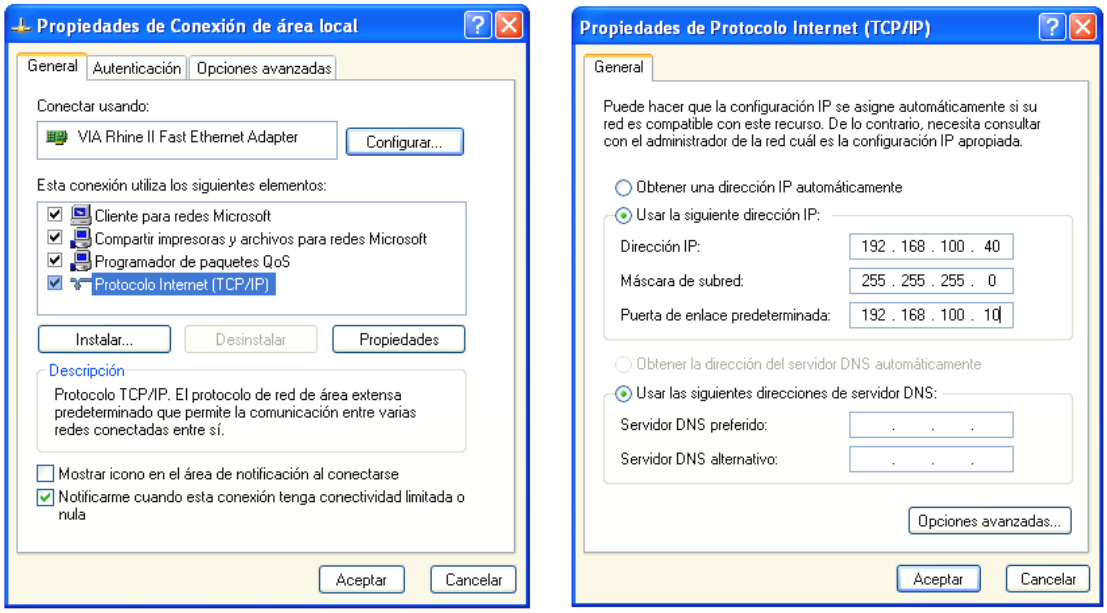


Figura E.2. (EEUU) Configuración de propiedades de protocolo Internet

Configuración del RUTEADOR (CISCO 1600)

Con la computadora PC 1 (sistema operativo Windows XP) conectada al RUTEADOR se inicia la configuración.

- *Paso 1. Iniciar el programa HyperTerminal*

En la barra de tareas de Windows XP:
Inicio > Todos los programas > Accesorios > Comunicaciones > HyperTerminal

- *Paso 2. Indicar nombre para la sesión de HyperTerminal*

En la ventana emergente “Descripción de la conexión” se introduce el nombre en el campo Nombre de la conexión y se selecciona Aceptar

Figura E.3. (EEUU) Descripción de la conexión

- *Paso 3. Especificar la interfaz de conexión de los computadores y las propiedades de conexión de la interfaz*

En la ventana emergente “Conectar a”, se selecciona el COM habilitado del computador al cual se encuentra conectado el computador PC1.En la ventana emergente “Propiedades de COM1” se selecciona los parámetros

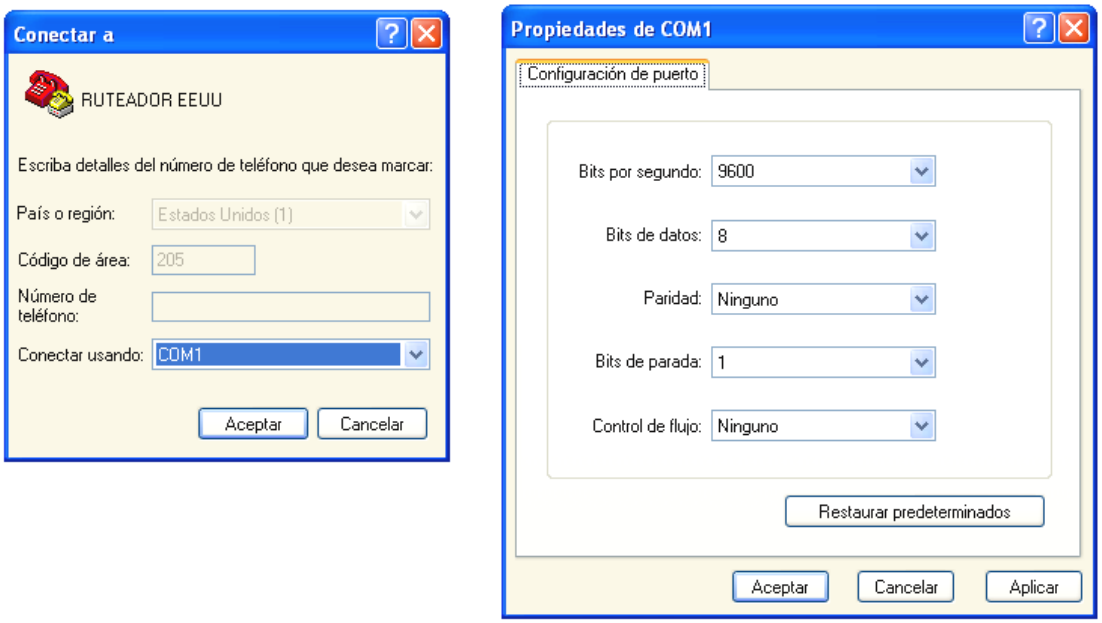


Figura E.4. (EEUU) Especificación de las propiedades de conexión de la interfaz

Realizado el procedimiento correcto se establece la sesión, y mediante el programa HyperTerminal se inicia la configuración del RUTEADOR.

Parámetros a ser configurados en el RUTEADOR EEUU.

Nombre del router	Tipo de interfaz	Dirección serial 0	Dirección Ethernet 0	Máscara de subred	Contraseña enable secret	Contraseñas enable / VTY / Consola
EEUU	DCE	192.168.50.10	192.168.100.10	255.255.255.0	STAR	EEUU

NOTA:

- Los parámetros a ser configurados son asignados por la persona que configura el RUTEADOR del local clandestino en EEUU.
- Existen varias consideraciones al momento de configurar el RUTEADOR, sin embargo se ha tomado en cuenta únicamente los parámetros necesarios para establecer el enlace.
- El tipo de interfaz correspondiente al telepuerto privado debe ser configurado como DTE para poder establecer el enlace entre el local clandestino y el telepuerto privado.

- *Paso 4. Configuración del RUTEADOR*

En la figura se indican los comandos utilizados para la configuración del RUTEADOR

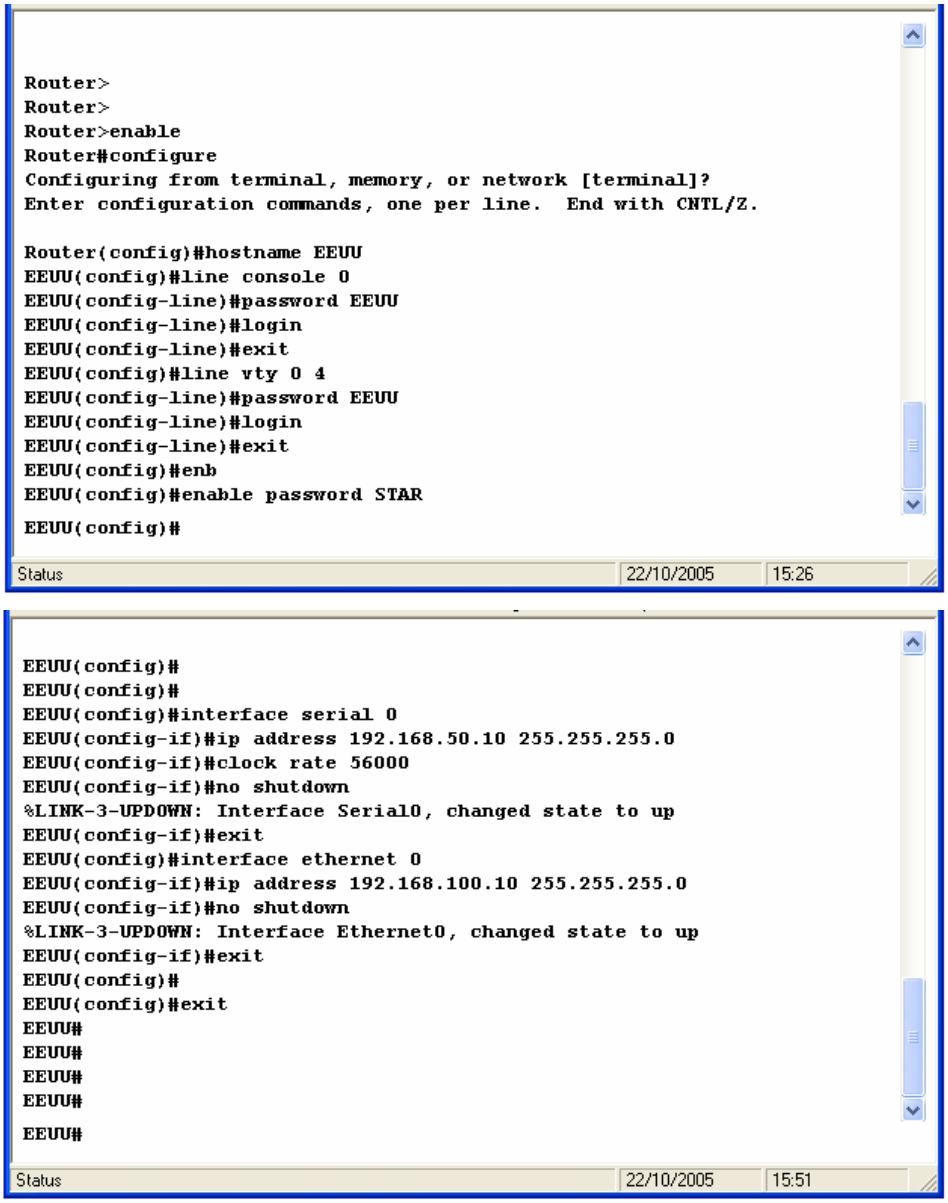


Figura E.5. (EEUU) Comandos de configuración del RUTEADOR

Configuración del GATEWAY 1 (MVP 800)

Se requiere tener instalado el software MultiVOIP MVP800 en el computador desde el cual se configuran los GATEWAYS, con el software instalado en el computador PC 2 (Sistema operativo Windows 98) y conectado al mismo el GATEWAY se inicia la configuración.

- *Paso 1. Iniciar el programa MultiVOIP 800*

En la barra de tareas de Windows 98:
Inicio > Programas > MultiVOIP 800 v.301E > Download Factory Defaults

- *Paso 2. Configuración de IP Protocol Default Setup*

En la ventana emergente "MultiVOIP 800 - IP Protocol Default Setup" se configura los parámetros para Ethernet y se selecciona OK.

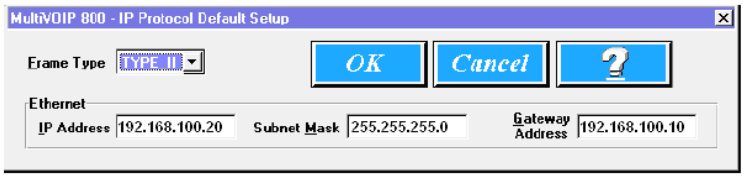


Figura E.6. (EEUU) Configuración de IP Protocol Default Setup

- *Paso 3. Selección de opciones para configuración del GATEWAY*

En la ventana emergente "MultiVOIP 800 v.301E Setup (Firmware: Apr 20 2001) Voice Coder: v1.60" se escoge las opciones para configuración del GATEWAY.

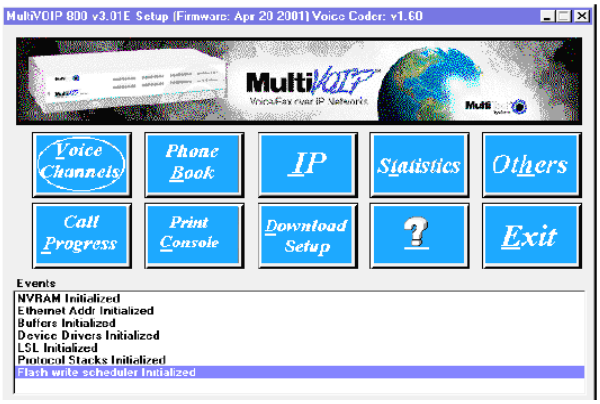


Figura E.7. (EEUU) Opciones para configuración del GATEWAY

- *Paso 4. Selección de Voice Channels*

En la ventana emergente "MultiVOIP 800 – Channel Setup" se escoge el tipo de interfaz y el canal al cual se conectan las líneas telefónicas, se selecciona OK.

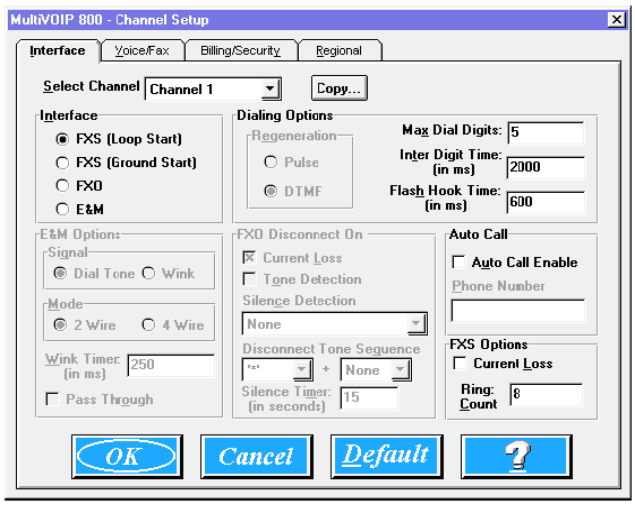


Figura E.8. (EEUU) Selección de Voice Channels

- *Paso 5. Selección de Phone Book*

En la ventana emergente "MultiVOIP 800 – Phone Directory Database" se selecciona Add (+) para empezar a llenar la base de datos del GATEWAY.

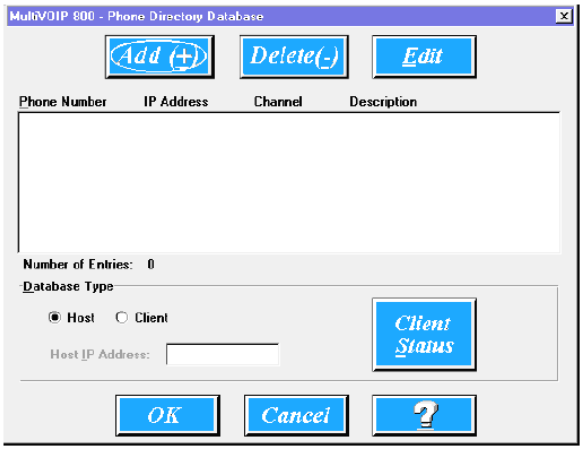


Figura E.9. (EEUU) Selección de Phone Book

- *Paso 6. Ingreso, edición de la base de datos*

En la ventana emergente "MultiVOIP 800 – Add/Edit Phone Entry" se ingresa la información para alimentar la base de datos del GATEWAY.

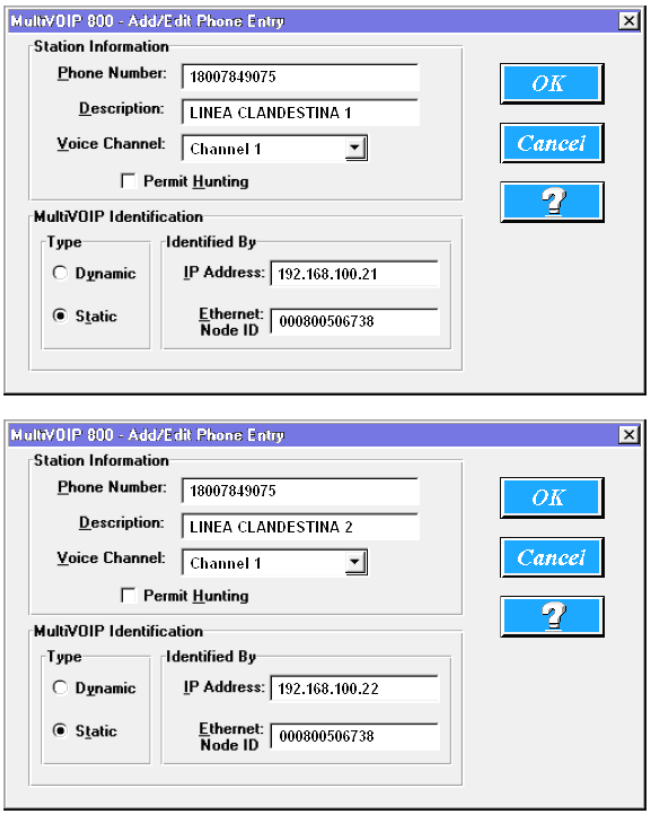


Figura E.10. (EEUU) Ingreso, edición de la base de datos

Al terminar de ingresar los datos, se observa en la ventana emergente “MultiVOIP 800 – Phone Directory Database” la información que será descargada en el GATEWAY.

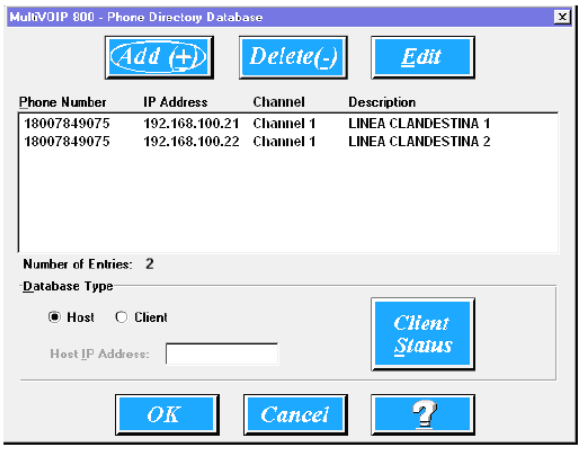


Figura E.11. (EEUU) Visualización de Phone Directory Database

- *Paso 7. Selección de Download Setup*

En la ventana emergente “MultiVOIP 800 – Checking MultiVOIP” se selecciona OK para transferir la base de datos al GATEWAY.

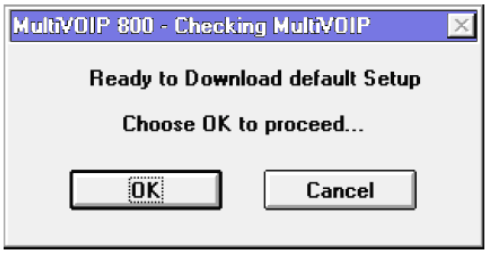


Figura E.12. (EEUU) Selección de Download Setup

ASIGNACIÓN DE DIRECCIONES IP, NÚMEROS TELEFÓNICOS Y CONFIGURACIÓN DEL EQUIPO EN EL LOCAL CLANDESTINO (ECUADOR)

El número telefónico correspondiente a las líneas telefónicas instaladas en el local clandestino en Ecuador, corresponde a las líneas telefónicas que han sido obtenidas ilícitamente.

Las direcciones IP de los equipos de telecomunicaciones instalados en el local clandestino en Ecuador son asignadas por la persona que comete el fraude, la dirección IP correspondiente al enlace proporcionado por el telepuerto privado es asignada por el proveedor del servicio.

Consideraciones:

En el ejemplo de configuración de los equipos de telecomunicaciones se considera varios aspectos como son:

- El número telefónico asignado a las líneas telefónicas ha sido representado por los números 02 2-111-111, 02 2 -222-222, 02 2-333-333, 02 2-444-444.

- Para la asignación de direcciones IP a los equipos de telecomunicaciones instalados en el local clandestino, se ha considerado la utilización de direcciones IP privadas clase C con máscara por defecto.

Una propuesta válida de asignación de direcciones IP y números telefónicos en el local clandestino en Ecuador, es la que se indica en la figura a continuación.

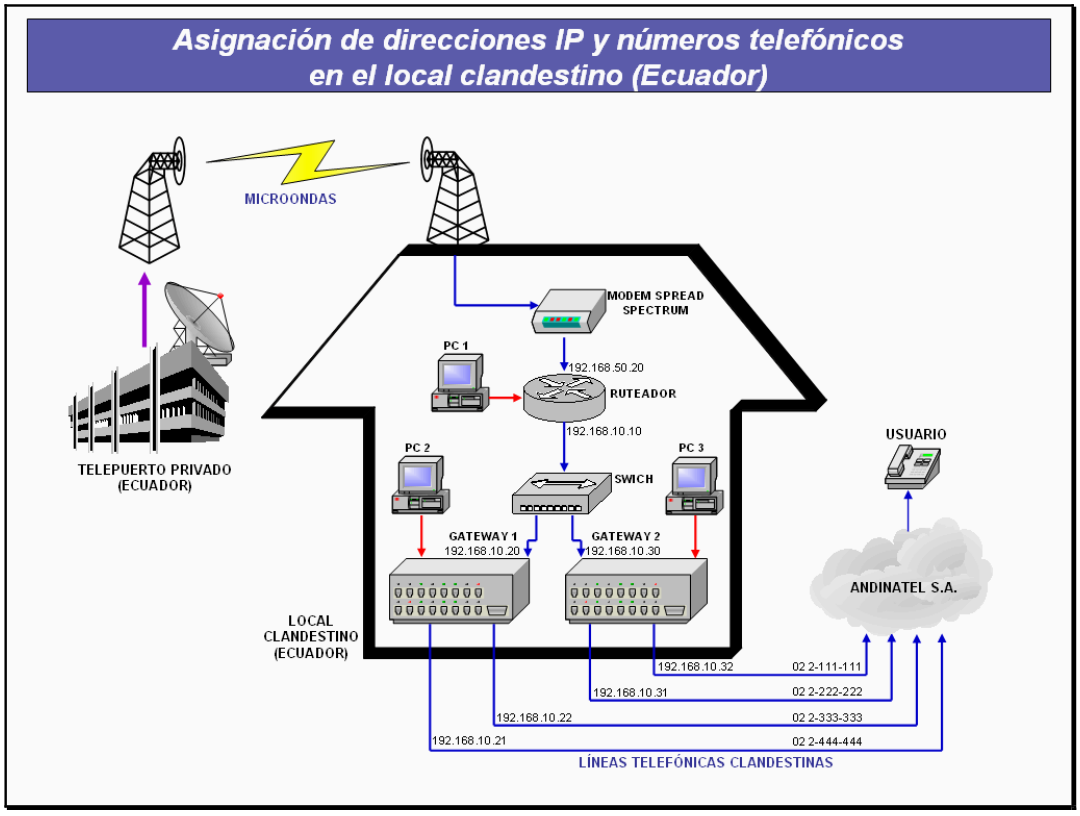


Figura E.13. (Ecuador) Asignación de direcciones IP y números telefónicos en el local clandestino

Como se observa en la figura, los equipos que requieren ser configurados son:

RUTEADOR (CISCO 1600)

Permite establecer el enlace entre la red de telecomunicaciones del local clandestino y la red del telepuerto privado.

GATEWAYS (MVP 800)

Permiten la convergencia entre una red de datos y una red telefónica pública conmutada.

Configuración del RUTEADOR (CISCO 1600)

Con la computadora PC 1 (sistema operativo Windows XP) conectada al RUTEADOR se inicia la configuración.

- *Paso 1. Iniciar el programa HyperTerminal*

En la barra de tareas de Windows XP:
Inicio > Todos los programas > Accesorios > Comunicaciones > HyperTerminal

- *Paso 2. Indicar nombre para la sesión de HyperTerminal*

En la ventana emergente “Descripción de la conexión” se introduce el nombre en el campo Nombre de la conexión y se selecciona Aceptar

Figura E.14. (Ecuador) Descripción de la conexión

- *Paso 3. Especificar la interfaz de conexión de los computadores y las propiedades de conexión de la interfaz*

En la ventana emergente “Conectar a”, se selecciona el COM habilitado del computador al cual se encuentra conectado el computador PC1. En la ventana emergente “Propiedades de COM1” se selecciona los parámetros

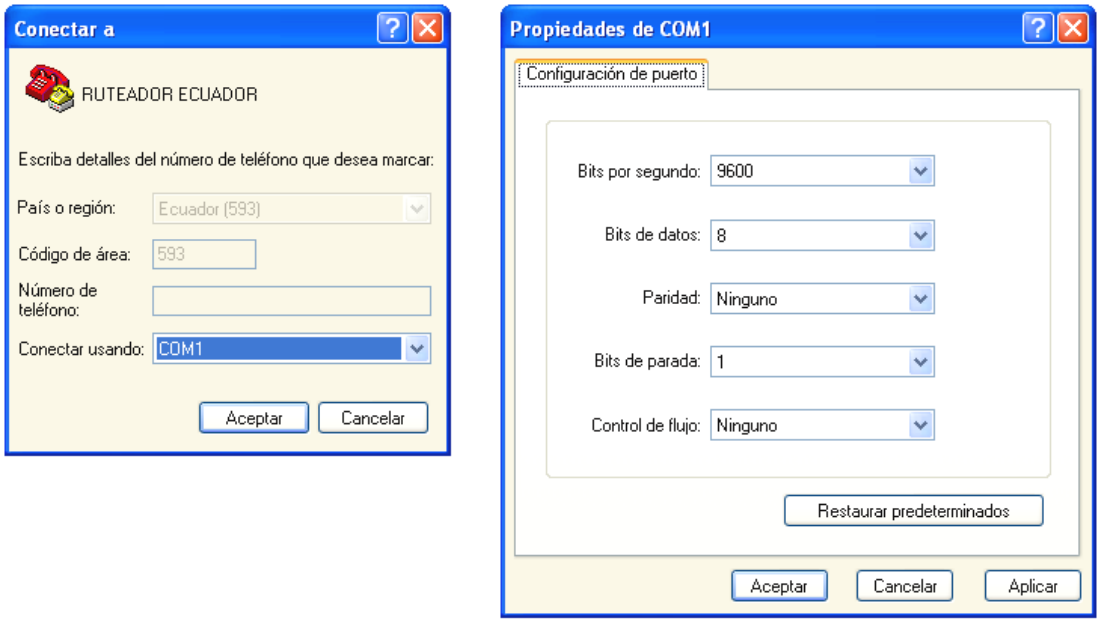


Figura E.15. (Ecuador) Especificación de las propiedades de conexión de la interfaz

Realizado el procedimiento correcto se establece la sesión, y mediante el programa HyperTerminal se inicia la configuración del RUTEADOR.

Parámetros a ser configurados en el RUTEADOR ECUADOR.

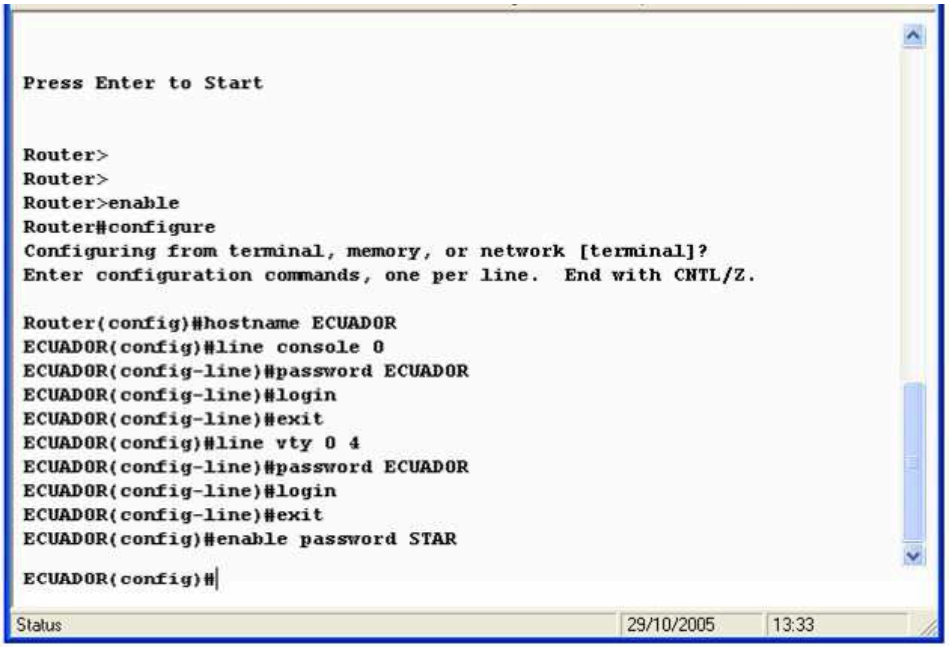
Nombre del router	Tipo de interfaz	Dirección serial 0	Dirección Ethernet 0	Máscara de subred	Contraseña enable secret	Contraseñas enable / VTY / Consola
ECUADOR	DCE	192.168.50.20	192.168.10.10	255.255.255.0	STAR	ECUADOR

NOTA:

- Los parámetros a ser configurados son asignados por la persona que configura el RUTEADOR del local clandestino en ECUADOR.
- Existen varias consideraciones al momento de configurar el RUTEADOR, sin embargo se ha tomado en cuenta únicamente los parámetros necesarios para establecer el enlace.
- El tipo de interfaz correspondiente al telepuerto privado debe ser configurado como DTE para poder establecer el enlace entre el local clandestino y el telepuerto privado.

- *Paso 4. Configuración del RUTEADOR*

En la figura se indican los comandos utilizados para la configuración del RUTEADOR.



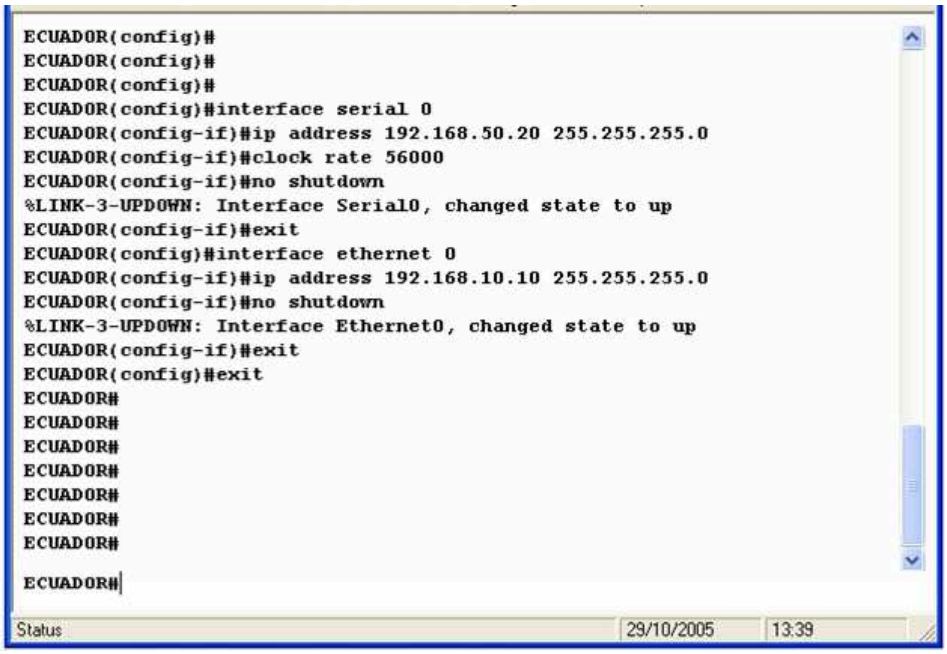


Figura E.16. (Ecuador) Comandos de configuración del RUTEADOR

Configuración del GATEWAY 1 (MVP 800)

Se requiere tener instalado el software MultiVOIP MVP800 en el computador desde el cual se configuran los GATEWAYS, con el software instalado en el computador PC 2 (Sistema operativo Windows 98) y conectado al mismo el GATEWAY se inicia la configuración.

- *Paso 1. Iniciar el programa MultiVOIP 800*

En la barra de tareas de Windows 98:
Inicio > Programas > MultiVOIP 800 v.301E > Download Factory Defaults

- *Paso 2. Configuración de IP Protocol Default Setup*

En la ventana emergente "MultiVOIP 800 - IP Protocol Default Setup" se configura los parámetros para Ethernet y se selecciona OK.

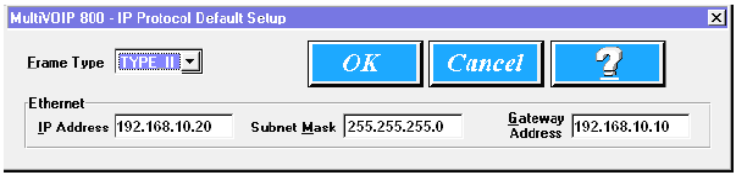


Figura E.17. (Ecuador) Configuración de IP Protocol Default Setup

- *Paso 3. Selección de opciones para configuración del GATEWAY*

En la ventana emergente "MultiVOIP 800 v.301E Setup (Firmware: Apr 20 2001) Voice Coder: v1.60" se escoge las opciones para configuración del GATEWAY.

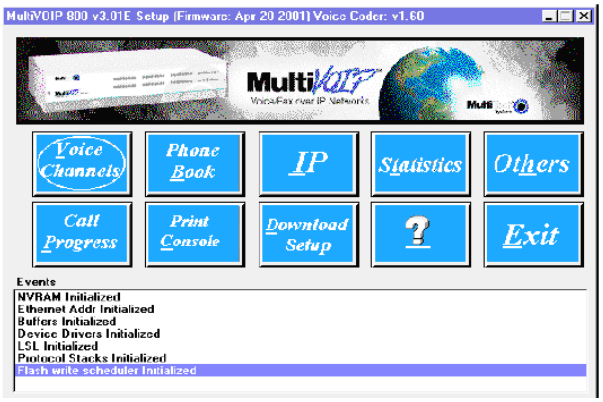


Figura E.18. (Ecuador) Opciones para configuración del GATEWAY

- *Paso 4. Selección de Voice Channels*

En la ventana emergente "MultiVOIP 800 – Channel Setup" se escoge el tipo de interfaz y el canal al cual se conectan las líneas telefónicas, se selecciona OK.

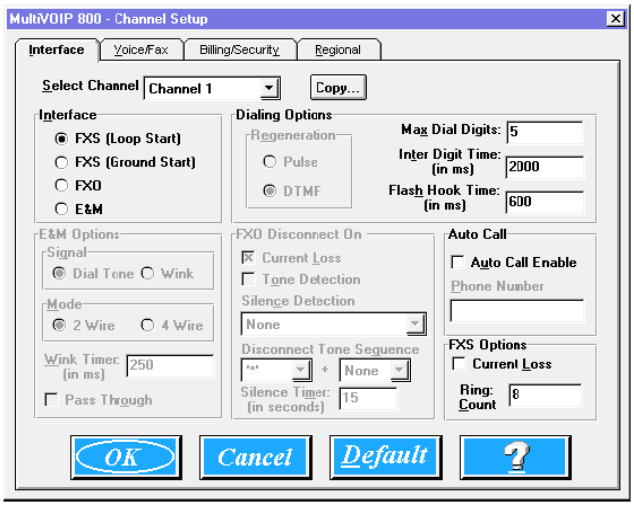


Figura E.19. (Ecuador) Selección de Voice Channels

- *Paso 5. Selección de Phone Book*

En la ventana emergente "MultiVOIP 800 – Phone Directory Database" se selecciona Add (+) para empezar a llenar la base de datos del GATEWAY.

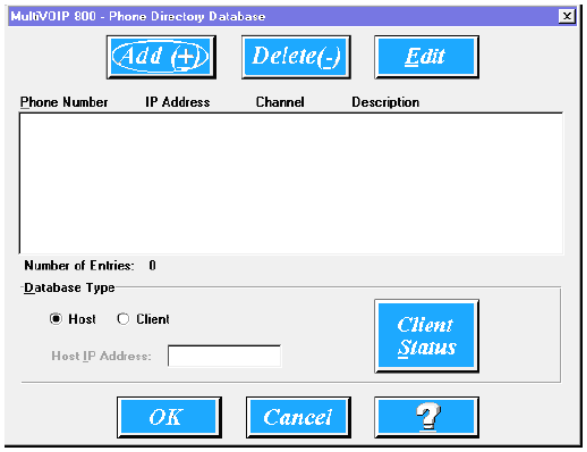


Figura E.20. (Ecuador) Selección de Phone Book

- *Paso 6. Ingreso, edición de la base de datos*

En la ventana emergente "MultiVOIP 800 – Add/Edit Phone Entry" se ingresa la información para alimentar la base de datos del GATEWAY.

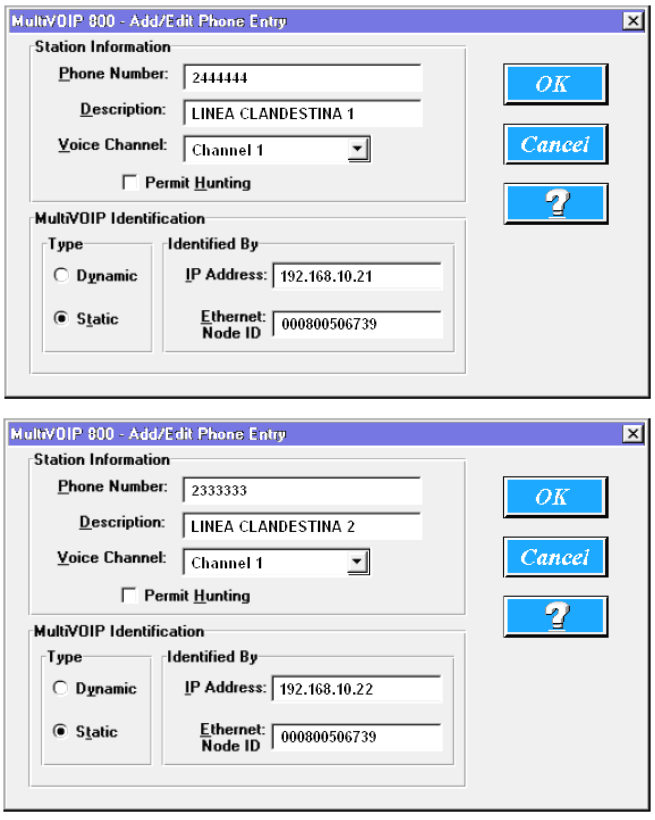


Figura E.21. (Ecuador) Ingreso, edición de la base de datos

Al terminar de ingresar los datos, se observa en la ventana emergente “MultiVOIP 800 – Phone Directory Database” la información que será descargada en el GATEWAY.

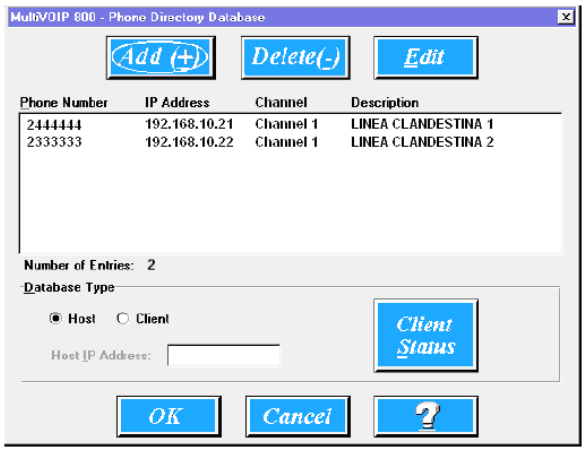


Figura E.22. (Ecuador) Visualización de Phone Directory Database

- *Paso 7. Selección de Download Setup*

En la ventana emergente “MultiVOIP 800 – Checking MultiVOIP” se selecciona OK para transferir la base de datos al GATEWAY.

Figura E.23. (Ecuador) Selección de Download Setup

Prueba de conexión de los equipos de telecomunicaciones en el local clandestino (Ecuador)

Para verificar que el RUTEADOR y los GATEWAYS estén configurados y funcionen correctamente, se utiliza el comando ping, el cual indica si existe comunicación entre los equipos.

Al hacer ping desde el RUTEADOR hacia los interfaces de los GATEWAYS la respuesta es favorable, tal como se indica en la siguiente figura.

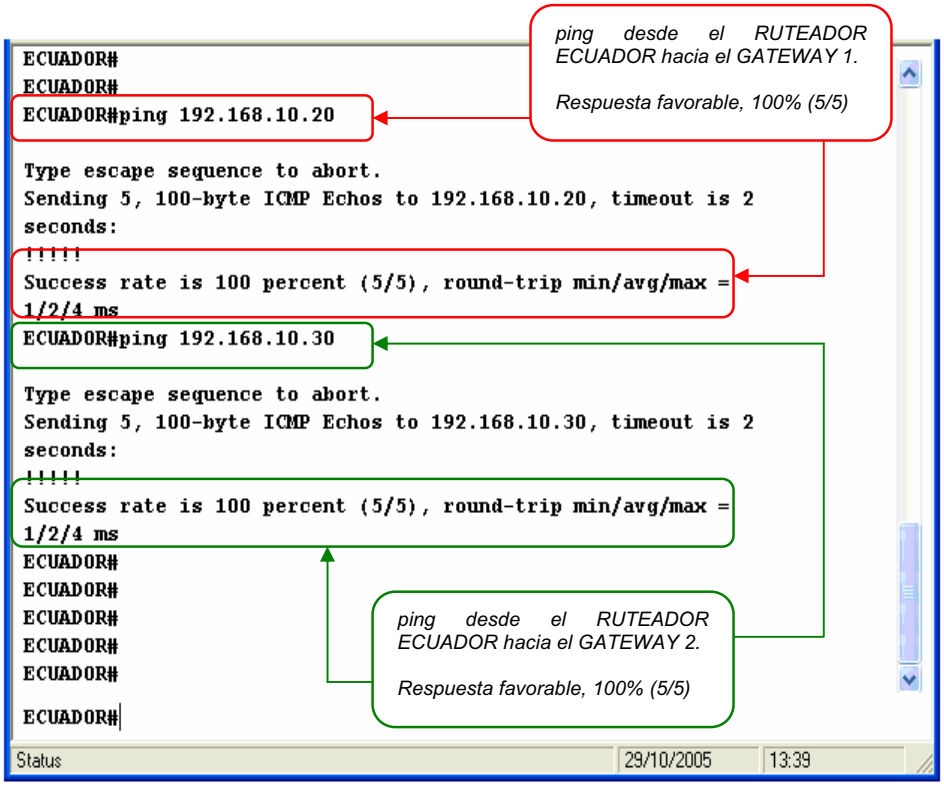


Figura E.24. (Ecuador) Prueba de conexión de los equipos de telecomunicaciones en el local clandestino

Fotos de equipos de telecomunicaciones en el local clandestino (Ecuador)

Figura E.25. Conexión del computador al RUTEADOR

Figura E.26. Conexión del computador al GATEWAY

Figura E.27. Antena Spread Spectrum

Figura E.28. Conexión de la antena al MODEM SPREAD SPECTRUM, Conexión del MODEM SPREAD SPECTRUM al RUTEADOR

Figura E.29. Conexión del RUTEADOR al SWICH

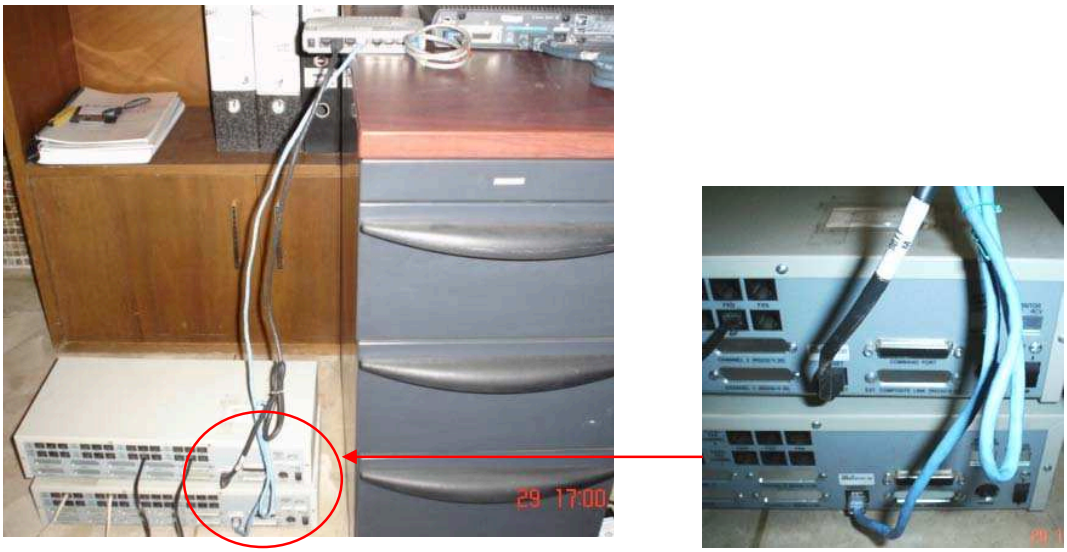


Figura E.30. Conexión del SWICH al GATEWAY

Figura E.31. Conexión del GATEWAY a las líneas telefónicas

ANEXO

6

Interconexión internacional

(Documento proporcionado por la SUPTEL)

SUPERINTENDENCIA DE TELECOMUNICACIONES

Oficio No. ITG.2006. 1600

Quito, 09 JUN. 2006

Señor
Christian Gallardo
Quito

De mi consideración:

Me refiero a su comunicación ingresada a esta Superintendencia con hoja de trámite No. 03336, en la cual usted manifiesta que, en razón de que se encuentra desarrollando su proyecto de titulación, previa obtención del título de Ingeniero en Electrónica y Telecomunicaciones, ante lo cual manifiesto lo siguiente:

- En el Anexo 1 de este documento encontrará el Cuadro de Intervenciones realizadas por esta Superintendencia a estaciones y sistemas de telecomunicaciones que operaban sin autorización, actualizado a la fecha de emisión de este oficio.
- En el Anexo 2 se incluye el documento denominado: "Interconexión Internacional", solicitado en su comunicación.
- Al respecto del valor promedio aproximado en cuanto a la tasa de terminación para llamadas telefónicas internacionales entrantes a Ecuador, considero que para efectos de un cálculo aproximado se puede considerar un valor de promedio de 11.8 centavos de dólar.

Atentamente,

Ing. Nelson Peñafiel Barrezueta
INTENDENTE GENERAL DE TELECOMUNICACIONES

ANEXO 2

AYUDA DE MEMORIA

TEMA: INTERCONEXIÓN INTERNACIONAL

RÉGIMEN TRADICIONAL

Su sistema de remuneraciones se basa en la TASA DE DISTRIBUCIÓN.

Definiciones:

- *Tasa de Distribución.-* Tasa fijada por las Administraciones en una relación dada y que sirve para el establecimiento de las cuentas internacionales,
- *Tasa Contable.-* La tasa contable, también denominada tasa de contabilidad, tasa de distribución o tasa de percepción, es la tarifa que se negocia por cada minuto de comunicación entre operadores de larga distancia internacional, por cursar, originar y terminar llamadas entre dos países. El proceso de liquidación de las tasas contables entre países se realiza en base a la negociación de una tarifa entre las partes, al momento de conciliar tráfico entre dos países, el de mayor tráfico originado debe transferir el monto correspondiente a la mitad de la tasa contable -denominada tasa de liquidación- por los minutos excedentes al país receptor del mismo.
- *Tasa de Liquidación.-* Mitad de la tasa de distribución.

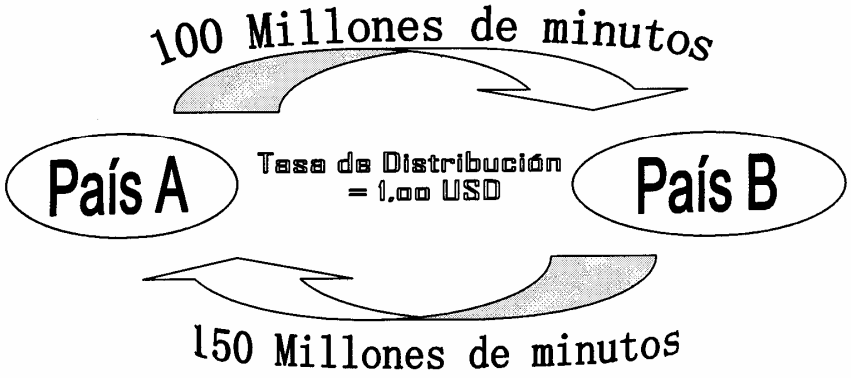
Fundamentos:

- Abarca dos operadores de distintos países,
- Para cursar una comunicación internacional, dos operadores de diferente país **deben cooperar o actuar conjuntamente,**
- Cada operador proporciona en su propio territorio lo que se conoce como una mitad del circuito,
- No ha sido orientada a costos (Se elaboró la Recomendación D.140 para corregir este factor),
- Es discriminatoria (Se elaboró la Recomendación D.140 para corregir este factor).

Ejemplo:

Si la empresa del país A envía a la empresa del país B 100 Millones de minutos y la empresa del país B envía a la empresa del país A 150 Millones de minutos, el número de minutos excedentes es de 50 millones. Si la tasa de distribución es de USD 1, la tasa de liquidación es de USD 0.5. Por lo tanto, sobre la base de 50

Millones de minutos de exceso, la empresa del país B tendría que pagar a la empresa del país A un importe de USD 25 millones.



Diferencia B-A = 50'000.000

50'000.000 x 0,5 (tasa de liquidación) = 25'000.000

De los 150 millones de dólares cobrados por la empresa del país B, debe entregar 25 millones a la empresa del país A.

Ambos países han recibido la cantidad de 125 millones de dólares

Nota:

1. Los pagos de Liquidación han servido para financiar la construcción de las infraestructuras de telecomunicaciones nacionales y para subsidiar las comunicaciones locales y nacionales
2. La UIT estima que durante el decenio 1990-2000 los pagos de liquidación desde los países desarrollados hacia los países en desarrollo ascendió a unos 50'000'000.000,oo de dólares americanos.
3. Con la aprobación de la Recomendación D.140 en 1992, se produjo una notable reducción de las tasas de distribución, hacia los costos.

En 1998 se aprueba la revisión de la Recomendación D.150 y se incluyeron tres nuevos procedimientos para compensar a las empresas que terminan tráfico internacional, estos son:

- Procedimiento de las Tasas de Terminación,
- Procedimiento de las Tasas de Liquidación, y,
- Acuerdos comerciales negociados bilateralmente.

TASA DE TERMINACIÓN

Es el valor establecido por el operador (o el gobierno) de destino para terminar el tráfico de entrada en su red de telecomunicaciones.

Fundamentos:

- Es una tasa única establecida por un operador (o gobierno) y se aplica a todo el tráfico, con independencia de su origen,
- No puede ser impuesta unilateralmente, sino como el resultado de un acuerdo bilateral y de acuerdo a los costos,
- Se pueden aceptar variaciones significativas de costos por: diferencias de volumen de tráfico, zona geográfica, (tecnología). Siempre que no sean discriminatorias y se pongan a disposición de todas las empresas de manera transparente,
- Permite la introducción de tasas asimétricas, ya que toma en cuenta que la mayor parte de los bienes capitales de las empresas operadoras de los países en desarrollo son importados,
- Es de fácil manejo, sin embargo es el único que va acompañado de condiciones pormenorizadas para la puesta en práctica,
- Esta diseñada para los acuerdos de tráfico suscritos entre operadores en régimen de monopolio y operadores en mercados en régimen de competencia.

La tasa de terminación debe ser fijada de acuerdo a:

- Una metodología de determinación de costos aceptada mutuamente por las operadoras origen y destino,
- Una formula de determinación de costos contenida en las Recomendaciones de la UIT.

La tasa de terminación debe recuperar los costos para:

- Utilización de la central internacional de la empresa que termina la llamada,
- La extensión nacional incluido el bucle local,
- El circuito internacional si este fuera proporcionado por el operador que termina la llamada, y,
- Se puede incluir cualquier costo adicional que se imponga a un operador en virtud de la reglamentación nacional.

Ejemplo:

Supongamos una llamada originada en el Ecuador por ANDINATEL hacia USA, a través de la empresa AT&T. Los costos reales son de aproximadamente 3,0 cent/min para ANDINATEL y de 2,5 cent/min para AT&T.

El costo básico de la llamada internacional saliente será la suma de los dos costos reales, más los costos para subir la señal al satélite (up link) y subsidios cruzados para la telefonía local, regional y nacional.

	3,0	Valor recaudado para ANDINATEL S.A.
+	**2,5**	Valor recaudado para AT&T
	0,5	Costos satelitales
	6,0	Costos de ANDINATEL para completar la llamada internacional
+	**36,0**	Subsidio a la telefonía local, regional y nacional
	42,0	Valor final de la llamada, que debe ser cancelado por el abonado en Ecuador

Para el caso de una llamada internacional entrante, el abonado en Ecuador no cancela ningún valor por recibir la llamada, únicamente ANDINATEL recibirá directamente de AT&T el valor de 11,8 cent/min, por concepto de tasa de terminación.

TASA DE LIQUIDACIÓN

Este procedimiento no tiene nada que ver con el procedimiento tradicional de división de la tasa de distribución.

El operador que origina el tráfico compra una terminación al operador que termina el tráfico y le paga una tasa de liquidación por minuto.

Fundamentos:

- Esta se negocia bilateralmente entre los operadores de originación y terminación de la llamada internacional,
- Es una tasa teóricamente basada en costos,
- Los servicios de telecomunicaciones se consideran como objeto de comercio y no como un servicio suministrado en forma conjunta,
- Está diseñado para adaptarse al entorno de las **nuevas telecomunicaciones,**
- Permite la introducción de tasas asimétricas, ya que toma en cuenta que la mayor parte de los bienes capitales de las empresas operadoras de los países en desarrollo son importados,
- **Es transparente**, los valores serán divulgados ya sea mediante la publicación o como resultado de una solicitud.

Ejemplo: Será similar a la tasa de terminación, sin embargo los minutos serán negociados como artículos de consumo, el valor a pagar por la terminación de tráfico será de dominio público y estará teóricamente basado en costos.

ACUERDOS COMERCIALES NEGOCIADOS BILATERALMENTE

Fundamentos:

- Diseñado para los países con mercados de telecomunicaciones abiertos y en régimen de competencia,
- Los acuerdos **serán dictados por el mercado, oferta y demanda,**
- Con respecto al tráfico terminado en una tercera administración (fuera de las dos que tienen uno de estos acuerdos), los procedimientos no deberán afectar la compensación de esa administración de terminación, sin su previo acuerdo.

Ejemplo: Existe total libertad de las empresas de negociar los valores que se cobrarán por cursar tráfico telefónico internacional, se podría mencionar como ejemplo de estos acuerdos el roaming internacional ofertado por Bellsouth.

RESUMEN DE LA AYUDA DE MEMORIA

Existen cuatro procedimientos para que dos operadores internacionales puedan intercambiar su tráfico telefónico, estos son:

Tasa de Distribución: Tasa fijada por las Administraciones para el establecimiento de las cuentas internacionales, se negocia por cada minuto de comunicación entre operadores de larga distancia internacional, por cursar, originar y terminar llamadas entre dos países, el de mayor tráfico originado debe transferir el monto correspondiente a la mitad de la tasa de distribución -denominada tasa de liquidación- por los minutos excedentes al país receptor del mismo

Tasa de Terminación: Permite a los gobiernos u operadores establecer una tasa única para terminar el tráfico en su país, siempre que la tasa satisfaga ciertos criterios acordados multilateralmente.

Tasa de Liquidación: Permite que los operadores negocien tasas de liquidación orientadas a los costos y asimétricas, que podrían adaptarse mejor a la nueva situación del mercado.

Acuerdos Comerciales Bilaterales: Permite llegar a cualquier acuerdo comercial bilateral dictado por el mercado, la oferta y la demanda.

BIBLIOGRAFÍA:

- Recomendación UIT-T D.000 (06/2002).
- Recomendación UIT-T D.140 (07/98).
- Recomendación UIT-T D.150 (06/99).
- Reforma del sistema internacional de tasas de distribución – 1999, Unión Internacional de Telecomunicaciones, Primera edición , junio de 2000.
- Tendencias en las Reformas de Telecomunicaciones 2000 – 2001, UIT, Reglamentación de la interconexión, Tercera edición, 2001.

Consideraciones para el desarrollo del capítulo 3:

- Los valores por concepto de tasa de terminación son confidenciales, debido a que son negociados por las operadoras telefónicas de manera independiente y son utilizados para estrategia de mercado, razón por la cual para el desarrollo del capítulo 3 se ha tomado un valor de referencia.

- El tráfico telefónico internacional entrante al Ecuador, ingresa tanto a operadoras telefónicas fijas y móviles, lo que implica que al considerar un solo valor por concepto de tasa de terminación se tendrá una estimación de pérdidas económicas debido al fraude.

- En el documento INTERCONEXIÓN INTERNACIONAL, se indica que la operadora telefónica ANDINATEL recibía el valor de 11,8 cent/min por concepto de tasa de terminación, valor vigente en el año 2003.

  El valor de 11,8 cent/min ha sido tomado como referencia para el desarrollo del capítulo 3.

ANEXO

H

Operadoras que poseen concesión de servicio de telecomunicaciones y están autorizadas a cursar tráfico telefónico internacional

(Documento proporcionado por la SENATEL)

SENATEL
Secretaría Nacional de Telecomunicaciones

Oficio No. **DGGST-2006-** 0664

Quito, [illegible] 2006

Señor
Christian Gallardo
INSTRUCTOR DEL LABORATORIO DE FÍSICA
ESCUELA POLITÉCNICA NACIONAL
Ciudad.-

ASUNTO: Operadores de Telefonía Larga Distancia Internacional

De mi consideración:

En atención al oficio s/n ingresado a esta Secretaría con trámite No. 1667 de 18 de abril del 2006, mediante el cual consulta cuales son las operadoras telefónicas fijas y móviles que se encuentran autorizadas para cursar tráfico telefónico internacional, al respecto sírvase encontrar el listado de operadores que poseen concesión de servicios de telecomunicaciones y están autorizadas a cursar tráfico telefónico internacional:

OPERADORES TELEFONÍA FIJA

ANDINATEL S.A.
PACIFICTEL S.A.
ETAPA
SETEL S.A. (A sus propios abonados)
ECUADORTELECOM S.A. (A sus propios abonados)
ETAPATELECOM S.A. (A sus propios abonados)
LINKOTEL S.A. (A sus propios abonados)

OPERADORES TELEFONÍA MÓVIL

CONECEL S.A. (A sus propios abonados)
OTECEL S.A. (A sus propios abonados)
TELECSA S.A. (A sus propios abonados)

Atentamente,

Ing. José Jiménez Andrade
DIRECTOR GENERAL DE GESTIÓN DE
LOS SERVICIOS DE TELECOMUNICACIONES

1/1

ANEXO

I

Ejercicios prácticos referentes a fraudes en telecomunicaciones

EJERCICIOS PRÁCTICOS[1]
REFERENTES A FRAUDES EN TELECOMUNICACIONES

1 FML SECURING BUSINESS, Ejercicios prácticos y respuestas sugeridas: Detección, control y gestión del fraude en telecomunicaciones, FML Americas Inc. 2002

Ejercicios Prácticos - Información Referencial

Las informaciones siguientes pueden ser usadas como complemento en los ejercicios prácticos.

Códigos para llamadas

Destino	Código
Australia	61
Francia	33
Alemania	49
Ghana	233
Holanda	31
Nigeria	234
Pakistán	92
Arabia Saudita	966
Somalia	252
África del Sur	27
Suiza	46
EEUU (Boston)	1617
EEUU (New Orleans)	1504
EEUU (Nueva York)	1212
Código de llamada Internacional	00
Celular Móvil	07xxx
Llamada Gratuita	0800
Llamada Gratuita	0500
Llamada Local	0345
Servicio Premium (PRS)	09xx

Equivalencias de Tiempo

Segundos	Tiempo (Hrs:Mins)
120	0:02
900	0:15
1800	0:30
3600	1:00
7200	2:00
14400	4:00
28800	8:00
43200	12:00
86400	24:00
172800	48:00
604800	7 días

Tipo deTarifa		Costo por minuto
0	Tarifa Cero	0.00
1	Tarifa Local	0.03
2	Tarifa Nacional	0.06
3	Móvil	0.25
4	Tarifa Servicio Premium PRS	0.45
5	Internacional	1.00

Información Adicional

Todas las informaciones mostradas están impresas y distribuidas.
Todos los costos son en Dólares Fraudianos ($).
Todos los números son inventados - Cualquier semejanza con número o llamada real es pura coincidencia, y no deben ser consideradas como fraudulentas para análisis reales.

01 500xxx = Línea gubernamental de meteorología.

Ejercicio Individual 1

El objetivo de este ejercicio es identificar tipos de llamadas y asociarlos a potenciales riesgos de fraude. Los siguientes datos fueron extraídos de una única central telefónica en un determinado período de tiempo. Suponga que todas los Identificadores de Llamadas (CLI's) están correctamente encaminados a través de esta central.
Para cada llamada, haga un registro y diga si considera el evento de riesgo alto, medio o bajo, en términos de posibilidad de fraude. Trabaje solo e intente terminar el trabajo en más o menos 10 minutos.

CLI	*Número Llamado*	*Fecha*	*Tipo de Tarifa*	*Tiempo*	*Duración (s)*	*Costo*	*Riesgo (A/M/B)*
01604398881	0012129347865	16.06.2000	5	09.07	327	$5.45	
0160419888	0092398349	16.06.2000	5	09.21	8659	$144.32	
0115854786	267593	16.06.2000	1	09.23	642	$0.32	
01716499031	0900123986	16.06.2000	4	09.37	3594	$26.96	
01716499031	0900123985	16.06.2000	4	10.38	9128	$68.46	
01816492100	0345500200	16.06.2000	4	10.49	1764	$13.23	
01908139476	0115267593	16.06.2000	2	10.58	89	$0.09	
0115267593	0150939726	16.06.2000	2	11.10	96	$0.10	
01908176576	00466604389752	16.06.2000	5	11.17	549	$9.15	
01716491234	0012124924390	16.06.2000	5	11.24	1156	$19.27	
0160419888	0092459358	16.06.2000	5	11.39	1347	$22.45	
0127473784	017144876	16.06.2000	2	11.52	210	$0.21	
01211976041	0900234000	16.06.2000	4	12.16	1057	$7.93	
0150939726	0113590026	16.06.2000	2	12.24	642	$0.64	
016047842816	154897	16.06.2000	1	12.37	34	$0.02	
01211976039	0900234000	16.06.2000	4	12.39	1296	$9.72	
0160419888	0092347863	16.06.2000	5	12.42	89	$1.48	
01274728875	73784	16.06.2000	1	12.53	1203	$0.60	
01211976041	378492	16.06.2000	1	12.59	641	$0.32	
0115842196	0500365888	16.06.2000	0	13.10	321	$0.00	

CLI	*Número Llamado*	*Fecha*	*Tipo de Tarifa*	*Tiempo*	*Duración (s)*	*Costo*	*Riesgo (A/M/B)*
01211976048	0900234000	16.06.2000	4	13.12	983	$7.37	
01716499031	0900123985	16.06.2000	4	13.17	1047	$7.85	

Ejercicio de Grupo 2

El objetivo de este ejercicio es identificar qué tipo de fraude existe (si es que lo hay). Esto debe ser hecho mediante el análisis de los registros de facturación de cada cliente para los dias y períodos de tiempo mostrados. Trabajando grupalmente, procure terminar el ejercicio en 15 minutos, anotando el tipo de fraude usando las 4 M's: Motivo, Medio, Modo y Método (y la extensión del método en lo posible).

Cliente 1 - Empresa de tamaño Mediano, línea fija

CLI	Número llamado	Fecha	Tipo de Tarifa	Tiempo	Duración (s)	Costo
01908176576	0161142234	15.06.2000	2	13.27	1089	$1.09
01908176576	0171175348	15.06.2000	2	15.59	620	$0.62
01908176576	01136479821	15.06.2000	2	16.48	931	$0.93
01908176576	0161142234	15.06.2000	2	17.27	35	$0.04
01908176576	009212573487	15.06.2000	5	23.59	9235	$153.92
01908176576	009218410830	16.06.2000	5	02.37	11349	$189.15
01908176576	0171175348	16.06.2000	2	08.34	72	$0.07
01908176576	3846795	16.06.2000	1	09.15	146	$0.07
01908176576	0161142234	16.06.2000	2	09.37	2937	$2.94
01908176576	0121189543	16.06.2000	2	10.15	27	$0.03

Cliente 2 - Residencial, línea fija

CLI	Número llamado	Fecha	Tipo de Tarifa	Tiempo	Duración (s)	Costo
01716499031	0900123985	15.06.2000	4	18.24	298	$2.24
01716499031	0900123985	15.06.2000	4	18.30	303	$2.27
01716499031	0900123985	15.06.2000	4	18.36	300	$2.25
01716499031	0900123985	15.06.2000	4	18.41	301	$2.26
01716499031	0900123985	15.06.2000	4	18.46	297	$2.23
01716499031	0900123985	15.06.2000	4	18.52	299	$2.24
01716499031	0900123985	15.06.2000	4	18.59	302	$2.27
01716499031	0900123985	15.06.2000	4	19.04	299	$2.24
01716499031	0900123985	15.06.2000	4	19.10	300	$2.25
01716499031	0900123985	15.06.2000	4	19.17	304	$2.28

Cliente 3 - Empresa pequeña, teléfono móvil

CLI	Número llamado	Fecha	Tipo de Tarifa	Tiempo	Duración (s)	Costo
07802508647	002343894576925	15.06.2000	5	14.27	1579	$26.32
07802508647	987423	15.06.2000	1	14.29	1486	$0.74
07802508647	002347485701769	15.06.2000	5	15.38	2874	$47.90
07802508647	6952341	15.06.2000	1	15.42	865	$0.43
07802508647	012741956834	15.06.2000	2	15.57	1379	$1.38
07802508647	01908297330	15.06.2000	2	16.20	628	$0.63
07802508647	002346124088430	15.06.2000	5	17.42	1664	$27.73

Ejercicio Practico : Recarga de Créditos en PrePago via Internet

Informaciones Previas

Ud. es parte del departamento de fraude de una operadora de telefonia móvil, siendo una de sus funciones principales incrementar la seguridad a los nuevos productos desarrollados por la empresa. La misma que ofrece servicios post pago y prepago, siendo que 80% de total de clientes y 40 % del tráfico es prepago y el restante post pago. Devido a las altas tasas de fraude de subscrición, usted está muy interesado en el incremento del servicio prepago para los nuevos clientes que no sean corporativos

El problema

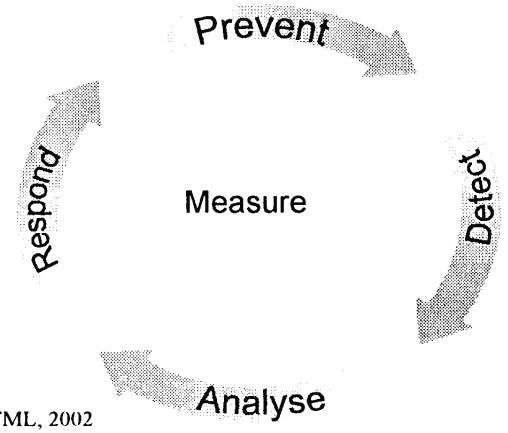
Actualmente sus clientes prepago hacen la recarga de crédito usando la tarjeta de prepago convencional. Para hacer el serviço prepago mas atractivo para los usuários, el Gerente de Produtos quiere que sea considerado un nuevo servicio que permita a los clientes hacer la recarga de créditos diretamente por internet usando su tarjeta de crédito

Como el servicio prepago ya está experimentando un nível de fraude, el Gerente de Produtos tiene recelo del uso de Internet, por eso solicito que usted especifique los requisitos para un servicio seguro de recargas de créditos via internet y/o recomendar otro tipo de recarga.

El trabajo

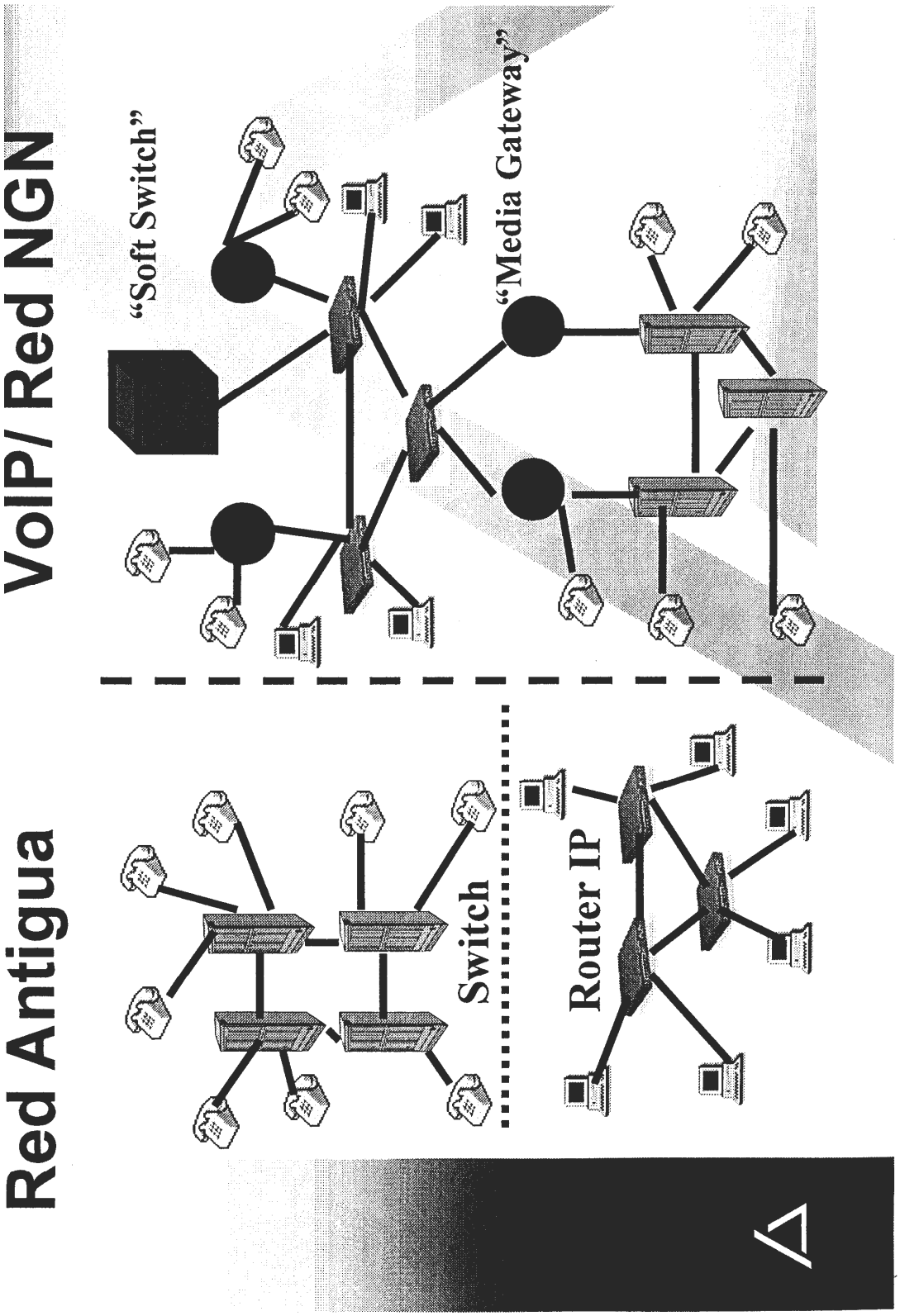
1. Hacer un análisis preliminar de como Usted enfrentaria este desafio.
2. Determinar las características del nuevo produto
3. Desarrollar una evaluación de riesgo de seguridad del produto
4. Identificar los riesgos
5. Determinar las mediciones de seguridad que incluyan todos los ciclos de Business Value Assurance™ (mostrado abajo)
6. Elaborar la recomendación final para el Gerente de Produtos. Lanzar o no el produto?

Durante el ejercicio, anote cualquer suposición que Usted considere. Recuerde que Usted tiene acceso directo al Gerente de Produtos, pudiendo obtener respuestas para preguntas con relativa facilidad.



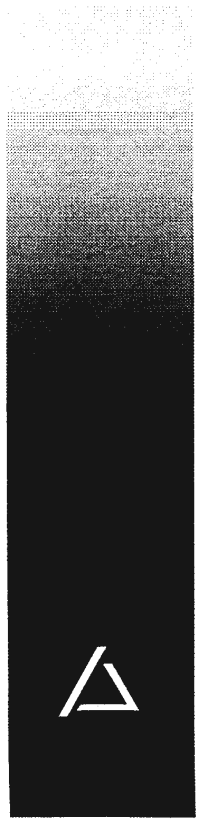
Ejercicio Práctico

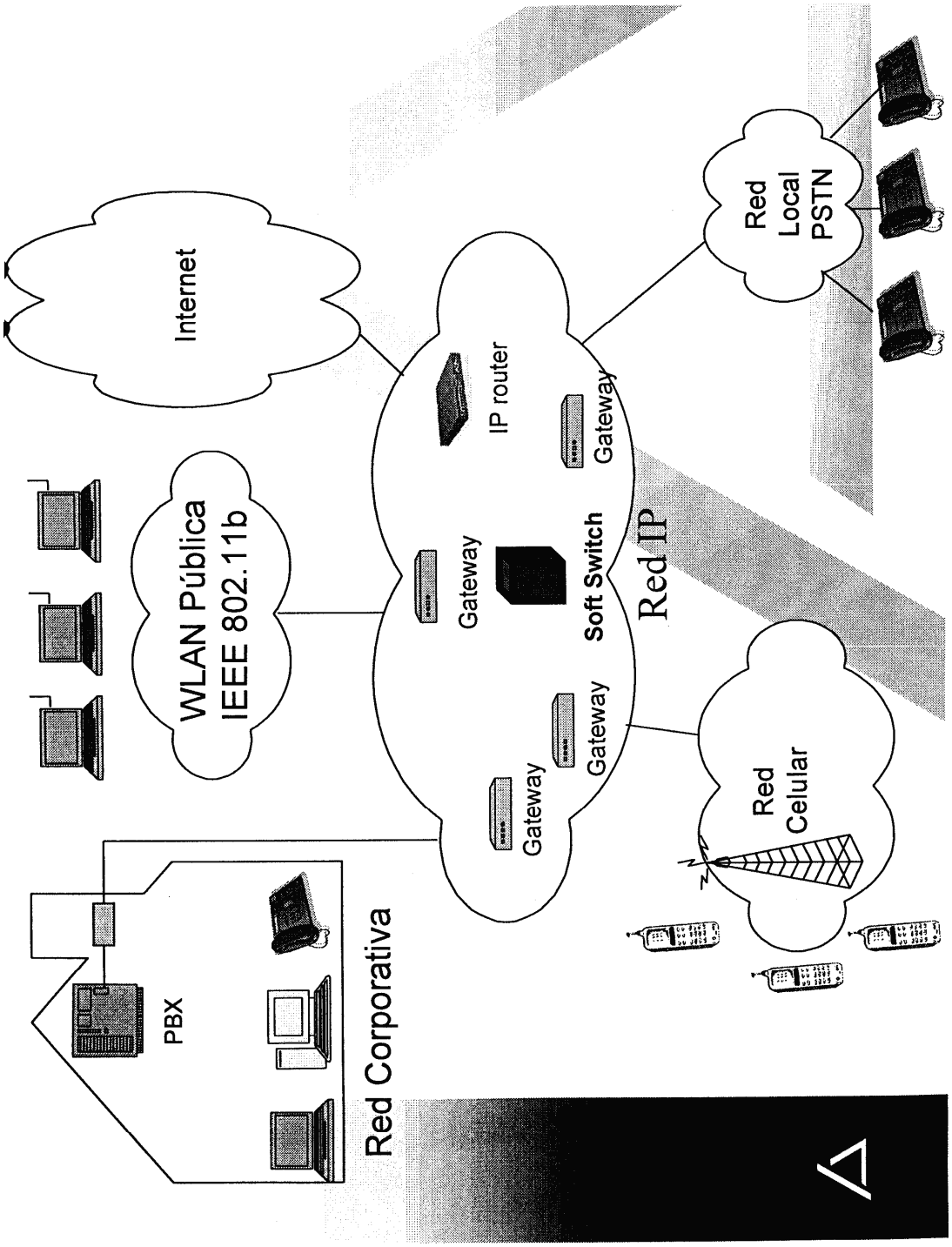
Redes VoIP & Next Generation Networks (NGN)


Red Antigua
VoIP/ Red NGN
"Soft Switch"
"Media Gateway"
Switch
Router IP

Ejercicio

- Para el ejemplo siguiente :
  - Identificar las vulnerabilidades
  - Sugerir soluciones




Internet
WLAN Pública
IEEE 802.11b
IP router
Gateway
Gateway
Soft Switch
Gateway
Gateway
Red IP
Red
Local
PSTN
Red
Celular
PBX
Red Corporativa

RESPUESTAS SUGERIDAS
EJERCICIOS PRÁCTICOS[2]

2 FML SECURING BUSINESS, Ejercicios prácticos y respuestas sugeridas: Detección, control y gestión del fraude en telecomunicaciones, FML Americas Inc. 2002

Ejercicio 1 (individual) – Respuestas sugeridas

CLI	*Número llamado*	*Fecha*	*Tipo de Tarifa*	*Hora*	*Duración (hh:mm:ss)*	*Costo*	*Evaluación de Riesgo (A/M/B)*
01604398881	0012129347865	16.06.2000	5	09.07	00:05:45	$5.45	B
0160419888	0092398349	16.06.2000	5	09.21	02:40:00	$144.32	A
0115854786	267593	16.06.2000	1	09.23	00:10:07	$0.32	B
01716499031	0900123986	16.06.2000	4	09.37	00:59:00	$26.96	A
01716499031	0900123985	16.06.2000	4	10.38	02:53:00	$68.46	A
01816492100	0345500200	16.06.2000	4	10.49	00:29:40	$13.23	M/A*
01908139476	0115267593	16.06.2000	2	10.58	00:01:48	$0.09	B
0115267593	0150939726	16.06.2000	2	11.10	00:01:36	$0.10	B
01908176576	00466604389752	16.06.2000	5	11.17	00:09:15	$9.15	B
01716491234	0012124924390	16.06.2000	5	11.24	00:19:26	$19.27	B/M
0160419888	0092459358	16.06.2000	5	11.39	00:22:45	$22.45	A
0127473784	017144876	16.06.2000	2	11.52	00:03:50	$0.21	B
01211976041	0900234000	16.06.2000	4	12.16	00:17:00	$7.93	B
0150939726	0113590026	16.06.2000	2	12.24	00:10:42	$0.64	B
016047842816	154897	16.06.2000	1	12.37	00:00:34	$0.02	B
01211976039	0900234000	16.06.2000	4	12.39	00:21:06	$9.72	M
0160419888	0092347863	16.06.2000	5	12.42	00:01:48	$1.48	A
01274728875	73784	16.06.2000	1	12.53	00:20:05	$0.60	B
01211976041	378492	16.06.2000	1	12.59	00:10:07	$0.32	B
0115842196	0500365888	16.06.2000	0	13.10	00:05:35	$0.00	B
01211976048	0900234000	16.06.2000	4	13.12	00:16:38	$7.37	A
01716499031	0900123985	16.06.2000	4	13.17	00:17:45	$7.85	A

* Parece haber un error de tarifa que puede ser accidental o deliberado. Requiere más investigación.

Ejercicio 1 – Observaciones

- Es necesario el uso de una herramienta referencial para interpretar la información y los datos:
  - Numeración Telefónica (prefijo/área)
  - Codificación de números internacionales
  - Planes tarifarios

- No toda llamada de larga duración significa fraude, sin embargo, continúan siendo un buen indicativo

- Fraudes de ingresos son más fáciles de ser identificados a partir de situaciones particulares de flujos de llamadas.

- Existen dos categorías de destinos de alto riesgo:
  - Aquellas que generalmente forman los elementos del riesgo principal (destinos fraudulentos conocidos).
  - Aquellas que varían de tiempo en tiempo, dependiendo de varios factores (frecuencia, volumen, valor, relación con otras cuentas, etc.).

- Elementos únicos de llamadas no son, en sí, un indicador de riesgo eficiente.

- Llamadas de riesgo que aparecen en varias cuentas aumentan su peso de riesgo a medida que se repiten (ocurrencias en varias cuentas pueden indicar fraude de surfing).

- Diferencias en tarifas puede resultar pérdida de ingresos.

Ejercicio 2 (en grupos) – Respuestas sugeridas

Cliente 1

CLI	Número llamado	Fecha	Tipo de Tarifa	Hora	Duración (hh:mm:ss)	Costo
01908176576	0161142234	15.06.2000	2	13.27	00:18:15	$1.09
01908176576	0171175348	15.06.2000	2	15.59	00:10:33	$0.62
01908176576	01136479821	15.06.2000	2	16.48	00:15:51	$0.93
01908176576	0161142234	15.06.2000	2	17.27	00:00:35	$0.04
01908176576	009212573487	15.06.2000	5	23.59	02:56:00	$153.92
01908176576	009218410830	16.06.2000	5	02.37	03:16:00	$189.15
01908176576	0171175348	16.06.2000	2	08.34	00:01:20	$0.07
01908176576	3846795	16.06.2000	1	09.15	00:02:43	$0.07
01908176576	0161142234	16.06.2000	2	09.37	00:48:09	$2.94
01908176576	0121189543	16.06.2000	2	10.15	00:00:27	$0.03

Este cliente ciertamente tiene un problema con las horas de uso fuera de horario normal. Esto puede suceder debido a los siguientes factores:

- Alguien está teniendo acceso al escritorio, ya sea por razones legítimas o ilegítimas.
- "Staple"
- Fraude de PBX

Las llamadas también son destinadas a lugares de alto riesgo (Pakistán), y con una duración lo suficientemente larga como para levantar sospechas.
Motivo = Hacer dinero, Medios = Venta de llamadas, Modo = Surfing, Método = se necesita más investigación.

Cliente 2

CLI	Número llamado	Fecha	Tipo de Tarifa	Hora	Duración (hh:mm:ss)	Costo
01716499031	0900123985	16.06.2000	4	18.24	00:04:58	$2.24
01716499031	0900123985	16.06.2000	4	18.30	00:05:03	$2.27
01716499031	0900123985	16.06.2000	4	18.36	00:05:00	$2.25
01716499031	0900123985	16.06.2000	4	18.41	00:05:01	$2.26
01716499031	0900123985	16.06.2000	4	18.46	00:04:57	$2.23
01716499031	0900123985	16.06.2000	4	18.52	00:04:59	$2.24
01716499031	0900123985	16.06.2000	4	18.59	00:05:02	$2.27
01716499031	0900123985	16.06.2000	4	19.04	00:04:59	$2.24
01716499031	0900123985	16.06.2000	4	19.10	00:05:00	$2.25
01716499031	0900123985	16.06.2000	4	19.17	00:05:04	$2.28

El patrón normal de llamadas en esta cuenta indica que se puede estar utilizando un aparato de auto-discado. Estos aparatos pueden ser utilizados con mayor eficiencia en los casos de fraude relacionados, por ejemplo, con servicios de tarifas altas. Ellos pueden tener varias formas, desde aparatos caseros simples, también conocidos como 'smart-sockets' hasta programas más sofisticados basados en micro computadores personales. Algunos equipos de auto-discado pueden ser programados para que varíen el número de destino (normalmente dentro del mismo rango numérico) o la duración de la llamada. Esto produce una variación en las cuentas con la finalidad de confundir a las personas y a los sistemas que están rastreando los patrones regulares.

Motivo = Hacer dinero, Medios = Servicios de Tarifas Altas, Modo = Suscripción, Método = Dispositivo fraudulento (con auto-discado).

Cliente 3

CLI	Número llamado	Fecha	Tipo de Tarifa	Hora	Duración (hh:mm:ss)	Costo
07802508647	002343894576925	16.06.2000	5	14.27	00:26:31	$26.32
07802508647	987423	16.06.2000	1	14.29	00:24:46	$0.74
07802508647	002347485701769	16.06.2000	5	15.38	00:47:54	$47.90
07802508647	6952341	16.06.2000	1	15.42	00:14:41	$0.43
07802508647	012741956834	16.06.2000	2	15.57	00:22:59	$1.38
07802508647	01908297330	16.06.2000	2	16.20	00:10:46	$0.63
07802508647	002346124088430	16.06.2000	5	17.41	00:27:44	$27.73
07802508647	853241	16.06.2000	1	17.42	00:15:42	$0.47
07802508647	01908276347	16.06.2000	2	17.57	00:12:02	$0.72

Este ejemplo de llamadas traslapadas demuestra el uso de servicios de red, tales como llamadas tripartitas (o de tres vías) o transferencia de llamadas, haciendo el papel de una 'telefonista' en una operación de Venta de Llamadas ("Call Selling"). Combinado con los destinos de alto riesgo (Nigeria), las probabilidades de que esta cuenta sea fraudulenta son altas. Operadores de Venda de Llamadas normalmente conectan una cantidad de 'clientes' durante una única llamada internacional. Aparecerán una variedad de números discados en la cuenta.

Normalmente se verá este tipo de patrón de llamadas en una cuenta corporativa a cuya PBX se le está cometiendo un fraude de "surfing". Muchas PBX's permiten funciones similares, y una vez activadas, pueden ser utilizadas como un teléfono normal.

Motivo = Hacer dinero, Medios = Venta de Llamadas, Modo = Suscripción, Método = Uso fraudulento de una opción (llamada tripartita).

Ejercicio 2 (en grupos) – Observaciones

- Es importante conocer la base de clientes
- Conocer sus productos y servicios, y cómo pueden ser utilizados por defraudadores
- Las características de fraude siguen siendo comunes en diferentes productos, servicios o tipos de clientes
- Un volumen mayor de información de llamadas permite un análisis más completo de las tendencias del fraude resultando en una clasificación y medición más precisas
- Los fraudes de ingresos tienden a ser más fáciles de ser identificados a partir de registros de llamadas o solamente por la información obtenida de facturación.
- Un análisis más profundo de las cuentas sería necesario efectuar en la mayor parte de los casos, principalmente cuando están relacionados a fraudes sin ingresos.

Respuestas Sugeridas al Ejercicio : Recarga de Créditos en Prepago via Internet

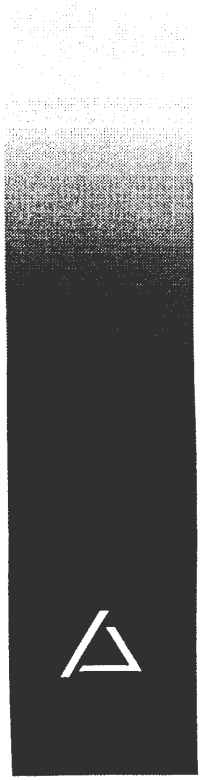
1. Hacer un análisis préliminar de como Usted enfrentaria esta nueva iniciativa
   - RIESGO MUY ALTO
     - Tarjeta de crédito = Móvil = Fácil de Fraudar
     - Internet = Anonimato = Fácil de Fraudar
     - Prepago = Móvel + Anonimato = Fácil de Fraudar
   - Será necesário una política de gestion de fraude y seguridad bien especifica y detallada
     - Exigir Relatórios semanales o desarrollar herramienta de analisis con base informaciones de las recargas
     - Prevención : Usar limites para cada tarjeta y telefono por costo y tiempo
     - Detección : Analisis de Charge Back y relatórios
2. Determinar las características del producto
   - Permitido el uso de las recargas via Internet
     - Site própio desarrollado por TI con los requisitos de seguridad previstos
   - Permitido las Recargas via Call center
     - Atendimiento 24x7 com política y control interno
   - Límite de $ X por recarga en un determinado intervalo de tempo Z dias
     - Límite por número de telefono
     - Límite por número de tarjeta de crédito
3. Desarrollar una evaluación de riesgo de seguridad del produto
   - Produto con alto riesgo sin una adecuada política de prevención y detección
   - Impacto en el negocio
     - perdidas financeiras
     - imagen
     - trafico de red
   - Impacto en los clientes
   - Impacto en los clientes de las administradoras de tarjetas
   - Impacto a los socios de negócios
4. Identificar los riesgos
   - Almazenamiento del número de las tarjetas de crédito
   - Abuso de autoridad en la Central de Atendimento

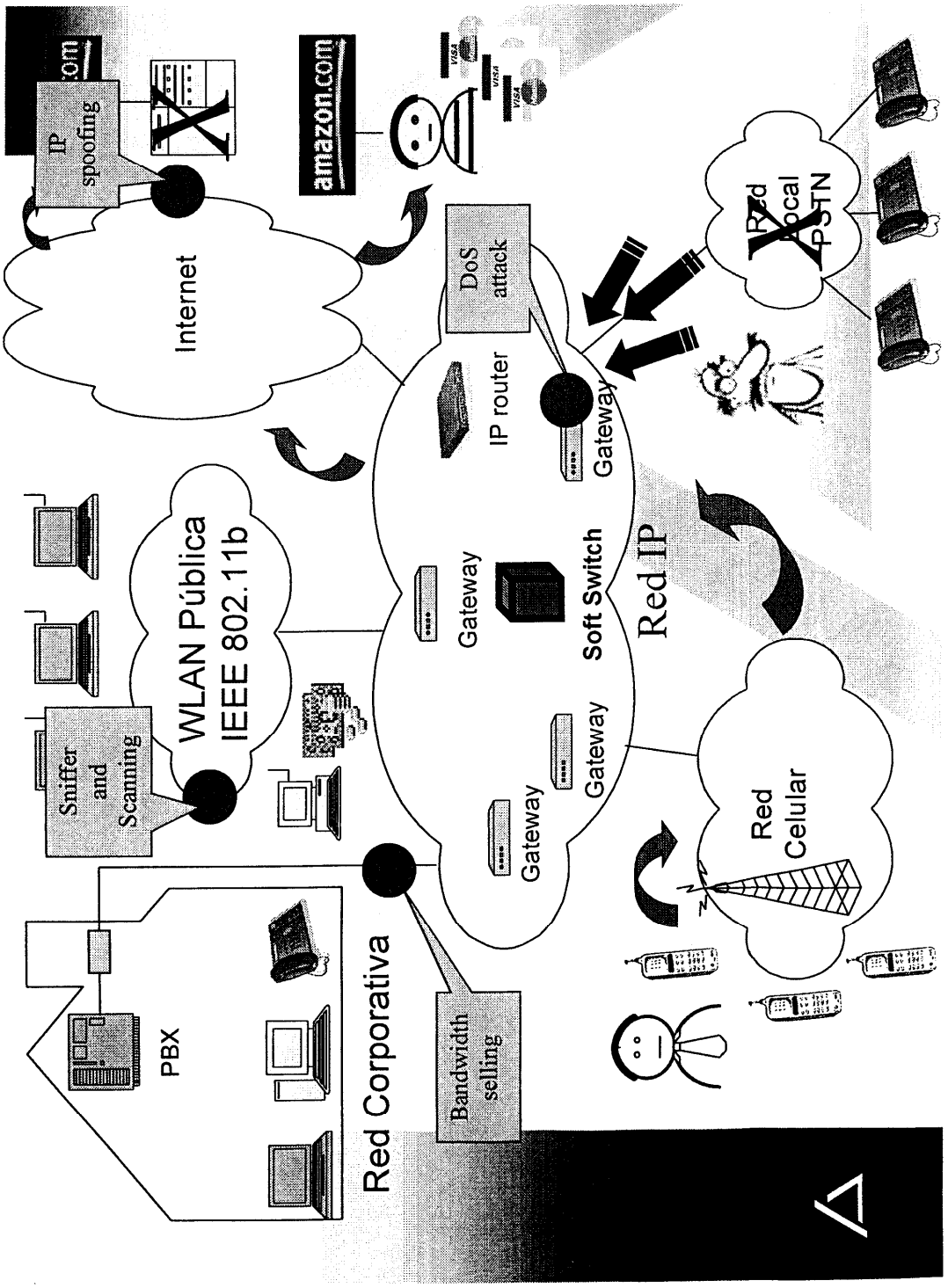
- Hacking Site

5. Determinar las mediciones de seguridad que incluya todos los ciclos del Business Value Assurance™ cycle
   - Reporte Volumen de recargas por semana : Internet y Call Center
   - Reporte do Revenue semanal
   - Reporte de recargas por región
   - Numero de charge back por semana
   - Perdidas por fraude a cada semana
   - Analisar las informaciones y reportes
   - Identificar la región con mayor índice de fraude
   - Identificar los numero telefonos donde fueron hechas las recargas fraudulentas
   - Entrar en contacto con los clientes dueños de estos telefonos
   - Tomar las aciones : suspender el serivicio parcial y corte
   - Trabajar junto a administradora de tarjeta
6. Elaborar recomendacion final para el Gerente de Produto. Lanzar o no el producto
   - Lanzar el producto
   - No autorizar recargas sin límite de credito por tarjeta y telefono
   - Usar Call center e Internet para las recargas
   - Facilitar el desarrollo de reportes

Respuestas Sugeridas
Ejercicio Práctico

Redes VoIP & Next Generation Networks (NGN)




IP spoofing
Internet
amazon.com
DoS attack
IP router
Gateway
Red IP
Soft Switch
Gateway
Gateway
Gateway
Red Local PSTN
WLAN Pública IEEE 802.11b
Sniffer and Scanning
Red Celular
PBX
Red Corporativa
Bandwidth selling

Vulnerabilidades en VoIP / NGN

- Todas las vulnerabilidades asociadas a una red **IP + Telecom**
  - **Surfing**
    - Ataque DoS ("Denied of Service")
    - "Spoofing" a direcciones IP
    - Programas "Sniffers"
    - "Scanning"
    - Virus
  - **Ghosting**
    - Hacking Interno
  - **Identidad Falsa**
    - Venta de ancho de banda o "bandwith selling"

Algunas soluciones en NGN/IP

- "Firewalls"
  - Intermediación PROXY
  - Filtraje
  - Análisis de contenido
  - Monitoreo
- Control de acceso
- Auditoria de archivos "logs"
- Criptografía avanzada
  - Firma digital
  - Certificación digital

ANEXO

J

EQUIPOS

Características técnicas

Cisco 1600 Series Routers and WAN Interface Cards

Flexible, Secure Data Access for Small Businesses and Small Branch Offices

As companies realize the benefits of the Internet, intranets, and extranets, they require access solutions that can accommodate growth and change. The Cisco 1600 series routers deliver the flexibility, security, and functionality that small offices demand today and as networks evolve.

The Cisco 1600 series has become the proven choice for data access for small branch offices and small businesses because they offer a range of features specifically designed for such applications:

- Modular design for wide-area network (WAN) choice and flexibility
- Advanced security, including optional integrated firewall, encryption, and virtual private network (VPN) software
- End-to-end quality of service (QoS) and multimedia support
- Integrated data service unit/channel service unit (DSU/CSU) with up to T1 speed and integrated Network Termination (NT1)
- Low cost of ownership through WAN bandwidth optimization
- Ease of use, deployment, and management

The Cisco 1700 modular access router series builds upon the success of the Cisco 1600 series routers, delivering greater flexibility and investment protection. The Cisco 1700 series routers are fully modular enabling customers to tailor an access solution to serve their needs today and cost effectively add new services including voice/data integration, VPNs, and broadband connections when needed.

Cisco 1600 Series Router

Cisco 1600 Series Modular Routers

Cisco 1600 series routers connect small offices with Ethernet LANs to WANs through Integrated Services Digital Network (ISDN), asynchronous serial, and synchronous serial connections. The five basic configurations of the Cisco 1600 product family offer the following connections:

- Cisco 1601 R—one Ethernet, one serial, one WAN interface card slot
- Cisco 1602 R—one Ethernet, one serial with integrated 56-kbps DSU/CSU, one WAN interface card slot
- Cisco 1603 R—one Ethernet, one ISDN Basic Rate Interface (BRI) (S/T interface), one WAN interface card slot

- Cisco 1604 R—one Ethernet, one ISDN BRI with integrated NT1 (U interface), one S-bus port for ISDN phones, one WAN interface card slot
- Cisco 1605 R—two Ethernet ports, one WAN interface card slot

The serial WAN port on the Cisco 1601 R router supports asynchronous serial connections of up to 115.2 kbps and synchronous serial connections—such as Frame Relay, leased lines, Switched 56, Switched Multimegabit Data Service (SMDS), and X.25—of up to 2.048 Mbps. The Cisco 1602 R router integrates a 56-kbps four-wire DSU/CSU, and it supports the same synchronous serial connections as the Cisco 1601 R router (except SMDS). The ISDN BRI port on the Cisco 1603 R router has an S/T interface, while the Cisco 1604 R includes an integrated NT1 with a U interface. The Cisco 1605 R router provides a 10BaseT and an AUI port on the first Ethernet interface and a 10BaseT port on the second Ethernet interface.

Modularity for Flexibility and Investment Protection

The WAN interface card slot allows customers to change or add WAN interfaces as their requirements grow or change. With this feature, the Cisco 1600 series offers more flexibility and investment protection than any other product in its class. What's more, the ability to use the same WAN interface cards in Cisco 1600, 1700, 2600, and 3600 routers reduces requirements for spare parts inventory and protects investments in existing routers.

All Cisco 1600 models support the following WAN interface cards:
- One-port serial (asynchronous and synchronous)
- One-port T1/Fractional T1 DSU/CSU
- One-port 56/64-kbps four-wire DSU/CSU

The Cisco 1601 R, Cisco 1602 R and Cisco 1605 R also accept the one-port ISDN BRI cards for dial or leased line with either S/T or U (NT1) interfaces.

Device Integration

Cisco 1600 routers deliver a complete solution for remote access for small businesses and small branch offices. They provide not only advanced routing capabilities but also the option to integrate DSU/CSU and ISDN network termination 1 device (NT1), as well as firewall, encryption, and VPN functionality. This integration reduces deployment time and expense because fewer devices and cables need to be installed and configured. An integrated product also saves space and increases reliability because fewer stand alone devices are required to build the solution. The Cisco 1600 routers simplify ongoing support of small branch offices from a central site through remote configuration, monitoring, and troubleshooting of all integrated functions in the router.

Advanced Security

To leverage the unprecedented opportunities offered by communications and commerce over the Internet, private information must remain secure. Cisco IOS security services provide many technologies to build a custom security solution. The elements of security services include perimeter security, firewalls, encryption, and VPNs.

Perimeter Security—Perimeter security refers to the control of traffic entry and exit between network boundaries, such as between private networks, intranets, extranets, or the Internet. Cisco IOS perimeter security technologies provide a highly flexible, superior solution with features such as:
- Standard and extended access control lists (ACLs)
- Lock and Key (dynamic ACLs)
- Router/route authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS)

Firewall—The optional Cisco IOS Firewall Feature Set, available on all Cisco 1600 models, provides formidable firewall functionality, including:
- Context-based access control (CBAC)
- Java blocking
- Attack detection and prevention
- Improved logging and alerts

CBAC provides stateful application-layer security by examining traffic sessions on a per-application basis and allowing return traffic through the firewall. When a session is initiated internally, CBAC writes a temporary, session-specific ACL entry and deletes the ACL entry upon session termination.

The Cisco 1605 R router—which supports one WAN slot, two Ethernet ports, and the Cisco IOS Firewall Feature Set—makes an ideal integrated and flexible firewall for small offices. This integrated router/firewall effectively segments an internal, secure LAN from a perimeter LAN with Web servers exposed to an untrusted network (such as the Internet), thus creating a "demilitarized zone."

See the Cisco IOS Firewall Feature Set data sheet for further details.

Virtual Private Networks (VPNs) and Encryption—The Cisco 1600 series routers may be deployed as an entry-level VPN access solution, supporting DES encryption at rates of up to 128 kbps. The Cisco 1700 modular access router is recommended for VPN applications that require greater performance or 3DES or both. Cisco IOS software for the Cisco 1600 series provides a comprehensive set of VPN features, including the following key technologies:

- IPSec tunneling with data encryption standard (DES)
- Layer 2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP)
- VPN management tools such as support for VPN policy configuration in Cisco ConfigMaker

Cisco IOS Software Features for Small Office Internet/Intranet Access

Cisco 1600 series routers offer small businesses and small branch offices a complete set of internetworking software features. In addition to the features mentions earlier, Cisco IOS software differentiates the Cisco 1600 series from the competition with:

- Multiprotocol routing (IP, IPX, AppleTalk), IBM/SNA, and transparent bridging over ISDN, asynchronous serial, and synchronous serial such as leased lines, Frame Relay, SMDS, Switched 56, X.25, and X.25 over D
- Network Address Translation (NAT), which eliminates the need to re-address all hosts with existing private network addresses and hides internal addresses from public view.
- Easy IP—a combination of NAT, Point-to-Point Protocol/Internet Control Protocol (PPP/IPCP) and Dynamic Host Configuration Protocol (DHCP) server—which enables the router to dynamically negotiate its own IP address and dynamically allocate local IP addresses to the remote LAN hosts, simplifies deployment, and minimizes Internet access costs
- End-to-end QoS features that include Resource Reservation Protocol (RSVP), IP Multicast, WFQ, and AppleTalk Simple Multicast Routing Protocol (SMRP), which support multimedia applications such as desktop videoconferencing, distance learning, and voice/data integration
- WAN optimization features such as dial-on-demand routing (DDR), bandwidth-on-demand (BOD), and Open Shortest Path First (OSPF)-on-demand circuit, Snapshot routing, compression, filtering, and spoofing to reduce WAN costs

Ease of Use and Deployment

The Cisco 1600 series includes a variety of easy, user-friendly installation and configuration features such as color coded ports, removable Flash memory PC cards for easy software deployment, the Cisco ConfigMaker configuration tool and the Cisco Fast Step™ software tool. These features combine to give the lowest total cost of ownership of any small office router.

Each Cisco 1600 series router includes the Cisco Fast Step easy-to-use Windows 95, 98, and NT 4.0-based software tool that simplifies the setup, monitoring, and troubleshooting of Cisco routers. The Cisco Fast Step setup application leads users through simple, step-by-step, wizards-based procedures to configure Cisco routers connected to an Internet service provider and remote corporate network. Cisco Fast Step software includes the Cisco Fast Step monitor application, which provides users with router LAN and WAN performance statistics, fault alarms, and troubleshooting assistance.

The Cisco ConfigMaker application is appropriate for advanced configuration of the Cisco 1600 series routers. A Windows 95, 98, 2000, and NT 4.0-based software tool, Cisco ConfigMaker is designed to configure a small network of Cisco routers, switches, hubs, and other network devised from a single PC. Cisco ConfigMaker is designed for resellers and network administrators of small and medium-sized businesses who are proficient in LAN and WAN fundamentals and basic network design. Cisco ConfigMaker includes support for the Cisco IOS Firewall Feature Set (which provides integrated enhanced security capabilities), Network Address Translation (NAT), and Cisco Easy IP software.

In addition to easy-to-use software, the hardware for the Cisco 1600 routers is designed to be "plug-and-play" in four notable areas. First, each of the ports on the Cisco 1600 routers and WAN interface cards is color coded, and optional color-coded cables can be purchased from Cisco. Second, preconfigured software may be loaded into a Flash memory PC card at a central site, and then a user at remote site may deploy the router by simply inserting the Flash card, plugging in cables, and turning on the power. Third, once the router is running, software upgrades and configuration modifications can be downloaded over the WAN from a central site. And finally, the Cisco 1600 series allows for centralized administration and management via Simple Network Management Protocol (SNMP) or Telnet or through the console port.

Part of the Cisco Networked Office

The Cisco 1600 series is part of the Cisco Networked Office (CNO) stack, a suite of flexible and integrated products designed to provide complete networking solutions for small businesses and small branch offices. Other compatible products in the CNO stack include the Cisco 1720 router, Cisco 1528 Micro Hub 10/100, Cisco 1538 Micro Hub 10/100, Cisco 1548 Micro Switch 10/100, Cisco IOS Firewall, and Cisco ConfigMaker software.

Technical Specifications

Cisco 1600 Product Family

	Cisco 1601 R Models	Cisco 1602 R Models	Cisco 1603 R Models	Cisco 1604 R Models	Cisco 1605 R Models
First Fixed Interface (LAN)	Ethernet: 10Base-T (RJ-45) and AUI (DB-15)				
Second Built-In Interface (WAN or LAN)	Serial Sync/ Async: DB-60	56K 4-wire DSU/ CSU: RJ-48S	ISDN BRI S/T: RJ-45	ISDN BRI U with NT1: RJ-45	Ethernet: 10Base-T (RJ-45) Only
WAN Interface Card Slot	All Models				
Optional WAN Interface Cards					
Serial Sync/Async	Yes	Yes	Yes	Yes	Yes
T1/FT1 DSU/CSU	Yes	Yes	Yes	Yes	Yes
56/64K DSU/CSU	Yes	Yes	Yes	Yes	Yes
ISDN BRI S/T	Yes	Yes	—	—	Yes
ISDN BRI U	Yes	Yes	—	—	Yes
ISDN BRI Leased Line S/T	—	—	Yes	Yes	—
Processor	Motorola 68360 at 33 MHz				
Memory Architecture	Run-from-RAM				
DRAM: Default	8 MB				
DRAM: Maximum	24 MB				
Flash Memory: Default	4 MB				
Flash Memory: Maximum	16 MB				
Console Port	RJ-45				

WAN Interface Cards

Product Number	Interfaces	Supported Cisco 1600 Models
WIC-1T	one-port, serial, async, and sync (T1/E1)	All
WIC-1DSU-T1	one-port, T1/fractional T1 DSU/CSU	All
WIC-1DSU-56K4	one-port, 56/64-kbps 4-wire DSU/CSU	All
WIC-1B-S/T	one-port, ISDN BRI S/T (dial and leased line)	Cisco 1601 R, Cisco 1602 R, and Cisco 1605 R
WIC-1B-U	one-port, ISDN BRI U with NT-1 (dial and leased line)	Cisco 1601 R, Cisco 1602 R, and Cisco 1605 R
WIC-1B-S/T-LL	one-port, ISDN BRI S/T (leased line only)	Cisco 1603 R and Cisco 1604 R

The ISDN BRI leased line S/T card (WIC-1B-S/T-LL) is designed specifically for the Cisco 1603 R and 1604 R routers. It is intended for users who require a dialup ISDN BRI line (from the Cisco 1603 R or 1604 R router fixed-WAN port) and an ISDN leased line (from the ISDN BRI leased line card inserted into the Cisco 1603 R or 1604 R router). This card is automatically configured only in ISDN leased line mode. ISDN leased line is also known as ISDN Digital Subscriber Loop (IDSL).

Serial Interfaces Supported by the Cisco 1601 R and 1602 R Routers and Serial WAN Interface Cards

	Cisco 1601 R Onboard WAN	Cisco 1602 R Onboard WAN (four-wire)	WIC-1T Card	WIC-1DSU-56 K4 Card (four-wire)	WIC-IDSU-T1 Card
Asynchronous Serial Connection over Basic Analog Telephone	Up to 115.2 kbps	Not supported	Up to 115.2 kbps	Not supported	Not supported
Synchronous Serial Connections					
Leased Line / Digital Data Service (DDS)	Up to 2.0 Mbps with external DSU/ CSU	56 kbps	Up to 2.0 Mbps with external DSU/CSU	56 or 64 kbps	NX56 or NX64 (N=1 to 24)
Switched 56	56 kbps with external DSU/CSU	56 kbps	56 kbps with external DSU/CSU	56 kbps	Not applicable

- Asynchronous serial protocols: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP)
- Asynchronous interface: EIA/TIA-232
- Synchronous serial WAN services: Frame Relay, X.25, SMDS
- Synchronous serial protocols: PPP, HDLC, LAPB, IBM/SNA
- Synchronous serial interfaces supported on Cisco 1601 R and WIC-1T card: EIA/TIA-232, V.35, X.21, EIA/TIA-449, EIA-530

ISDN Interfaces Supported by the Cisco 1603 R and 1604 R Routers and ISDN WAN Interface Cards

Feature	Cisco 1603 R/ 1604 R Onboard WAN	WIC-1B-S/T Card	WIC-1B-U Card	WIC-1B-S/T-LL Card
ISDN Dialup	Yes	Yes	Yes	Not supported
ISDN Leased Line 64 kbps (IDSL)	Yes	Yes	Yes	Yes*
ISDN Leased Line 128 kbps (IDSL)	Rel 11.3(1)T	Rel 11.3(1)T	Rel 11.3(1)T	Rel 11.3(3)T*
Frame Relay Encapsulation over ISDN Leased Line (IDSL)	Yes	Yes	Yes	Yes
PPP Encapsulation over ISDN Leased Line (IDSL)	Yes	Yes	Yes	Yes
PPP Compression (up to 4:1)	Yes	Yes	Yes	Yes

* 64-kbps ISDN leased-line support on the WIC-1B-S/T-LL card is available on B1 channel only. 128-kbps ISDN leased line support on the WIC-1B-S/T-LL leased line card in Cisco IOS Release 11.3(3)T.

Memory and Software

The Cisco IOS software image is stored in Flash memory (in compressed form), but is loaded into RAM before being executed by the router.

The 1600 series Run-from-RAM models offer the following benefits:

- Greater Performance: The Cisco 1600 R models deliver greater performance for memory-intensive applications such as encryption and compression.
- Easier Upgradability: The Cisco 1600 R routers permit software upgrades over any interface while the router is running.
- Lower Cost: Because the Cisco 1600 R models store the software in compressed form in flash memory, less flash memory is required to run advanced feature sets (such as Cisco 1600 series IOS IP Plus).

The available software feature sets for the Cisco 1600 R models are listed below:

Minimum Memory Requirements and Software Feature Sets for Cisco IOS Release 12.0 and 12.0T

	Cisco 1601 R - 1605 R	
	Flash	DRAM
IP	4 MB	8 MB
IP/IPX	4 MB	8 MB
IP Plus	4 MB	10 MB
IP Plus 40	4 MB	10 MB
IP Plus 56	4 MB	10 MB
IP Plus IPSec 56	4 MB	12 MB
IP/IPX/AppleTalk/IBM	4 MB	12 MB
IP/IPX/AppleTalk/IBM Plus	6 MB	16 MB
IP Firewall	4 MB	8 MB
IP/IPX Firewall Plus	4 MB	10 MB
IP Firewall Plus IPSec	4 MB	12 MB
IP/IPX/AppleTalk/IBM/Firewall Plus IPSec 56	6 MB	16 MB

Starting with Cisco IOS software Release 12.0, the base feature sets include some features formerly in Plus: Network Address Translation (NAT), Open Shortest Path First (OSPF), Remote Access Dial-In User Service (RADIUS), and Next Hop Resolution Protocol (NHRP). Plus feature sets contain all the features in their corresponding base feature sets as well as an additional value-added features such as Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F), Border Gateway Protocol (BGP), IP Multicast, Frame Relay switched virtual circuit (SVC), Resource Reservation Protocol (RSVP), NetWare Link Services Protocol (NLSP), AppleTalk Simple Multicast Routing Protocol (SMRP), and Network Timing Protocol (NTP).

Software Feature Sets Part Numbers, Cisco IOS Release 12.0

Feature Set	Cisco 1601 R–1605 R	CDs for All Models
IP	S16RC-12.0.X	CD16-C-12.0=
IP/IPX	S16RB-12.0.X	CD16-B-12.0=
IP Plus	S16RCP-12.0.X	CD16-CP-12.0=
IP Plus 40	S16RCW-12.0.X	CD16-CW-12.0=
IP Plus 56	S16RCY-12.0.X	CD16-CY-12.0=
IP Plus IPSec 56	S16RCL-12.0.X	CD16-CL-12.0=
IP/IPX/AppleTalk/IBM	S16RQ-12.0.X	CD16-Q-12.0=
IP/IPX/AppleTalk/IBM Plus	S16RQP-12.0.X	CD16-QP-12.0=
IP Firewall	S16RCH-12.0.X	CD16-CH-12.0=
IP/IPX Firewall Plus	S16RBHP-12.0.X	CD16-BHP-12.0=
IP Firewall Plus IPSec	S16RCHL-12.0.X	CD16-CHL-12.0=
IP/IPX/AppleTalk/IBM/Firewall Plus IPSec 56	S16RQHL-12.0.X	CD16-QHL-12.0=

Dimensions and Weight Specifications

	Cisco 1600 Series	WAN Interface Cards
Width	11.15 in. (28.32cm)	3.1 in. (7.9 cm)
Height	2.19 in. (5.56 cm)	0.8 in. (2.1 cm)
Depth	8.67 in. (22.02 cm)	4.8 in. (12.2 cm)
Weight (minimum)	1.65 lb. (0.75 kg)	0.13 lb (57 g)
Weight (maximum)	1.80 lb. (0.82 kg)	0.19 lbs (85 g)

Power Requirements for Cisco 1600 Series

Output, Watts	27 W maximum
AC Input Voltage	100 to 240 VAC
Frequency	50 to 60 Hz
AC Input Current	0.2 to 0.4 Amps

Environmental Specifications for Cisco 1600 Series and WAN Interface Cards

Operating Temperature	32 to 104 F (0 to 40 C)
Nonoperating Temperature	- 4 to 149 F (-20 to 65 C)
Relative Humidity	10% to 85% noncondensing operating; 5% to 95% noncondensing non-operating

Regulatory Compliance for Cisco 1600 Series and WAN Interface Cards

Safety

- UL 1950
- CSA 22.2 No 950
- EN60950
- EN41003
- AUSTEL TS001
- AS/NZS 3260
- ETSI 300-047
- BS 6301 (power supply)

EMI

- AS/NRZ 3548 Class A
- Class B
- FCC Part 15 Class B
- EN60555-2 Class B
- EN55022 Class B
- VCCI Class II
- CISPR-22 Class B

Immunity

- 55082-1 Generic Immunity Specification Part 1: Residential and Light Industry
- IEC 1000-4-2 (EN61000-4-2)
- IEC 1000-4-3 (ENV50140)
- IEC 1000-4-4 (EN61000-4-4)
- IEC 1000-4-5(EN61000-4-5
- IEC 1000-4-6(ENV50141)
- IEC 1000-4-11
- IEC 1000-3-2

Network Homologation

Europe	CTR2,CTR3
Canada	CS-03
United States	FCC Part 68
Japan	Jate NTT
Australia/New Zealand	TS-013
Hong Kong	CR22

Bellcore Compliance

The Cisco 1604 R router is certified under Bellcore Easy ISDN codes (formerly known as ISDN Ordering Codes or IOCs).

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les- Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam •

4/01 LW2333

Lynx.sc

Digital Microwave Radio

Fast, Cost-Effective Wireless Connectivity

Lynx.sc is a digital microwave radio that provides wireless connectivity with capacity up to two T1/E1 lines at distances exceeding 50 miles (80 km)—and is less expensive than leasing lines.

Using high-quality radios and standard telco interfaces, Lynx.sc allows you to quickly connect or extend your infrastructure over long distances. Because it is wireless, Lynx.sc offers significant cost savings compared to leased-line connections, and provides a time-to-market advantage where installing new lines is impossible or too costly.

In addition, Lynx.sc is license-exempt in most countries, so you can install it when and where you need it, without right-of-way limitations, frequency licensing delays, or waiting for your telecommunications provider to deliver new lines.

Extend or Enhance Your Network Virtually Overnight

Easy installation and hassle-free operation allow you to quickly extend networks and eliminate bandwidth bottlenecks, making Lynx.sc wireless radios the ideal solution for:

- Cellular carriers connecting cell towers and backhauling traffic to central offices or leased line access points
- Cellular carriers and service providers needing to build out infrastructure in remote locations where leased lines are unavailable or cost-prohibitive
- Service providers establishing new Points of Presence and direct connections to customers

About the Lynx® Product Family

The Lynx family of digital microwave radios provides a broad range of point-to-point wireless solutions, delivering a proven and cost-effective alternative to wire and fiber for telco connectivity applications.

In addition to Lynx.sc, the entry-level Lynx product, the Lynx product line includes:

Lynx.HD, offering up to 8xT1/E1 capacity at distances exceeding 40 miles (64 km).

Lynx DS-3, offering DS-3 capacity at distances exceeding 15 miles (24 km).

Lynx OC-3, offering 155 Mbps capacity at distances exceeding 7 miles (11 km).

PRODUCT HIGHLIGHTS

Fast and Easy to Deploy

- License-exempt frequencies eliminate regulatory delays
- Wireless connectivity eliminates the need for leasing or installing lines
- Easy integration with new high-speed switches, legacy data, and voice network products
- Multiple frequency options offer flexibility when co-locating radios

Rapid Return on Investment

- Fast payback compared to leasing T1 lines or building new wireline infrastructure
- Fast deployment opens up new revenue streams and enables faster customer acquisition

99.999% Carrier-Class Reliability

- Meets or exceeds traditional telco wireline standards and requirements
- Transmission rates not affected by weather
- Longer distances and highest reliability due to superior system gain

KEY FEATURES

- 1 to 2 T1/E1 connections
- Frequency Ranges:
  2.4 GHz license-exempt;
  5.8 GHz license-exempt
- Compliant with industry standards
- Point-to-point communications from less than 1 mile/km to more than 50 miles/80 km
- Wide DC power input (±20 to ±63 V), AC adapter available
- Wide operational temperature
- Built-in loopback, far-end monitoring, and private telephone network orderwire
- 2-year warranty

Product Specifications

PRODUCT	MODEL NUMBER	FREQUENCY BAND	DIGITAL CAPACITY (FULL DUPLEX)	CHANNEL PLANS	THRESHOLD (BER=1X10^{-6})	OUTPUT POWER (MINIMUM)	SYSTEM GAIN	DISTANCE (MILES/KM)
Lynx.sc T1	31250	2400-2483.5 MHz	T1 (1.544 Mbps)	2 (A, B)	-94 dBm	+27 dBm	124 dB	>60/96
Lynx.sc 2xT1	31650	2400-2483.5 MHz	2xT1 (2x1.544 Mbps)	1 (A)	-91 dBm	+27 dBm	121 dB	>55/88
Lynx.sc T1	31000	5725-5850 MHz	T1 (1.544 Mbps)	3 (A, B, C)	-93 dBm	+20 dBm	116 dB	>50/80
Lynx.sc 2xT1	31600	5725-5850 MHz	2xT1 (2x1.544 Mbps)	2 (A, B)	-90 dBm	+20 dBm	113 dB	>48/77
Lynx.sc 1E1	31500	2400-2483.5 MHz	E1 (2.048 Mbps)	2 (A, B)	-93 dBm	+27 dBm	123 dB	>60/96
Lynx.sc 1E1	31400	5725-5850 MHz	E1 (2.048 Mbps)	3 (A, B, C)	-92 dBm	+20 dBm	115 dB	>50/80
Lynx.sc 2xE1	31700	5725-5850 MHz	E1 (2x2.048 Mbps)	2 (A, B)	-90 dBm	+20 dBm	113 dB	>48/77

System

Antenna Connector	N-Type female
Full Output Power (2.4 GHz)	≥ +27 dBm, +30 dBm max
RF Attenuation Range	16 dB, minimum
Full Output Power (5.8 GHz)	≥ +20 dBm, +23 dBm typical
RF Attenuation Range	20 dB, minimum
Maximum Receive Level	-5 dBm, error-free
Processing Gain	10 dB, minimum
Transmission Delay	
Radio Only	500 µs, maximum
10-mile path	550 µs, maximum
30-mile path	650 µs, maximum
50-mile path	750 µs, maximum
Regulatory Compliance	US: FCC part 15.247 (ISM), Class B, Canada: IC RSS 210/139 DSX-1: CCITT G.823, AT&T Pub 62411, Bellcore TR-TSY-000499 CEPT-1: ITU-TG703

Digital Line Interfaces

Digital Interface	CEPT-1 (E1) or DSX-1 (T1)
Connector: E1	BNC female
Connector : T1	RJ-45 female, DB-9 female
Line Code: T1	B8ZS or AMI selectable
Line Code: E1	HDB3
Line Build Out: T1	0 to 600 feet/200 m, selectable
Blue Code	AIS (Alarm Indication Signal)
Far-end Loopback	Local or remote control Internal or external signal source

Auxiliary Connections

Orderwire Handset	2-wire, RJ-11
VF Orderwire Bridge	600 ohm balanced, 4-wire, 0 dBm, DB25

Auxiliary Connections Continued

Diagnostics Port	RS-232/RS-422 (craft/TBOS), DB9
Aux. Data Port (Clear Service Channel)	RS-232/RS-422, ≤19.2K baud, DB9
Alarm Port	2 ea. Form C, 6 TTL, DB25
Test Points	Output power, near- and far-end RSL

Power/Environment

DC Power	±20 to ±63 Volts, <45 Watts
Optional AC Adapter	100-250 Volts, 50-60 Hz
Power Connector	6-pin barrier strip, plug-in
Operational Temperature	-30° to +65° C
Humidity	0 to 95%, non-condensing
Altitude	15,000 feet/5000 meters, max.

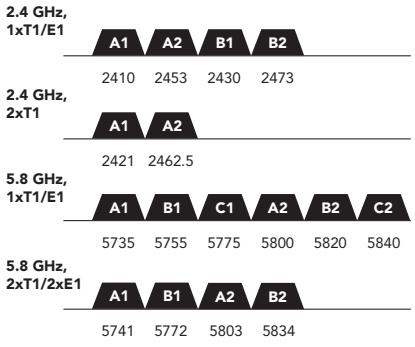
Physical

Size (WxHxD)	17.2 x 3.5 x 14.5 inches 43.7 x 8.9 x 36.8 cm
Weight	11 lbs/5 kg

Mounting (Installation)

EIA Rack Mount	19 inch, 2-unit height (mounting brackets supplied)

Frequency Channel Plans (MHz)



Proxim
The Capacity to Do Great Things.

Proxim Corporation
935 Stewart Drive
Sunnyvale, California 94085

tel: 800.229.1630
tel: 408.731.2700
fax: 408.731.3675

MultiVOIP™

Voice/Fax over IP Networks

Standalone Voice/IP Gateway
Model MVP800

Proprietary Mode

MultiTech® Systems

Multi-Tech MultiVOIP Gateway MVP800

Multi-Tech MVP800 is a stand-alone Voice/IP Gateway which allow analog voice and fax communication over an IP network. The MultiVOIP model number MVP800 has eight voice/fax channels. Multi-Tech's voice/fax over IP gateway technology allows voice and fax communication to ride, with no additional expense, over your existing IP network, which has traditionally been data-only. To access this free voice and fax communication, all you have to do is connect your MultiVOIP to your telephone equipment, and then to your existing Ethernet LAN. The MVP800 is designed with eight voice/fax channels, 10M bps Ethernet LAN interface, and command port.

General	
Device Type	Gateway
Width	44.2 cm
Depth	20.3 cm
Height	9.6 cm
Weight	3.4 kg
Localisation	Canada, United States

Networking	
Form Factor	External
Connectivity Technology	Wired
Data Transfer Rate	10 Mbps
Data Link Protocol	Ethernet
Remote Management Protocol	SNMP, Telnet, HTTP
Status Indicators	Link activity, collision status, power, Boot State, transm it, receive
Features	Manageable

Communications	
Type	Voice interface card - integrated
Digital Signaling Protocol	H.323
Data Compression Protocol	G.729, G.726, G.723
Voice Communication Support	VoIP
Analogue Ports Qty	8

Expansion / Connectivity	
Interfaces	1 x network - Ethernet 10Base-T - RJ-45 ¦ 8 x modem - E&M - RJ-48 ¦ 8 x modem - FXO - RJ-11 ¦ 8 x modem - FXS - RJ-11 ¦ 1 x management - RS-232C - 25 pin D-Sub

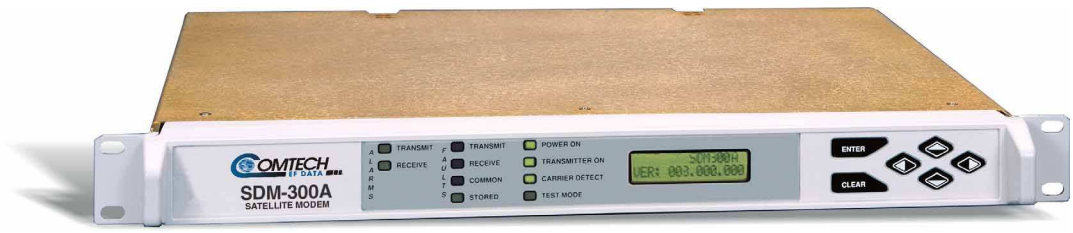
Miscellaneous	
Compliant Standards	CE, CTR 21, UL 1950, FCC Part 15, IC

Power	
Power Device	Power adapter - external
Voltage Required	AC 120/230 V (50/60 Hz)
Power Consumption Operational	30 Watt

Software / System Requirements	
Software Included	Drivers & Utilities
OS Required	Microsoft Windows 95/98, Microsoft Windows 2000 / NT4.0, Microsoft Windows Millennium Edition

Manufacturer Warranty	
Service & Support	2 years warranty
Service & Support Details	Limited warranty - 2 years

SDM-300A
Satellite Modem



FEATURES

- 2.4 kbps to 5 Mbps
- Fully Accessible System Topology (FAST)
- Intermediate Data Rate (IDR)
- INTELSAT Business Services (IBS)
- Drop and Insert (D&I)
- Automatic Uplink Power Control (AUPC)
- Asynchronous Channel Unit Overhead
- Turbo Product Codec (Option)
- Reed-Solomon
- Built-In Self Test
- Burst Mode Operation

APPLICATIONS

Fully configured, the SDM-300A will meet or exceed all of the applicable requirements in IESS-308, 309, and 310 and is available with a full range of industry standard digital interfaces.

COMPATIBILITY

Maintaining Comtech EF Data's excellent history of modem compatibility, the SDM-300A is a direct replacement for many Comtech EF Data modems. When configured properly, the SDM-300A can be installed to communicate with or replace the following Comtech EF Data modems:

- SDM-100
- SDM-650B
- SDM-6000
- SDM-300
- SDM-308B
- CDM-600 (Open Network w/Turbo)
- SDM-309B

COST EFFECTIVE

Comtech EF Data's SDM-300A employs Fully Accessible System Topology (FAST). This technology provides a cost-effective approach to upgrading satellite modem configurations. FAST is an exclusive, industry-first feature that eliminates the need to purchase options before they are needed. Modem selection is easy with no guesswork.

An SDM-300A base modem includes the following features:

- BPSK and QPSK
- Viterbi or Sequential decoding
- Variable data rate to 512 kbps
- IF range from 50 to 180 MHz (1 Hz steps)

FEATURE ENHANCEMENTS

Enhancing the SDM-300A's performance is easy. Some features are added quickly on site, using the FAST access code purchased from Comtech EF Data, other features may require an overhead card. To enable FAST features, simply enter the code at the front panel. Unit enhancements include:

- Variable Data Rate to 5 Mbps
- Viterbi and Sequential Decoding
- 8-PSK
- Turbo Product Codec
- Reed-Solomon (R-S) Codec
- Duplex R-S Codec (for R-S and Turbo in the same unit)
- IDR / IBS / D&I / AUPC / ASYNC
- I/O Connector (25-, 50-, 34-, 37-, 100-pin)
- Asymmetrical Loop Timing
- G.703 Interface with DB-9 and BUC
- 2 x ADPCM Voice in 64 kbps IBS Frame
- 4 or 8 Channel Mux
- Flex Mux

BUILT-IN SELF-TEST

Comtech EF Data's unique built-in self-test feature allows the SDM-300A to complete a bit error rate (BER) measurement without the use of expensive noise generators and BER test equipment. The built-in self test:

- Provides fully functional modem testing with noise
- Displays pass or fail results
- Establishes modem confidence
- Eliminates BER test equipment

When commanded to the self test mode through the front panel or remote port, the SDM-300A disables the Tx and Rx IF ports and internally tests modulator, demodulator, and interface functions by means of a BER measurement. The BER measurement is achieved via an internal IF noise generator and BER test equipment built into the SDM-300A.

REDUNDANCY

The SDM-300A redundancy is supported by the SMS-301 (1:1) and SMS-7000 (2:8) switches.

2114 West 7th Street, Tempe, Arizona 85281 USA Voice 1 480 333 2200 Fax 1 480 333 2540 Email sales@comtechefdata.com

SDM-300A Satellite Modem

SYSTEM SPECIFICATIONS (FULLY ENHANCED)

Operating Frequency Range	50 to 180 MHz, in 1 Hz steps
Digital Interface (Standard)	EIA-232, EIA-422, and V./35 (25-pin D)
Digital Data Rate	2.4 kbps to 5 Mbps, in 1 bit/s steps
Symbol Rate	4.8 kbps to 2.5 Mbps
Modulation and Coding	
Viterbi (K=7)	BPSK 1/2 QPSK / OQPSK 1/2, 3/4, 7/8 8-PSK 2/3 TCM
Sequential	BPSK 1/2 QPSK / OQPSK 1/2, 3/4, 7/8
Concatenated Viterbi and Reed-Solomon	BPSK 1/2 QPSK / OQPSK 1/2, 3/4, 7/8 8-PSK 2/3 TCM
Turbo	BPSK 21/44, 5/16 QPSK / OQPSK 3/4 8-PSK 3/4
Uncoded	BPSK, QPSK, OQPSK
Plesiochronous Buffer	2 to 99 ms, in 2 ms steps 32 to 262,122 bps, in 16 bit steps
Data Scrambling	IESS-308 (V.35), IESS-309, IESS-310, or None
External Reference Input	1, 5, 10, or 20 MHz
Agency Approvals	CE Mark

MODULATION SPECIFICATIONS

Output Power	-5 to -30 dBm, adjustable in 0.1 dB steps Optional: +5 to –20 dBm, high-power output
Output Spurious	< -55 dBc, 0 to 500 MHz (4 kHz band)
Output Frequency Stability	± 10 PPM
Output Return Loss	> 20 dB
Output Impedance	75Ω (Optional: 50 Ω)
Data Clock Source	Internal or External

DEMODULATION SPECIFICATIONS

Input Power:	
Desired Carrier	-30 to –55 dBm
Maximum Composite	-5 dBm to +40 dBc
Input Impedance	75Ω (Optional: 50 Ω)
Input Return Loss	> 20 dB
Carrier Acquisition Range	± 35 kHz from 100 Hz to 35 kHz
Acquisition Time	< 1 second for 64 kbps 1/2 rate
Clock Acquisition Range	± 100 PPM
AGC Output	0 to 10 V at 10 mA maximum

ENVIRONMENTAL AND PHYSICAL

Prime Power, AC	90 to 264 VAC, 47 to 63 Hz, 30W 38 to 64 VDC, 40W
Size	1.75H x 19.0W x 15.7D inch (1 RU) (4.4H x 48 W x 40 D cm)
Weight	< 11 lbs. (4.9 kg)
Temperature	0 to 50°C (32° to 122°F) Operating -40° to +70°C (-40° to +158°F) Storage
Humidity	< 0 to 95%, non-condensing

BURST MODE SPECIFICATIONS

Operating IF Range	50 to 180 MHz, in 1 Hz steps
Type of demodulation	QPSK
Operating Channel Spacing	< 0.5 dB degradation operating with 2 adjacent-like channels, each 10 dB higher at 1.3 times the symbol rate, or a minimum of 1.2 times the specified acquisition range.
Carrier Acquisition Range	± 4kHz at E_b/N_0 = 8 dB, 99% prob.
Digital Data Rate, QPSK, R=1/2	19.2 kbps
Forward Error Correction	Convolutional encoding with soft-decision, K=7 Viterbi decoding
Data Descrambling	Selectable or none, 2^{15-1}, Synchronous

AVAILABLE OPTIONS

How Enabled	Option
FAST	Variable data rate
FAST	Add Viterbi or Sequential decoder
FAST	8-PSK
FAST	Asymmetrical loop timing
FAST + Card	IBS / IDR / D&I (requires Overhead card)
FAST + Card	2XADPCM Voice (included with IBS or IDR)
FAST + Card	G.703 interface (50-pin D connector, requires UB530 BOP)
FAST + Card	G.703 interface (PL/7838 interfaces module option, BNC)
FAST + Card	Reed-Solomon (R-S) Codec
FAST + Card	Duplex R-S Codec (Suitable with Turbo Codec)
Card	Turbo Product Codec
FAST + Card	AUPC only (requires Tx & Rx bds)
FAST + Card	Asynchronous overhead (ASYNC/AUPC) w/50-pin D connector
Hardware	50Ω IF
Hardware	High output power to +5 dBm
Hardware	2- to 8-channel multiplexer
Hardware	Flex Mux
Hardware	-48 VDC power supply
Hardware	2 x 10^{-7} internal stability for IF and data clock
Hardware	25-pin (F) D connector with EIA-530 (EIA-422), EIA-232, & V.35
Hardware	50-pin (F) D connector for use **with overhead card**
Hardware	50-pin (F) D connector for use **without overhead card** Includes EIA-422, EIA-232, & V.35
Hardware	34-pin (F) V.35 'Winchester' connector with V.35

BER PERFORMANCE (E_b/N_0, dB)

Viterbi

BER	1/2	3/4	7/8
10^{-3}	3.8	4.9	6.1
10^{-4}	4.6	5.7	6.9
10^{-5}	5.3	6.4	7.6
10^{-6}	6.0	7.2	8.3
10^{-7}	6.6	7.9	8.9
10^{-8}	7.2	8.5	9.6

Viterbi & Reed-Solomon

BER	1/2	3/4	7/8
10^{-6}	4.1	5.6	6.7
10^{-7}	4.2	5.8	6.9
10^{-8}	4.4	6.0	7.1
10^{-10}	5.0	6.3	7.5

56 kbps, Sequential

BER	1/2	3/4	7/8
10^{-3}		4.6	5.5
10^{-4}	4.1	5.1	6.1
10^{-5}	4.5	5.5	6.6
10^{-6}	5.0	5.9	7.3
10^{-7}	5.4	6.4	7.8
10^{-8}	5.8	6.8	8.4

1544 kbps Sequential

BER	1/2	3/4	7/8
10^{-3}	4.8	5.2	6.0
10^{-4}	5.2	5.7	6.4
10^{-5}	5.6	6.1	6.9
10^{-6}	5.9	6.5	7.4
10^{-7}	6.3	7.0	7.9
10^{-8}	6.7	7.4	8.4

1544 kbps,Sequential & RS

BER	1/2	3/4	7/8
10^{-6}	4.1	5.6	6.7
10^{-7}	4.2	5.8	6.9
10^{-8}	4.4	6.0	7.1
10^{-10}	5.0	6.3	7.5

8-PSK with/without RS

BER	2/3 w/o RS	2/3 with RS
10^{-6}	8.7	6.1
10^{-7}	9.5	6.4
10^{-8}	10.2	6.6
10^{-9}	11	6.9
10^{-10}	11.8	7.2

Viterbi, OQPSK

BER	1/2	3/4	7/8
10^{-3}	4.1	5.2	6.4
10^{-4}	4.9	6.0	7.2
10^{-5}	5.6	6.7	7.9
10^{-6}	6.3	7.5	8.6
10^{-7}	6.9	8.2	9.2
10^{-8}	7.5	8.8	9.9

Uncoded, BPSK, QPSK, OQPSK

BER	1/1
10^{-3}	8.0
10^{-4}	9.6
10^{-5}	10.8
10^{-6}	11.6
10^{-7}	12.4

Turbo Product Codes

	QPSK	BPSK	8-PSK
BER	3/4	21/44	5/16	3/4
10^{-6}	3.9	2.8	-	7.0
10^{-7}	4.1	3.1	-	7.3
10^{-8}	4.3	3.3	-	7.6
10^{-9}	4.8	3.7	4.0	8.0

CNSH-800 Eight (8) Port 100/10Mbps Fast Ethernet Switch

CNSH-800 is a powerful Eight (8) 10/100Mbps ports Fast Ethernet Switch. Every port is equipped with a Built-In Auto-Negotiation function. Simply attach a network device to any port and the port will automatically set to operate at the fastest possible speed. This Switch is designed to provide lots of bandwidth with minimum hassle. They are 100% Plug & Play and require no configuration. These models fully comply with IEEE 802.3u and IEEE 802.3 standards for Fast Ethernet and Ethernet operation.

Key Features

Eight (8) independent bandwidths with 10Mbps - 200Mbps capability.

Eight (8) ports with Auto-Negotiation function.

Full wire speed Store-and-Forward technology instantly eliminates bad packets.

All ports support Auto-MDI/MDIX which can detect and correct crossover cables.

IEEE 802.3u and 802.3 standards compliant.

IEEE 802.3x Flow-Control support for Full-Duplex operaion.

Back-Pressure support for Half-Duplex operation.

Broadcast Storm control.

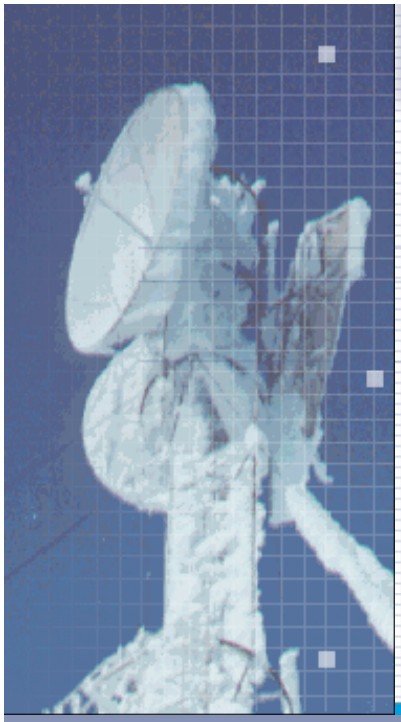
Plug & Play with easy to read diagnostic LEDs.

Product Name	**Eight (8) Port 100/10Mbps Fast Ethernet Switch**
Standards	IEEE 802.3u: 100BASE-TX IEEE 802.3: 10BASE-T
Ports	Eight (8)ports 100BASE-TX/10BASE-T
Media Supports	100BaseTX: Category 5 TP 10BaseT: Category 3, 4, or 5 TP
Bandwidth	100BaseTX/10BASE-T: 200/100/20/10Mbps, via Auto-Negotiation
Forwarding/Filtering Rate	148,800 packets/second per port @ 100Mbps, maximum. 14,880 packets/second per port @ 10Mbps, maximum.
Latency	2.7msec. @100Mbps minimum 13 msec. @10Mbps minimum
MAC Addresses	1K Six (6) Bytes MAC address entries (maximum) Self-Learning
Buffer Memory	1M bits
Duplex Modes	All ports support Half-Duplex or Full-Duplex operation

Auto-MDI/MDIX	All ports support Auto-MDI/MDIX
LED Indicators	One (1) for Power On/Off One (1) per port for Link / Activity
External Power Adapter	Output: 9VDC, 1Amp (Input according to country)
Power Consumption	9W maximum
Environment	Operating Temperature: 0° ~ 45° C (32° ~ 113° F) Storage Temperature: -20° ~ 70° C (-4° ~ 158° F) Humidity: 10% ~ 90% Non-Condensing
Certifications	FCC, CE
Dimensions	145 x 85 x 25mm (5.7 x 3.4 x .98 inches)

ORDERING INFORMATION

CNet Model#	Description
CNSH-800(L)	Eight (8) ports 10/100Mbps Fast Ethernet Switch (Plastic case)



Telecomunicaciones
Antenas

ANTENAS

Total Quality

NHC

ISO 9002

NRD Comunicaciónes S.A.

Fábrica de Antenas y Filtros

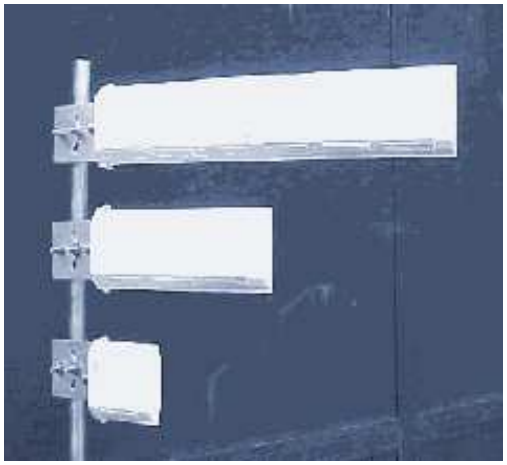
PRODUCTOS

Productos

Antenas
Wireless - Spread Spectrum
2300 - 2500 Mhz

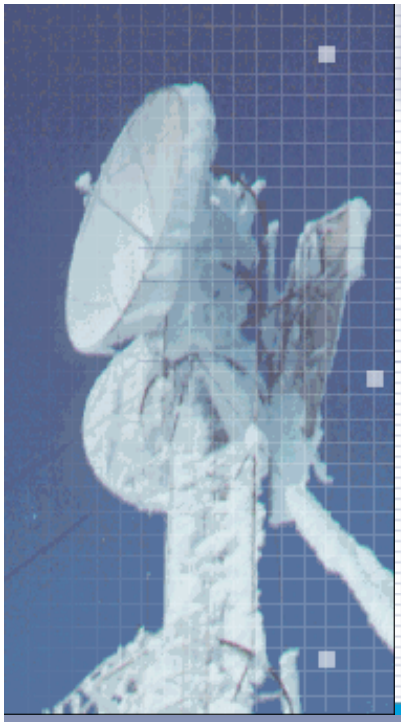
Este conjunto de antenas para estaciones base en la banda de frecuencias de 2300 a 2500 Mhz, cumple con las necesidades, de instalación en sistemas punto a punto y multipunto.

Estos modelos de reducido peso y poca resistencia al viento, permiten ser instalados hasta en lugares donde no se cuenta con la posibilidad de montar una torre ya que Las cargas y esfuerzos transferidos a los soportes son muy bajos.
Su montaje es extremadamente simple y rápido, no necesitando herramientas especiales.
Por el continuo control de calidad eléctrico y mecánico y los ajustes realizados en laboratorio las antenas se entregan listas para su instalación



DESCRIPCIÓN	Yagui NYS 03 / 07 / 14 elementos			Colineal NDC 04 / 08 / 16		Antena Parabólica NPR 08 / 10	
MODELO	03	07	14	04	08	08	10
Ganancia (dBi) Centro de banda	8	12	15	8	12	24 (dBi)	27
Ancho de haz Horizontal (grd) Vertical (grd)	85 54	75 40	57 45	n/c n/c		12.3 11.3	10 9
Relación Frente espalda	20 (dB)			n/c		30 (dB)	
Ancho de banda Para R.O.E. >1.5 : 1	200 (Mhz)			100 (Mhz)		200 (Mhz)	
Impedancia	50 (Ohms)			50 (Ohms)		50 (Ohms)	
Conector	N (Hembra)			N (Hembra)		N (Hembra)	
Velocidad de Viento	160 (Km)			160 (Km)		160 (Km)	

NRD Comunicaciónes S.A.
Tel / Fax : 54-11 4727-0018 - www.nrdcom.com - E-Mail: nrd@nrdcom.com
Pascal 147 y Esquiú - C.P. 1611 - Don Torcuato - Pcia. de Buenos Aires - Argentina
Horario: Lunes a Viernes de 9 Hs. a 13 Hs. y de 14 Hs. a 17 Hs. 30 min.



Telecomunicaciones
Antenas

ANTENAS
Total Quality
NHC
ISO 9002

NRD Comunicaciónes S.A.
Fábrica de Antenas y Filtros

Productos

Antenas Parábolicas
Wireless 2300 - 2500 mhz

Este conjunto de antenas para estaciones base en la banda de frecuencias de 2300 a 2500 Mhz, cumple con las necesidades, de instalación en sistemas punto a punto y cliente multipunto.

Estos modelos con poca resistencia al viento, permiten ser instalados hasta en lugares donde no se cuenta con la posibilidad de montar una torre ya que Las cargas y esfuerzos transferidos a los soportes son muy bajos.

Su montaje es extremadamente simple y rápido, no necesitando herramientas especiales.

Por el continuo control de calidad eléctrico y mecánico y los ajustes realizados en laboratorio las antenas se entregan listas para su instalación.

NPR06C24EH

NPR07C24ET

NPR08C24EH

NPR10C24EH

NPR15C24EH

DESCRIPCIÓN	Antenas Parabólica				
MODELO	NPR 06	NPR 07	NPR 08	NPR 10	NPR 15

Ganancia nominal (dBi)	21	23	24	27	30
Ancho de haz Horizontal (grd) Vertical (grd)	 18.1 18.1	 14.5 14.5	 12.8 12.8	 9.1 9.1	 6.4 6.4
Relación Frente espalda	25 (dB)	25 (dB)	25 (dB)	25 (dB)	27 (dB)
Polarización	H y V	V	H y V	H y V	H y V
Ancho de banda Para R.O.E. >1.5 : 1	200 (Mhz)				
Impedancia	50 (Ohms)				
Conector es disponibles	RPSMA, RPTNC, N				

NRD Comunicaciónes S.A.
Tel / Fax : 54-11 4727-0018 - www.nrdcom.com - E-Mail: nrd@nrdcom.com
Pascal 147 y Esquiú - C.P. 1611 - Don Torcuato - Pcia. de Buenos Aires - Argentina
Horario: Lunes a Viernes de 9 Hs. a 13 Hs. y de 14 Hs. a 17 Hs. 30 min.

ANEXO K

Análisis realizado por la Dirección General de Investigación Especial en Telecomunicaciones de la SUPTEL del documento "Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las Empresas de Telecomunicaciones"

(Documento proporcionado por la SUPTEL)

SUPERINTENDENCIA DE TELECOMUNICACIONES

Oficio No. IET-565-06

Quito, a 8 de agosto de 2006

Señor
Christian Gallardo
Presente

De mi consideración:

Me refiero a su comunicación presentada a esta Dirección General, el día de ayer 7 de agosto, y una vez analizados los temas contenidos en el documento denominado "Análisis de estrategias para el control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las empresas de telecomunicaciones", presentado por usted, me permito manifestar lo siguiente:

- ✓ Los contenidos del documento en mención, constituyen una recopilación y análisis de los principales fraudes que se presentan en el campo de las telecomunicaciones, enfocado a los servicios de telefonía fija.

- ✓ En términos generales, la forma descriptiva en que se analizan los diversos tipos de fraude, aportan dentro de la comprensión del alcance con que dichos ilícitos afectan tanto técnica como económicamente a las empresas operadoras de telecomunicaciones debidamente autorizadas.

- ✓ Es importante rescatar que, en nuestro país, sobre aspectos concernientes al fraude en telecomunicaciones, no existen textos de consulta, sino mas bien, dicho tema se asimila dentro del aspecto práctico, obtenido en base a la experiencia, lo que permite a nuestro criterio considerar al documento analizado como importante.

Finalmente, me permito solicitar a usted que de ser posible se proporcione a esta Dirección General una copia del documento en mención, a fin de que se lo utilice como una herramienta de consulta.

Atentamente,

Ing. José María Gómez de la Torre
DIRECTOR GENERAL DE INVESTIGACIÓN ESPECIAL EN TELECOMUNICACIONES (S)