# Graduate School of Business

# Master en Dirección de Empresas

**Tesis para optar al grado de Master de la Universidad de Palermo en Dirección de Empresas**

***La gestión del fraude en empresas de telefonía***

***Propuesta de mejoras***

**Tesista: Juan Manuel García Carral**

**Legajo: 56464**

**Director de Tesis: Dr. Leandro A. Viltard**

**2017**

Ciudad Autónoma de Buenos Aires – Argentina

# EVALUACIÓN DEL COMITÉ

# AGRADECIMIENTOS

Quisiera agradecer a mi tutor de tesis Leandro Viltard por tenerme fe y romperme la paciencia, por no decirlo de otro modo, cuando yo mismo no encontraba el empuje para abordar la tesis. ¡Gracias totales!

# RESUMEN DE LA TESIS

Todas las transacciones que posean valor en dinero son plausibles de sufrir un abuso por parte de alguno de los actores que la componen. El caso del servicio de telefonía no es ajeno a esta realidad dado que -cada llamada realizada-cuenta con un costo y -a la vez- un precio de venta, por lo cual representa una operación comercial.

El propósito de la presente tesis se relaciona con aportar una guía de buenas prácticas, aplicable a la industria del sector de las comunicaciones, que pueda ayudar para trabajar de forma proactiva sobre la problemática del fraude en el servicio de telefonía. Los aportes se han orientado a la elaboración de herramientas informáticas que ayuden a la prevención, detección temprana y –además- a la modificación de los procesos ya existentes con el objeto de minimizar los expuestos al fraude.

Se utilizó una metodología cuali-cuantitativa. El diseño de la investigación es no experimental y transversal.

# TABLA DECONTENIDOS

RESUMEN DE LA TESIS ..... IV

I. INTRODUCCIÓN ..... 1

I.1 Antecedentes y motivos que originan la investigación ..... 1

I.2 Planteo del problema ..... 2

I.3 Lineamientos generales de la investigación ..... 4

I.4 Objetivos ..... 5

I.5 Hipótesis ..... 6

I.6 Resumen conceptual del desarrollo del trabajo ..... 6

II. METODOLOGÍA ..... 8

III. MARCO TEÓRICO ..... 12

III. 1 Origen, evolución y proyección de la telefonía ..... 13

Historia de la telefonía ..... 13

Seguridad y privacidad en la telefonía tradicional ..... 16

Las nuevas tecnologías de comunicaciones ..... 17

El futuro de la telefonía ..... 19

Conclusiones del apartado ..... 26

III. 2 Tipologías de fraude telefónico ..... 28

Enumeración de los escenarios de fraude de mayor ocurrencia ..... 28

Conclusiones del apartado ..... 40

III. 3 Modelación y detección del fraude telefónico ..... 40

Comparativa con fraudes transaccionales en otras industrias ..... 41

Propuestas de modelos de detección de fraude ..... 47

El crecimiento del poder computacional ..... 53

El crecimiento de la disponibilidad de información ..... 56

Conclusiones del apartado ..... 57

III. 4 Buenas prácticas en los procesos anti fraude ..... 59
Conclusiones del apartado ..... 66
III. 5 Conclusiones del Marco Teórico ..... 67
IV. MARCO INVESTIGATIVO ..... 70
IV. 1 Análisis de un caso: Empresa NET ..... 71
Descripción general de la empresa y sus servicios ..... 72
Descripción de un proyecto de interés ..... 77
Conclusiones del análisis del caso: Empresa NET ..... 82
IV. 2 Entrevistas con informantes-clave ..... 82
El fraude es sintomático de la industria analizada ..... 83
Las herramientas utilizadas son insuficientes ..... 84
Los montos de los fraudes son grandes ..... 85
La complejidad de encontrar al perpetrador del fraude ..... 87
La industria telefónica no es colaborativa ..... 88
La adopción de tecnologías de punta ..... 89
El fraude es un problema de toda la organización ..... 90
El control del fraude y su tercerización ..... 90
Mejoras sugeridas por los encuestados ..... 91
Conclusiones de las entrevistas ..... 92
IV. 3 Encuestas a representantes de la industria ..... 93
Descripción y metodología empleada ..... 93
Análisis de los resultados de las encuestas ..... 94
Conclusiones de las encuestas ..... 106
IV. 4 Conclusiones del Marco Investigativo ..... 108
V. CONCLUSIONES GENERALES, PROPUESTAS Y APORTES PARA FUTURAS INVESTIGACIONES ..... 110
V.1 Conclusiones ..... 110
Respecto del estado del arte en tecnologías y prácticas ..... 110

Respecto al incidencia del fraude en la industria telefónica ..... 115
V.2 Propuestas ..... 118
Buenas prácticas en materia de procesos ..... 118
Buenas prácticas en materia de herramientas informáticas ..... 123
Buenas prácticas en materia de colaboración ..... 131
V.3 Aportes para futuras investigaciones ..... 133
BIBLIOGRAFÍA ..... 135
ANEXOS ..... 141
Anexo I: Encuesta a representantes de la industria ..... 141
ANEXO II: Guía de entrevistas a informantes-clave ..... 144
ANEXO III: Lista de costos mayorista de telefonía ..... 146
ANEXO IV: Destinos de alto riesgo ..... 150
ANEXO V: Estadísticas de telefonía ..... 151
CURRICULUM VITAE ..... 153

# LISTA DE FIGURAS

Figura 1 - Lineamientos generales ..... 5

Figura 2 - Flujo de una llamada telefónica normal ..... 29

Figura 3 - Flujo de una llamada telefónica víctima de “*blueboxing*” ..... 30

Figura 4 - Fases una llamada con un establecimiento normal ..... 32

Figura 5 - Fases de una llamada con falso establecimiento ..... 33

Figura 6 - Flujo de una llamada cursada por un secuestrador o hacker ..... 35

Figura 7 - Flujo de proceso conceptual de un sistema de detección de fraude ..... 44

Figura 8 - Proceso teórico de buenas prácticas propuesto por VISA ..... 61

Figura 9 - Flujo de trabajo para gestión del riesgo ..... 63

# LISTA DE CUADROS

Cuadro 1 - Metodología de la investigación ..... 11

Cuadro 2 - Crecimiento líneas fijas instaladas en La Argentina (período 2008 – 2012)..... 25

Cuadro 3 - Crecimiento llamadas de telefonía fija en La Argentina (período 2008 – 2012) . 26

Cuadro 4 - Crecimiento líneas móviles en La Argentina (período 2008 – 2012)..... 26

Cuadro 5 - Origen, evolución y proyección de la telefonía ..... 27

Cuadro 6 - Tipologías de fraude..... 39

Cuadro 7 - Pérdidas anuales (estimadas) ocasionadas por fraudes..... 96

Cuadro 8 - Presencia de fraude telefónico en las empresas ..... 98

Cuadro 9 - Facturación anual (estimada) declarada para la unidad de telefonía ..... 100

Cuadro 10 - Matriz de respuestas de la encuesta ..... 143

Cuadro 11 - Resumen de entrevistas a informantes-clave ..... 144

Cuadro 12 - Tarifas mayoristas de telefonía..... 146

Cuadro 13 - Destinos y prefijos asociados a fraudes ..... 150

Cuadro 14 - Líneas totales en servicio de telefonía fija ..... 151

Cuadro 15 - Abonados totales en servicio de telefonía móvil ..... 152

# LISTA DE GRÁFICOS

Gráfico 1 - Crecimiento usuarios de aplicación Whatsapp (período 2011 – 2014)..... 24

Gráfico 2 - Crecimiento usuarios de Facebook Messenger (período 2014 – 2016) ..... 24

Gráfico 3 - Pérdidas por fraude en tarjetas de crédito en los EEUU ..... 42

Gráfico 4 – Comparación análisis absoluto versus análisis diferencial ..... 49

Gráfico 5 – Evolución de la Ley de Moore ..... 55

Gráfico 6 - Presencia de áreas especializadas de antifraude en las organizaciones ..... 95

Gráfico 7 - Nivel de satisfacción con las áreas antifraude ..... 95

Gráfico 8 - Perdidas anuales (estimadas) ocasionadas por fraudes ..... 97

Gráfico 9 - Presencia de fraude telefónico en las empresas ..... 98

Gráfico 10 - Facturación anual (estimada) para la unidad de telefonía ..... 99

Gráfico 11 - Participación en agrupaciones de interés ..... 101

Gráfico 12 - Participación en agrupaciones de interés de las empresas que poseen áreas especializadas ..... 102

Gráfico 13 - Presencia de procesos para evitar proactivamente el secuestro del equipamiento telefónico de los usuarios ..... 103

Gráfico 14 - Presencia de limitaciones en cuanto a destinos habilitados. ..... 104

Gráfico 15 - Presencia de procesos para la detección del fraude de suscripción ..... 105

Gráfico 16 - Presencia de técnicas estadísticas en el análisis y detección de fraude ..... 106

Gráfico 17 - Líneas totales en servicio de telefonía fija ..... 151

Gráfico 18 - Abonados totales en servicio de telefonía móvil ..... 152

# I. INTRODUCCIÓN

El presente apartado pretende otorgar un marco de referencia ordenado al presente estudio en cuanto a sus antecedentes y motivos; el planteo del problema y las preguntas que lo han guiado; la hipótesis a verificar, los objetivos perseguidos y las conclusiones finales buscadas.

## I.1 Antecedentes y motivos que originan la investigación

Durante los últimos 15 años he ejercido mi rol de ingeniero electrónico en el sector de las comunicaciones. En ese sector he colaborado con distintas empresas tanto desde dentro de la organización en puestos gerenciales, como desde fuera en funciones consultivas. Si bien he tenido que trabajar en distintas áreas de estas empresas (infraestructura, Internet, seguridad informática, desarrollo de software, otros) encontré especial interés en los servicios de telefonía. Este interés -no solo está originado en la tecnología de base utilizada para construir y brindar el servicio- sino en los aspectos del negocio en sí, que tiene similitudes a un mercado de valores. El servicio de telefonía se construye mediante la interconexión de distintos operadores (locales y globales) que intercambian el tráfico de sus redes entre sí. En este ecosistema los distintos destinos telefónicos son comprados a otros operadores y vendidos a los clientes finales. Por lo general, la diferencia entre la compra y la venta de la unidad mínima de intercambio (el minuto o segundo de llamada) es pequeña y el negocio posee viabilidad comercial cuando se posee un volumen de llamadas mensuales grande. Es por este gran mercado de operaciones y en la sensibilidad entre la compra y la venta que aparece el fraude en este sector.

Como profesional he tenido que participar en la definición de buenas prácticas para la detección y disminución del fraude varias veces. No solo en el sector estudiado sino en otros,

como la industria de salud, más exactamente la salud pública. Esta experiencia me ha brindado un especial interés en estudiar y recopilar las técnicas que mejor se aplicarían a la resolución de la problemática. Por otro lado, la exposición en los últimos tiempos a soluciones de *Big Data*, *Data Science*, procesamiento distribuido y otros avances del último lustro me ha hecho entender que estos paradigmas deberían aplicarse de forma rutinaria a la resolución de cualquier problema que pueda ser modelado y predicho, en especial aquellos que poseen grandes cantidades de datos. La industria de la telefonía posee estas características.

En otro aspecto he presenciado -en primera persona- las quejas de distintos sectores de las organizaciones cuando deben lidiar con enormes montos de fraude. El sector financiero debe decidir cómo pagar ese gasto imprevisto, el sector operativo está urgido a implementar mejoras para evitar una nueva ocurrencia y los sectores comerciales se ven limitados en su oferta de servicios por miedo a lo desconocido. Todas estas áreas deberían colaborar de forma conjunta para mejorar sus prácticas y herramientas disponibles, y es mediante esta investigación donde se podrían encontrar un primer acercamiento a la resolución del problema.

Para finalizar, considero que el tema investigado puede ser fácilmente transportado a otros rubros, compartiéndose el beneficio de forma exponencial.

### I.2 Planteo del problema

En primera medida, el presente trabajo pretende verificar la vigencia del servicio telefónico a la luz de los rápidos cambios en materias de tecnologías de comunicación que se viven. Entendiendo que es un servicio que contará una vigencia de -al menos- una década, en

segunda medida, se busca entender el impacto que posee el fraude en este segmento y que hacen las empresas locales para mitigarlo. Finalmente y una vez comprendida la dimensión del problema y sus particularidades, se intenta brindar una serie de buenas prácticas que ayuden a la comunidad.

La necesidad de poseer procesos que contemplen la potencial exposición constante al fraude es crítica y debe ser trabajada desde todas las áreas de las organizaciones y mediante una metodología transversal. Es importante aceptar que la problemática ofrece una entidad tal que se le debe asignar recursos suficientes para poder detectarla preventivamente o, al menos, con las menores perdidas posibles.

De esta manera, se indagará en la actualidad de los prácticas y las herramientas comunes que las compañías emplean. También, se investigarán los problemas comunes a los que se enfrentan, planteándose las siguientes preguntas como base para este estudio:

- ¿Cuál es el impacto económico que posee el fraude en las compañías de servicio de telefonía?
- ¿Cuál es el impacto en el servicio prestado?
- ¿Debe asignarse recursos mayores a la gestión del fraude?
- ¿Qué prácticas implementan para la prevención, la detección temprana y su posterior contención?
- ¿Existen organizaciones locales o regionales donde compartir y enriquecer el conocimiento de la comunidad respecto a esta temática?
- ¿Cuál es el estado del arte respecto a la detección del fraude?

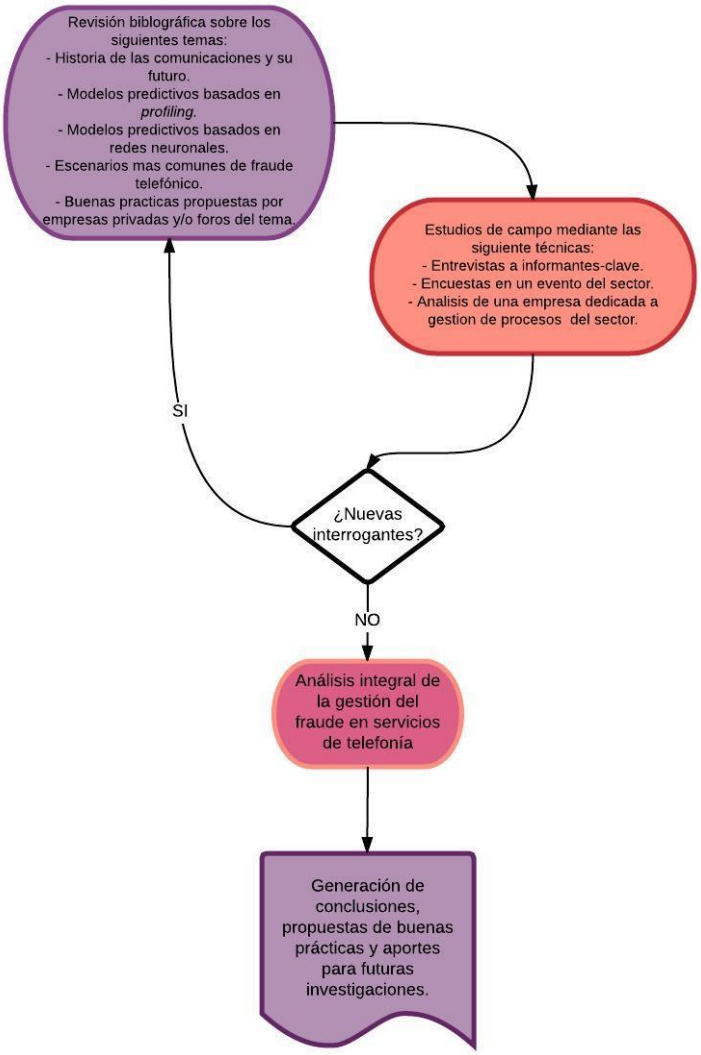
- ¿En que ayudan los avances de modelos probabilísticos y/o redes neuronales a la problemática?
- ¿Cómo deben modificarse los procesos de una organización para disminuir la probabilidad de fraude?
- ¿Cómo deben modificarse los procesos entre empresas de comunicaciones para disminuir el fraude?

A efectos de proponer ideas de gestión del fraude, se analizaran tanto las practicas del sector estudiado como las de otras industrias que tengan exposición cotidiana a fenómeno.

### I.3 Lineamientos generales de la investigación

En el siguiente gráfico se visualiza el proceso utilizado para la realización de la presenta investigación. El proceso consiste en una iteración constante entre teoría y práctica para lograr nuevas interrogantes que faciliten llegar a demostración de la hipótesis.

**Figura 1 - Lineamientos generales**




Fuente: Elaboración propia (2016)

## I.4 Objetivos

General: Analizar los procesos de detección y gestión de fraude en empresas de servicios telefónicos, entender sus limitación y proponer mejoras.

Específicos:

- Determinar la vigencia futura del servicio de telefonía a la luz la constante aparición de nuevas tecnologías en materia de comunicaciones.

- Estudiar el estado del arte en técnicas de modelos de comportamiento basados en datos cuantitativos.
- Determinar cuáles son los escenarios más comunes de fraude y sus actores.
- Entender –en el campo– las prácticas comunes que las empresas implementan para detectar y disminuir las probabilidades de ser víctimas de fraude.
- Proponer ideas y buenas prácticas que puedan ser incluidas en los procesos de las empresas de comunicaciones.

### I.5 Hipótesis

La generación de buenas prácticas en los procesos de las empresas de comunicaciones, que se basen en herramientas informáticas orientadas a la detección de patrones, puede ayudar en la disminución del fraude telefónico.

### I.6 Resumen conceptual del desarrollo del trabajo

A continuación, una breve descripción los aparatados que se encuentran en la presente tesis:

Capítulo I - Introducción: se refieren los objetivos del análisis, las motivaciones del investigador y las problemáticas que se buscan resolver a través de la investigación.

Capitulo II - Metodología: se desarrolla la explicación de las acciones realizadas durante la investigación para alcanzar los objetivos propuestos y corroborar la hipótesis. También son enumeradas las características de la investigación y los métodos de recolección de información usados.

Capitulo III - Marco Teórico: a través de material publicado por expertos en el tema se exponen los fundamentos teóricos que guía la investigación. El marco teórico busca entender

el estado del arte en la materia de fraude, los avances en sistemas de detección de patrones y la tendencia de las tecnologías de comunicaciones.

Capitulo IV - Marco Investigativo: se expone el resultado del trabajo de campo producto de las técnicas de recolección elegidas. Se utilizaron múltiples técnicas (entrevistas presenciales a informantes-clave, encuestas en eventos del sector y análisis de una empresa del rubro) para entender las similitudes y diferencias entre lo aprendido de la teoría y la realidad práctica.

Capítulo V - Conclusiones generales, propuestas y aportes: finalmente se realiza la comparación de la teoría expuestas por los expertos y los datos obtenidos en campo, con la intención de alcanzar los objetivos propuestos y corroborar – o no- la hipótesis de la tesis. Adicionalmente se realiza la enumeración de las buenas prácticas recomendadas para la disminución del fraude en el sector y se comparten aportes para futuras investigaciones.

La tesis se complementa con una bibliografía seleccionada que ha sido consultada.

# II. METODOLOGÍA

El estudio realizado es de tipo exploratorio descriptivo, con el objetivo de realizar una correcta representación del objeto de la investigación: la gestión del fraude en la industria de la telefonía.

Se hizo uso de una metodología cuali-cuantitativa -aunque con predominio cualitativo- que fue guiada, por un lado, por lo investigado durante el proceso de recolección de conocimiento puramente teórico y -por otro-con la información recogida de la praxis empresarial. De esta forma, se planteó un análisis que incluye tanto aquello escrito por investigadores internacionales de primer nivel, como lo que realizan o no las empresas en la práctica cotidiana.

Para el Marco Teórico se hizo uso de diversos estudios, tesis de grado y posgrado, publicaciones científicas, libros especializados en comunicaciones y/o seguridad informática, libros de divulgación de tópicos tecnológicos, informes de organizaciones internacionales, *brochures* de productos comerciales, casos de éxito, páginas web del tema y otros documentos de interés. Esta información fue recopilada, comparada y expuesta de manera unificada para un mejor entendimiento del objeto de estudio.

El diseño de investigación es no experimental y, dentro de este tipo de diseños, el estudio es transversal por haberse tomado información en una franja determinada del tiempo (entre noviembre de 2015 y junio de 2016).

El criterio de selección de las muestras es no probabilístico, intencional, no aleatorio y dirigido para todas las técnicas de campo utilizadas.

La unidad de respuesta buscada fue siempre direccionada a los tomadores de decisiones dentro de los procesos gestión del fraude. En las encuestas, esto abarcó distintos roles posibles dentro del proceso dado a la heterogeneidad de la concurrencia al evento elegido. Por otro lado, en las entrevistas, se focalizó en gerentes de operaciones o sistemas, que tuvieran experiencia concreta en la generación de las prácticas, proceso y/o herramientas utilizadas. La recolección de datos se ha fijado en tres etapas principales:

1. Sistematizada (encuestas): Las encuestas fueron dejadas a disposición del público en un evento del mercado donde concurren varios cientos de personas a informarse, generar vínculos y realizar negocios. El perfil exacto de los encuestados se ignora, pero puede acotarse dentro de las categorías de personal de áreas operativas del sector de telefonía, personal de áreas de negocio vinculado con telefonía y representantes comerciales del sector telefonía. Se dejaron un total de 200 encuestas, de las cuales solo 29 fueron completadas. Esto no ha representado una limitación de alcance, al ser un estudio de naturaleza cualitativa.

   La herramienta, un cuestionario que cuenta de preguntas de elección múltiple cerradas y algunas abiertas fueron construidas para abarcar las temáticas mas relevantes del estudio (ver Anexo II. Guía de entrevistas a informantes-clave).

2. Semi-presencial del tipo formal (entrevistas semi-estructuradas) con informantes-clave: Las encuestas permitieron obtener datos con mayor detalle. La interacción persona a persona también dio lugar a la aparición de nuevos conocimientos que

fueron realimentados al marco teórico. Las entrevistas fueron realizadas en el período mayo a junio de 2016 de forma presencial con duraciones entre una y dos horas cada una (ver Anexo I. Encuesta a representantes de la industria). Como fue mencionado con anterioridad, los entrevistados fueron seleccionados intencionalmente, ya que se pretendía realizar charlas con profesionales reconocidos en el tema o que tuvieran amplia experiencia –presente o pasada– en la materia. Algunos de los profesionales elegidos fueron encontrados por recomendación de contactos en el sector, mientras que con otros ya existía una previa relación laboral común. Todas las entrevistas aportaron detalles interesantes de las problemáticas cotidianas con que conviven las empresas y el acercamiento que cada una decide para su resolución.

3. Análisis del caso: en el marco investigativo se presenta el caso de la empresa Negentel (también llamada NET) de Argentina. La elección de esta fue dada por dos factores principales: a. El conocimiento directo del presidente de la misma que aportó toda la información requerida y brindó acceso transparente a todos sus procesos. Sin una relación estrecha muchos de los datos no hubieran podido ser accedidos, en especial por contratos de confidencialidad que vinculan a la empresa con sus clientes. Para no viciar estos contratos, la información fue removida de los datos que permitieran identificar al cliente. b. El posicionamiento único que posee NET ofreciendo servicios tercerizados a empresas de comunicaciones en lo relacionado servicios de telefonía. La empresa ofrece un amplio rango de servicios consultivos (gestión de fraude, aseguramiento de ingresos, análisis de rentabilidad y otros) donde colabora en el día a día con diversos operadores de telefonía, por lo que se encuentra empapada en las costumbres –buenas y malas– que estas poseen. También brinda servicios llave en mano de la operación completa del servicio de telefonía para

empresas pequeñas. En este papel le toca a la empresa el rol de generar las prácticas, proporcionar el capital humano necesario y brindar las herramientas informáticas necesarias.

Fue analizada la información proporcionada por la empresa sobre el tema de estudio, su alcance, sus principales metodologías y procedimientos. Por último, este permitió, asimismo, aprender de la realidad empírica y dar soporte en modo más apropiado las recomendaciones y conclusiones finales de este estudio.

Finalmente, las tres etapas anteriormente mencionadas, se contrastaron con el fin de lograr una triangulación del fundamento investigativo, verificar la información aportada por las unidades de respuesta en cada herramienta a la realidad y el fundamento teórico del estudio, garantizando consistencia, confiabilidad y enriqueciendo a las conclusiones finales.

En el siguiente cuadro se resume lo expuesto anteriormente:

**Cuadro 1 - Metodología de la investigación**

| | |
|---|---|
| Tipo de investigación | Exploratorio descriptivo |
| Metodología | Cuali-cuantitativa |
| Diseño de la investigación | No experimental, transversal |
| Unidad de análisis | Gestión del fraude en empresas de telefonía |
| Muestra | Intencional, dirigida y no probabilística |
| Unidad de respuesta | Tomadores de decisiones dentro de los procesos gestión del fraude |
| Técnicas de recolección de datos | • Cuestionarios con preguntas abiertas y cerradas.<br>• Entrevistas presenciales a referentes del sector<br>• Caso de estudio. |

Fuente: Elaboración propia (2016)

# III. MARCO TEÓRICO

El Marco Teórico de la presente investigación desarrollará temáticas que se consideran necesarias a los efectos de comprender el problema analizado, sus antecedentes, sus soluciones actuales y sus tendencias. Se buscará encontrar los fundamentos del proyecto e integrar conocimientos relacionados con el fin de apoyar la investigación que se propone realizar. Los conocimientos obtenidos permitirán sentar las bases como para, luego, plantear soluciones al problema investigado.

De este modo, los ejes de investigación abarcarán:

- Origen, evolución y proyección de la telefonía: Se investigará brevemente el marco tecnológico que compone al servicio de telefonía tradicional y actual. Se complementará con el camino evolutivo que recorrió este servicio, quedando en evidencia sus falencias –específicamente ante el fraude– desde distintas perspectivas. Esto se completará con una proyección de la telefonía en particular y de los servicios de comunicación que han surgido como su competencia y, a la vez, potencial reemplazo.
- Tipos de fraude telefónico y su impacto: Basándose en distintos organismos se generará una tipología de fraudes. Todas las conductas fraudulentas tienen como punto en común buscar un beneficio extra para una parte y perjuicio para la empresa prestataria del servicio de telefonía.
- Modelación del fraude telefónico: Las llamadas telefónicas poseen ciertos atributos comunes en todas ellas. Por lo general el tráfico telefónico de abonados normales posee una caracterización distinta al del tráfico anómalo. Con ayuda de

investigaciones anteriores se definirá los posibles patrones que puede tener el tráfico telefónico originado por una actividad de fraude. Estos patrones permitirán implementar políticas reactivas para minimizar las pérdidas de la organización.

- Mejores prácticas para la prevención de fraude telefónico: Si bien no existen reglas obligatorias a cumplir por una empresa de telefonía en materia de prevención de fraude telefónico, varios investigadores, organismos y empresas privadas han delineado mejores prácticas a seguir. Se propone investigar, conciliar y proponer un conjunto de prácticas a seguir que abarquen lo aprendido en los anteriores apartados, en especial el establecimiento de patrones de fraude telefónico y su detección mediante técnicas estadísticas y minería de datos. Estas técnicas son especialmente útiles para la industria telefónica.

## III. 1 Origen, evolución y proyección de la telefonía

### Historia de la telefonía

El telégrafo fue el invento revolucionario original que cambió las comunicaciones entre personas. Éste dio lugar luego al teléfono y juntos cambiaron la forma en que la gente se comunicaba y hacía negocios (Burton, 2005). El primer teléfono fue construido por Antonio Meucci en 1857 para comunicar su cuarto con el de su esposa enferma. Más tarde, la invención fue registrada por Alexander Graham Bell en el año 1876[1]. Patentada en los Estados Unidos describía a las comunicaciones telefónicas como la conversión de la voz humana a señales eléctricas para ser transmitidas -luego- a través de un medio metálico el que conducía la señal eléctrica hasta el destinatario final. En el destino, la señal eléctrica se convertía -nuevamente- a una señal sonora, la cual era escuchada por el oído humano.

[1] Patente US 174465. Recuperado del sitio web de la oficina de patentes de los Estados Unidos de América http://patft.uspto.gov/ el día 10/05/2016.

Wheen (2011) desarrolla los distintos estadios tecnológicos que llevaron, a través de los últimos 170 años, del simple invento de Morse a la red de comunicaciones global que fue denominada como Internet. Una pequeña línea de tiempo de los sucesos fundacionales se describe a continuación:

- **1877**. Se comienzan a comercializar los primeros equipos telefónicos. Estos trabajaban de a pares con un tendido telefónico dedicado entre los lugares que intercomunicaban.
- **1878**. Se introduce el primer conmutador telefónico. Los usuarios del servicio telefónico poseían líneas dedicadas entre su domicilio y el conmutador. En el conmutador una serie de trabajadores, denominados operadores, enlazaban manualmente el origen y destino de las comunicaciones.
- **1892**. Strowger desarrolla la central de telefónica con conmutación automática, necesitando solamente operadores humanos para las llamadas de larga distancia. Durante las siguientes décadas se desarrollan redes de telefonía en cada país. Se adopta un diseño jerárquico con centrales locales, regionales y centrales que permiten interconectar a cualesquiera dos abonados del servicio entre ellos.
- **1896**. Se introduce el disco rotativo para la marcación de números telefónicos.
- **1901**. Marconi realiza la primera transmisión inalámbrica de telégrafo entre Europa y América. En 1927 se comenzaron a realizar comunicaciones telefónicas inalámbricas intercontinentales.
- **1956**. Mediante cables y amplificadores submarinos se logra la primera llamada intercontinental.

- **1960s**. Gracias a los trabajos anteriores de Harry Nyquist (1928), Alec Reeves (1937) y Claude Shannon (1948) se desarrollan las comunicaciones digitales. La voz humana deja de ser transmitida como una señal electromagnética analógica y comienza a ser transmitida como una representación digital (PCM). Se introduce el concepto de "bit".
- **1969**. El Departamento de Defensa de EEUU desarrolla la red ARPANET[2] con la intención de unir varias computadoras existentes mediante la red de telefonía.
- **1973**. Vint Cerf y Robert Khan desarrollan el protocolo TCP/IP que sería adoptado como piedra fundacional de Internet.
- **1984**. La empresa Motorola lanza al mercado el primer dispositivo de telefonía celular: DynaTAC 8000X. El servicio móvil, diseñado originalmente para automóviles, comienza rápidamente a ser de uso masivo.
- **1987**. Se introduce el concepto de ADSL (Asymmetric Digital Subscriber Line) que utiliza el cableado telefónico existente para brindar acceso a Internet dedicado.
- **1995**. La empresa VocalTec comienza a ofrecer servicio de telefonía por Internet iniciando el desarrollo de la tecnología VoIP (*Voice over IP*)[3].

Según la opinión de Burton (2005), a pesar de todos los citados avances anteriores, la forma de comunicarse a distancia y la arquitectura de comunicaciones se han mantenido básicamente similares durante el proceso evolutivo descrito, con una red centralizada de

[2]**ARPANET** fue una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales.
[3]**VoIP** (Voz sobre protocolo de internet) es un conjunto de recursos y protocolos que hacen posible la señal de voz viaje a través de Internet en formato de datos.

comunicaciones, equipamientos intermedios que realizan conexiones orientadas a circuitos entre llamantes y terminales “bobas” de voz en los extremos para los usuarios.

### Seguridad y privacidad en la telefonía tradicional

Por lo general todas las redes de comunicaciones son concebidas y diseñadas sin tener en cuenta la seguridad del servicio. Isomäki (1999) comenta sobre seguridad en redes de comunicación que:

- La atmósfera social y política en la que se formaron las primeras redes de comunicaciones es ciertamente distinta la atmósfera donde se formaron las más recientes como Internet. Las fundamentos tecnológicos de la telefonía tradicional descansan en que las terminales son simples o “bobas”, el equipamiento encargado de conmutar las llamadas entre origen y destino es complejo y los operadores telefónicos son grandes monopolios regulados por el gobierno local. Los protocolos de comunicaciones encargados del diálogo entre equipamiento han sido desarrollados en secreto por organizaciones y, aún al día de hoy, existen detalles que no son accesibles públicamente.

- Es de público conocimiento que el servicio de telefonía fija no implementa ningún mecanismo criptográfico para proteger el canal de voz, por lo que la seguridad de las llamadas se basa enteramente en la premisa que un intruso no podrá acceder físicamente a la red (sea el equipamiento o el cableado) telefónica. En la última milla, o sea el segmento del servicio entre el equipamiento del operador telefónico y el abonado residencial, la identificación del abonado se basa enteramente en la confianza que la llamada se origina del conector físico donde se le entregó el servicio.

- Por otro lado, el abonado no tiene forma de saber si está utilizando el servicio de su operador o si éste fue sustituido por un tercero. De igual manera, dentro de la red telefónica misma del operador, ninguno de los protocolos encargados de encaminar las llamadas entre origen y destino fueron diseñados para proveer autenticación, integridad o confidencialidad. El protocolo utilizado para esta tarea, SS7[4], posee un especificación tan ambigua y generalista que en la práctica cada país, operador telefónica y fabricante de equipamiento genera variantes propias.

- Aún en redes más modernas como la red de telefonía celular GSM, que incorpora mecanismos criptográficos, el diseño sigue siendo centralizado y basado en la confianza mutua entre el aparato terminal del abonado y la red que le brinda servicio. Adicionalmente, todas las llamadas realizadas entre dos operadores móviles se realiza a través de la red de telefonía fija, por lo cual todas las vulnerabilidades inherentes a la telefonía fija también aplican para dichas comunicaciones.

### Las nuevas tecnologías de comunicaciones

Gunatilaka (2016) explica que durante la última década se ha dado origen a una vertiginosa aparición de nuevas tecnologías de comunicación telefónica, mensajería instantánea, videoconferencia y redes sociales. Zhang, Sun, Zhu y Fang (2010) ratifican que las nuevas tecnologías de comunicación ofrecen grandes ventajas en materia de seguridad, pero también incorporan nuevas amenazas, entre las que se puede citar: robo de identidad, vulneración del anonimato, pérdida de la privacidad, ataques de *hackers* a sitios de redes sociales, expansión

[4] Definida en la recomendación Q.700 (03/93) de la ITU (International Telecommunication Union).

de ataques por *malware*[5]en las terminales de usuarios, entre otros ejemplos. Es así como la forma de comunicación entre personas muta constantemente y cada año aparecen nuevas empresas que ofrecen nuevos paradigmas de comunicación. Entre ellas se pueden citar: Skype (fundada en 2003), Facebook (fundada en 2005), Whatsapp (fundada en 2009) y Periscope (fundada en 2015).

Según publica Castells (2014), en noviembre de 2007 el tiempo global anual utilizado en redes sociales sobrepasó al tiempo global anual utilizado en correo electrónico y el número global de usuarios de redes sociales sobrepasó al número global de usuarios de correo electrónico en julio de 2009. Considerando que el primer correo electrónico fue enviado en 1971 y la primer red social[6] fue lanzada en 2002, los tiempos de adopción de nuevas tecnologías se han acortado progresivamente. Los portales de redes sociales ofrecen a sus usuarios formas de comunicación e interacción para todas las actividades, desde relaciones personales a actividades de negocios. En la misma línea, el reporte de Radicate Group (2015) utiliza datos de 1993 a 2005 para predecir un crecimiento global muy moderado del uso del correo electrónico de tan solo un 3% anual por los próximos 5 años. Finalmente, Castells (2014) considera que debido a la creciente facilidad de los usuarios en interactuar mediante redes sociales específicamente, y mediante la web en general, los comercios, gobiernos, negocios y hasta la sociedad civil misma se encuentran masivamente en proceso de migración de su estructura a un formato online. Para acentuar la velocidad de progreso, y el abandono relacionado, de tecnologías deja asiento que aquellos usuarios que pertenecen a la generación de los Millenials directamente desconocen el uso de los aparatos telefónicos con disco.

[5] Tipología de software que comprende a aquellos códigos que tienen como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.
[6]Friendster.

## El futuro de la telefonía

En este orden de ideas, varios medios especializados consideran que la telefonía tradicional es una tecnología que tiene sus días contados por su experiencia de usuario limitada frente a nuevas tecnologías en constante expansión y aparición.

Singhal (2010) opina que en 10 años el servicio telefónico podría ya no existir. Comparándolo con servicios como Google Voice o Skype, encuentra que la experiencia de la telefónica clásica es muy limitada para los usuarios actuales. Adicionalmente, su utilización se encuentra atada a un cierto dispositivo (móvil o fijo), versus los servicios que emplean redes IP[7] que pueden ser consumidos desde cualquier parte del mundo con cualquier equipamiento con solo poseer conexión a Internet.

Ferro (2016) publica un análisis sobre las prácticas colaborativas actuales en ambientes altamente informatizados y las tecnologías de comunicación que mejor las acompañan. En este análisis afirma:

- Las conferencias de audio o video son sólo preferidas por audiencias de mayor edad (superiores a 40 años), pero se advierte además que esta clase de reuniones virtuales son en general disruptivas del trabajo, dado que poseen muchos tiempos muertos para los participantes y además bloquean al recurso humano durante un determinado período.

[7] Redes de datos basadas en el protocolo TCP/IP entre las que se encuentra Internet.

- Existe mayor valor en formas de comunicación asincrónicas o que no establezcan vínculos “uno a uno” en tiempo real. Citando el ejemplo del correo electrónico, aparecen los siguientes beneficios:
    - Comunicación de uno frente a muchos;
    - Participación silenciosa;
    - Posibilidad de compartir otros tipos de información;
    - Posibilidad de responder e interactuar de acuerdo a la agenda horario de cada participante.

  Similares beneficios existen para canales como el *WebChat* o la herramienta colaborativa Slack[8]. En su opinión los servicios de telefonía se convertirán en negocios de nicho donde los principales clientes serán empresas corporativas.

Por el contrario, White (2016), afirma que aún cuando la telefonía no sea una industria en crecimiento o una industria de moda esto no implica su rápida extinción. También brinda paralelos con otros servicios que si bien han disminuido por un reemplazo, permanecen como servicios de nicho.

En concordancia con lo anterior, Hollingsworth (2016) explica que aún existen grandes verticales de negocios (donde él incluye: hospitales, abogados, sectores financieros, farmacias, clínicas médicas, entre otros) que necesitan servicios telefónicos tradicionales para ser contactados. Su predicción se basa en la dificultad que experimentan estas empresas al intentar cambiar sus canales de relacionamiento clásicos con usuarios o clientes, por canales modernos de *WebChat*, muro de Facebook o correo electrónico. La existencia de tan diversas formas de contactación, la carencia de centralización y la falta de estandarización implican

[8]**Slack** es una herramienta de comunicación en equipo lanzada al mercado en 2013. Su sito oficial es https://slack.com/

que al momento de un usuario decidir contactar a una empresa debe pasar tiempo extra decidiendo cuál es la mejor o cuáles están disponibles en ese momento. Esto sucede con más impacto en las formas de comunicación asincrónicas, como los mensajes generados a través de la aplicación Whatsapp. El autor introduce la dificultad de realizar ciertos procesos por canales asíncronos. Uno de ellos es el proceso de ventas. Después del contacto persona a persona, la comunicación verbal es la mejor forma de vender un producto. Un contacto en frío mediante un correo electrónico o un mensaje de SMS posee un nivel mucho más bajo de movilización emocional por parte del receptor. Hollingsworth (2016) cierra su informe indicando que la mayoría de los *Call Centers* siguen manejando campañas de ventas mediante canales telefónicos y que aún es difícil encontrar métricas para medir la productividad con otros canales.

En contraria opinión, Spencer (2009) analiza la reducción de usuarios del servicio telefónico fijo y afirma:

- Para 2025 no existirán líneas tradicionales de telefonía fija. Realizando una analogía con la industria del periódico impreso, vaticina que este último dejará de existir en Norteamérica alrededor del año 2043. Las operadores de servicios de telefonía fija sufren una pérdida constante de clientes que abandonan su servicio para convertirse en los denominados CPOs (*cellphone-onlys*), es decir, aquellas personas que sólo poseen un teléfono móvil para realizar o recibir llamados. Esto se refleja en la deserción de usuarios al servicio que para los EEUU, en 2009, fue de 700.000 mensual.

- Realizando un análisis de negocio sobre el fenómeno, pronostica que la reducción de usuarios ocasionará que el costo operativo fijo de mantener la red de telefonía sea distribuido en un menor número de abonados, incrementado su valor.
- También advierte que la disminución de usuarios de telefonía fija pone en peligro la operatividad de muchos servicios críticos como la policía y bomberos. Estos descansan en poder identificar la localización geográfica de una llamada de auxilio basándose en el número de abonado de telefonía fija. Por el contrario, cuando una llamada se origina desde un teléfono móvil o desde un teléfono provisto en tecnología VoIP el origen geográfico de la misma puede ser desconocido. Ante este escenario es probable que los gobiernos se vean obligados a comenzar a subsidiar las redes de telefonía fija o que incluso deban crear impuestos que desalienten el uso de la telefonía móvil.
- En síntesis, los servicios de telefonía fija no pueden desaparecer de la noche a la mañana sin un gran impacto, y su disminución no es solo un problema para las empresas de telecomunicaciones, sino para los gobiernos y la sociedad civil.

Por su parte, Yager II (2011), especialista en gestión de empresas en Morris Anderson, explica que desde 2006 existe un proceso constante de sustitución de líneas telefónicas tradicionales por otras tecnologías de comunicación, donde empresas de telefonía móvil o cableoperadoras comienzan a captar clientes del servicio telefónica tradicional. La posesión de la llamada "última milla" (el cableado físico desde el operador hasta el abonado final) está rápidamente dejando de ser un patrimonio estratégico para los grandes operadores. Esta barrera que históricamente impedía que otros servicios compitieran en el territorio del operador local, cada día se hace cada vez más baja. También nota que el mercado de telecomunicaciones de los EEUU ha sufrido una gran consolidación a grandes empresas y

una convergencia de servicios de datos, video y voz. La telefonía tradicional orientada a circuitos se ve rápidamente reemplazada por tecnologías de paquetes como VoIP. Yager II (2011) afirma que en 30 años "Los teléfonos todavía sonarán y las personas seguirán hablando entre ellas, pero las empresas de telefonía tradicional, los titanes de la industria de las últimas décadas, ya no estarán".

Es así como el servicio de telefonía evoluciona según los requerimientos del mercado y las tecnologías que van desarrollándose. Dodd (2012) afirma que un gran número de empresas ha comenzado a mudar sus sistemas telefónicos a servicios en la nube (*hosted services*) mediante tecnología VoIP. En este servicio el proveedor con tecnología VoIP mantiene el procesamiento y servicios de valor agregado (buzón de correos, salas de conferencia, IVR[9], entre otros) en su propio centro de datos, mientras que sólo entrega al cliente los aparatos terminales, los cuales pueden ser usados desde cualquier parte del mundo con solo poseer conexión a Internet. Dodd (2012) continúa su exposición afirmando que el paradigma de la Comunicación Unificada (*Unified Communications*) se encuentra en amplia adopción. Aquellas implementaciones de Comunicación Unificada integran el correo electrónico, llamadas telefónicas, mensajería instantánea y otros servicios de colaboración en una sola interfaz de usuario.

Es por las razones expuestas a lo largo de este trabajo que a pesar de la proliferación de nuevas empresas y nuevas formas de comunicación, la telefonía sigue siendo utilizada por gran cantidad de usuarios locales y del mundo. A continuación se reproducen informes relativos a la industria de telecomunicaciones. Según el informe anual del laCellular Telephone Industries Association (2014), en el año 2013 se cursaron 2.6 trillones de minutos

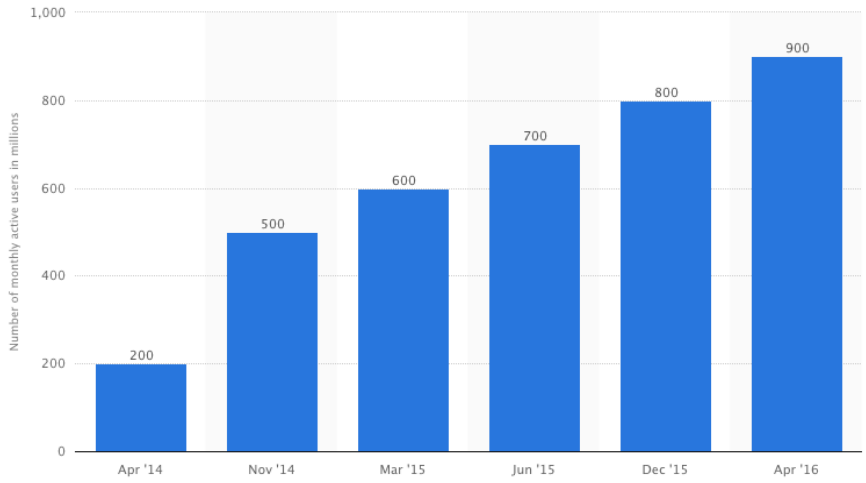
[9]**IVR (Interactive Voice Response)** sistema telefónico capaz de recibir una llamada e interactuar con el humano a través de grabaciones de voz y el reconocimiento de respuestas.

telefónicos globales, frente a 2.3 trillones de minutos en 2012. Esto es un crecimiento del 13% interanual que si bien es menor a los crecimientos de otros medios de telecomunicaciones como Whatsapp Messenger (400% de aumento en período 2013-2015)[10] o Facebook Messenger (450% de aumento en período 2014-2016)[11] muestra aún una industria en crecimiento.

**Gráfico 1 - Crecimiento usuarios de aplicación Whatsapp (período 2011 – 2014)**


Fuente: Portal de estadísticas: Statista (http://www.statista.com)

**Gráfico 2 - Crecimiento usuarios de Facebook Messenger (período 2014 – 2016)**




Fuente: Portal de estadísticas: Statista (http://www.statista.com)

[10] Valores obtenidos de estadisticas del sitio web Statista http://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ el día 01/05/2016.
[11] Valores obtenidos de estadisticas del sitio web Statista http://www.statista.com/statistics/417295/facebook-messenger-monthly-active-users/ el día 01/05/2016.

Un indicador local de importancia se obtiene de la ex Comisión Nacional de Comunicaciones (CNC) -actual Ente Nacional de Comunicaciones (ENACOM)-. Este organismo argentino informa periódicamente las estadísticas de servicios de telefonía fija, pública, móvil e internet. En el informe del ENACOM (2013) se observa para la telefonía fija un crecimiento mínimo y sostenido desde el año 2008 y luego, en el año 2012, adviene una caída de aproximadamente del 2,5% en el total de líneas instaladas. Por el contrario, en el mismo período, para la telefonía móvil se visualiza que la media va desde 120 a 156 líneas por cada 100 habitantes. Sobre la telefonía móvil el informe comenta "Siguiendo la tendencia mundial, desde sus inicios y sobre todo en la última década, se produjo un crecimiento explosivo de los servicios móviles, al mismo tiempo que la diversidad de sus aplicaciones y funciones derivadas ha impulsado su aumento exponencial en cuanto a su utilización" (p,38). El informe posee varios cuadros reproducidos a continuación que muestran la variación poblacional de los servicios discutidos.

**Cuadro 2 - Crecimiento líneas fijas instaladas en La Argentina (período 2008 – 2012)**

| Año | líneas instaladas | Var. % interanual | líneas en servicio | Var. % interanual |
|---|---|---|---|---|
| 2008 | 10.752.893 | | 9.343.701 | |
| 2009 | 10.952.112 | 1,85% | 9.419.513 | 0,81% |
| 2010 | 11.101.925 | 1,37% | 9.515.273 | 1,02% |
| 2011 | 11.324.065 | 2,00% | 9.635.163 | 1,26% |
| 2012 | 11.043.897 | -2,47% | 9.337.910 | -3,09% |

Fuente: ESTADÍSTICAS E INDICADORES DE TELECOMUNICACIONES ARGENTINA Serie 2008 - 2012. Nacional Comisión de Comunicaciones. Pagina 9.

**Cuadro 3 - Crecimiento llamadas de telefonía fija en La Argentina (período 2008 – 2012)**

| Telefonía fija - Cantidad de llamadas (en miles) | | | | |
|---|---|---|---|---|
| Año | urbanas | interurbanas | internacionales | Total |
| 2008 | 12.452.529 | 1.942.588 | 63.416 | 14.458.533 |
| 2009 | 12.142.332 | 2.062.662 | 58.416 | 14.263.410 |
| 2010 | 11.906.336 | 2.058.046 | 60.935 | 14.025.317 |
| 2011 | 11.444.045 | 2.019.375 | 62.779 | 13.526.199 |
| 2012 | 10.921.075 | 2.066.672 | 67.601 | 13.055.348 |

Fuente: ESTADÍSTICAS E INDICADORES DE TELECOMUNICACIONES ARGENTINA Serie 2008 - 2012. Nacional Comisión de Comunicaciones. Página 30.

**Cuadro 4 - Crecimiento líneas móviles en La Argentina (período 2008 – 2012)**

| AÑO | CANT. DE LINEAS | LINEAS C/ 100 HAB |
|---|---|---|
| 2008 | 47.577.743 | 119,71 |
| 2009 | 54.083.453 | 134,76 |
| 2010 | 58.196.197 | 143,63 |
| 2011 | 60.722.729 | 148,46 |
| 2012 | 64.327.647 | 155,83 |

Fuente: ESTADÍSTICAS E INDICADORES DE TELECOMUNICACIONES ARGENTINA Serie 2008 - 2012. Nacional Comisión de Comunicaciones. Pagina 41.

Si bien el servicio de telefonía fija se contrae o, en el mejor de los casos se mantiene constante, la telefonía móvil continúa en aumento, logrando que el servicio de comunicación de voz siga en crecimiento. Indicadores similares pueden observarse en otros países como Chile, cuya información estadística se encuentra reflejado en el Anexo V.

### Conclusiones del apartado

El siguiente cuadro refleja las posiciones de los distintos autores sobre el futuro de la telefonía.

**Cuadro 5 - Origen, evolución y proyección de la telefonía**

| | Organismos de estadísticas: CNC, CTIA y Statista | Tom Hollingsworth | Markus Isomäki |
|---|---|---|---|
| 1 | Las comunicaciones telefónicas mediante teléfonos fijos decrecen anualmente. | Existen verticales de negocios y servicios que no pueden migrarse fácilmente a nuevas tecnologías | Las redes de comunicaciones tradicionales son inherentemente inseguras. |
| 2 | Las comunicaciones telefónicas desde teléfonos móviles crecen anualmente. | Las nuevas tecnologías de comunicación son dispares, heterogéneas y poco normalizadas. | |
| 3 | Otras tecnologías de comunicación tienen crecimiento muy superior durante los mismos períodos. | No prevé la desaparición de los servicios de telefonía tradicional por muchas décadas por delante. | |

Fuente: Elaboración propia (2016).

Lo anteriormente expuesto permite sostener que la telefonía seguirá existiendo por los siguientes años y consecuentemente sus problemas deben seguir siendo abordados con la mayor seriedad dado los volúmenes de dinero que su industria aún moviliza. Existen muchos indicadores que muestran que la telefonía fija finalmente desaparecerá gradualmente y que será reemplazada en su mayor parte por la telefonía móvil, pero este no es un escenario de cercano o mediano plazo. Esta información indica que las formas y relaciones de comunicación entre personas están experimentando grandes cambios, en gran medida motivadas por nuevos paradigmas tecnológicos. Estos nuevos paradigmas reemplazarán con

el tiempo una parte de volumen comunicacional que en el presente se realiza mediante comunicaciones telefónicas (fijas o móviles). Nuevas tecnologías de comunicación pueden seguir siendo introducidas en el futuro e irán brindando un valor agregado mayor respecto a una llamada telefónica tradicional, pero su aparición espontánea, heterogeneidad, falta de regulación y no estandarización, impedirán que sean reemplazos naturales de la telefonía clásica en el intervalo de tiempo analizado.

### III. 2 Tipologías de fraude telefónico

Este apartado desarrollará las clasificaciones, definiciones e impacto de cada tipología de fraude en el sector de las telecomunicaciones.

#### Enumeración de los escenarios de fraude de mayor ocurrencia

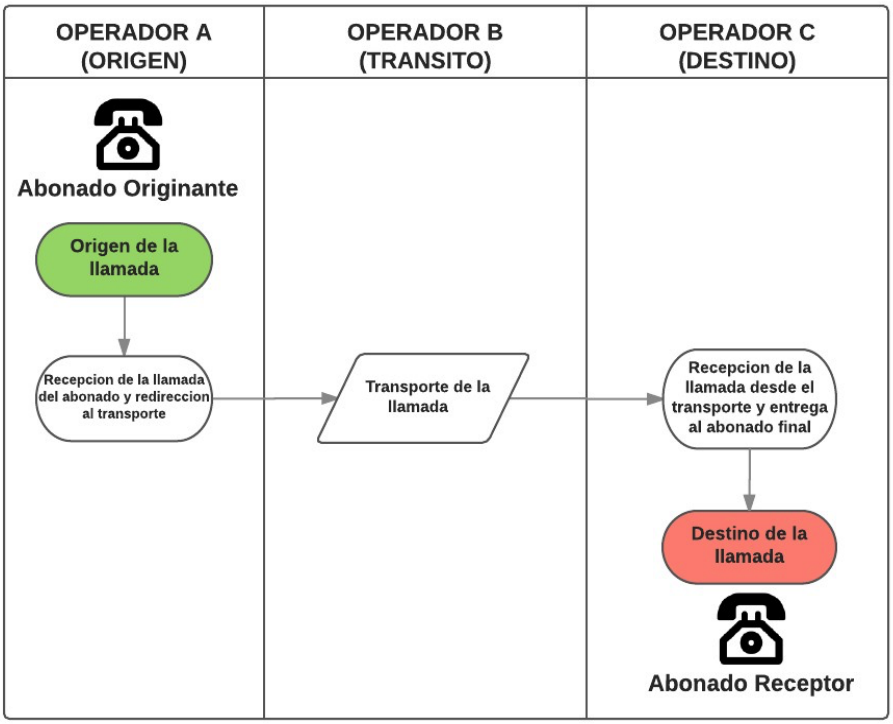
Tomando como base las definiciones del I3 Fórum (2014) y el trabajo de Howells, Scharf-Katz, Volkmar y Stapleton (2014) se generó una tipología de los fraudes más comunes en el mercado telefónico. El factor común de todas estas conductas fraudulentas consiste en tener, por un lado, un beneficio extra para un actor y, por el otro lado, causar un perjuicio para otro actor o actores.

- **Secuestro de llamadas**. También denominado *blueboxing* o manipulación del plan de numeración.

  En este escenario el origen de la llamada se genera en la red de telefonía del operador A y tiene como destino la red de telefonía del operador C, para lo cual se utiliza como intermediario la red de telefonía del operador B. El operador B, que debería servir como tránsito entre origen y destino cobra una tarifa pactada al operador A para llevar

sus llamadas hasta el operador C. El flujo normal de una llamada se ilustra en el siguiente cuadro.

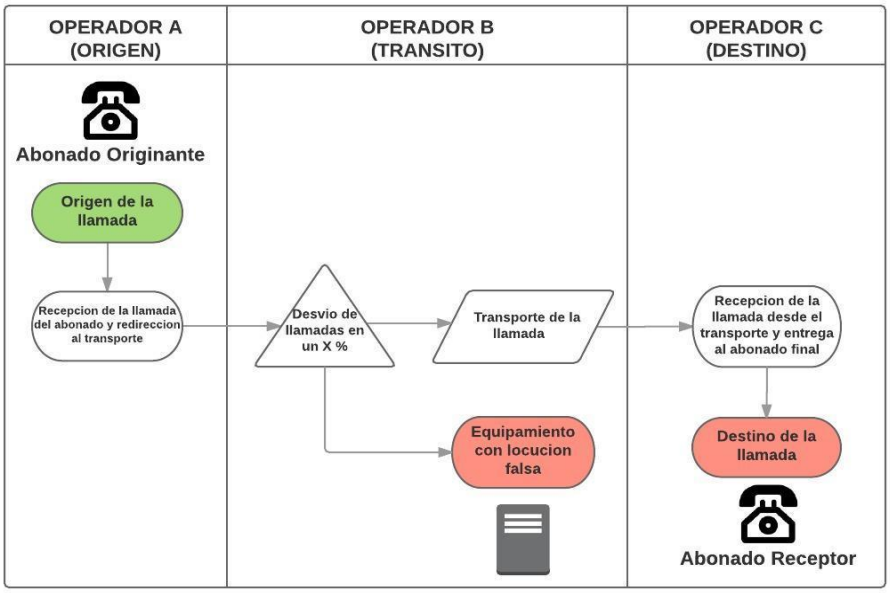
**Figura 2 - Flujo de una llamada telefónica normal**




Fuente: Elaboración propia (2016)

En este ambiente se genera fraude cuando el operador de tránsito B decide maliciosamente redireccionar un porcentaje de estas llamadas a algún equipamiento propio que atienda dichas llamadas con alguna locución pregrabada. Con este accionar el operador B cobra al operador A por llamadas que nunca llegan a su destino verdadero y que, por lo general, no poseen costo alguno para él. El flujo fraudulento se ejemplifica en el siguiente cuadro.

**Figura 3 - Flujo de una llamada telefónica víctima de "*blueboxing*"**




Fuente: Elaboración propia (2016)

Si el porcentaje de llamadas que son desviadas al servidor de la locución se mantiene a niveles bajos esto puede pasar desapercibido durante largos períodos por el operador A, quien pagará -y al mismo tiempo cobrará a su cliente- por llamadas atendidas falsamente.

El I3 Forum (2014) identifica los siguientes beneficiarios y perdedores en este escenario:

¿Quién gana?

El operador de tránsito B, que aumenta su ganancia en un porcentaje directamente proporcional a las llamadas que desvía internamente.

¿Quién pierde?

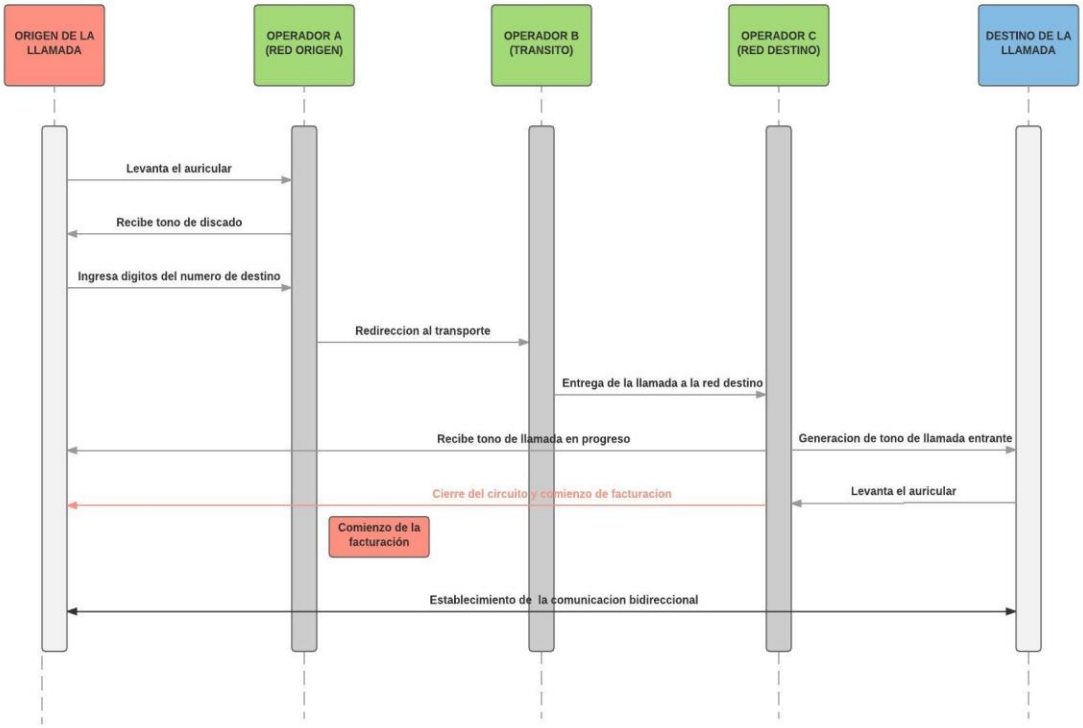
El cliente o usuario que generó la llamada y en consecuencia recibe cargos por servicios finalmente no concretados.

El operador A, que recibió la llamada del usuario y decidió usar al operador B, con quien posee una relación comercial, como tránsito.

- **Falso establecimiento de llamadas** - también denominado FAS (*False Answer Supervision).*

Una llamada telefónica comienza su tarifación desde el momento en que el destinatario de la misma la atiende. Toda la etapa anterior al establecimiento no genera cargos para el usuario que inició la llamada ni tampoco para los operadores de telefonía intermediarios. Por lo general, mientras se espera que el otro extremo de la llamada atienda la línea, se genera una señal sonora que indica al abonado originante que la llamada está aún en progreso de establecimiento. Estas señales se ajustan a la Recomendación E.180 de la ITU (03/1998). Para el caso de la Argentina es un tono de 425Hz con una cadencia de 1 segundo para el tono y 4 segundos de silencio.

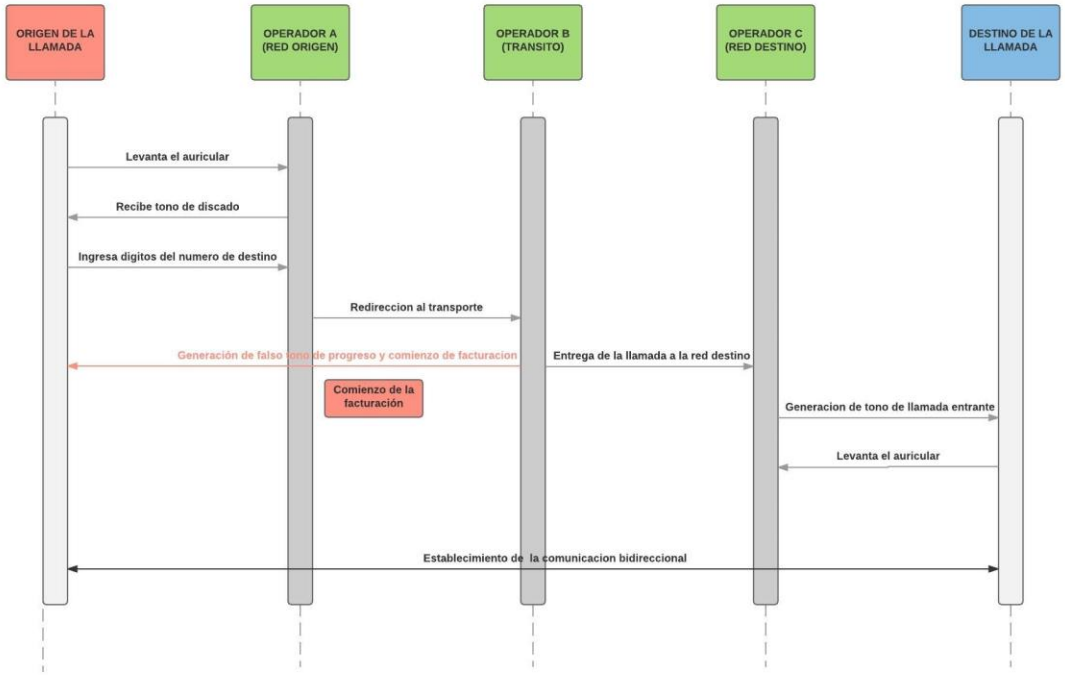
**Figura 4 - Fases una llamada con un establecimiento normal**




Fuente: Elaboración propia (2016)

Este escenario de fraude se basa en el establecimiento prematuro de la llamada por alguno de los operadores de telefonía intermedios y la generación de una falsa señal sonora de progreso de llamada hacia el origen. De esta forma la llamada es tarifada por un período mayor al verdadero tanto al Operador A como al abonado originante. En esencia, es posible que existan llamadas que finalmente nunca son atendidas por ausencia del destinatario y que también son tarifadas.

**Figura 5 - Fases de una llamada con falso establecimiento**




Fuente: Elaboración propia (2016)

El I3 Forum (2014) identifica los siguientes beneficiarios y perdedores en este escenario:

**¿Quién gana?**

El operador de tránsito que establece prematuramente el llamado y genera una falsa señal sonora. Este operador percibe ganancias superiores por la mayor duración de la llamada.

**¿Quién pierde?**

El cliente o usuario que generó la llamada que recibe cargos por servicios finalmente no concretados.

También pierde el operador A que recibió la llamada del usuario y decidió usar al operador B, con quien posee una relación comercial, como tránsito.

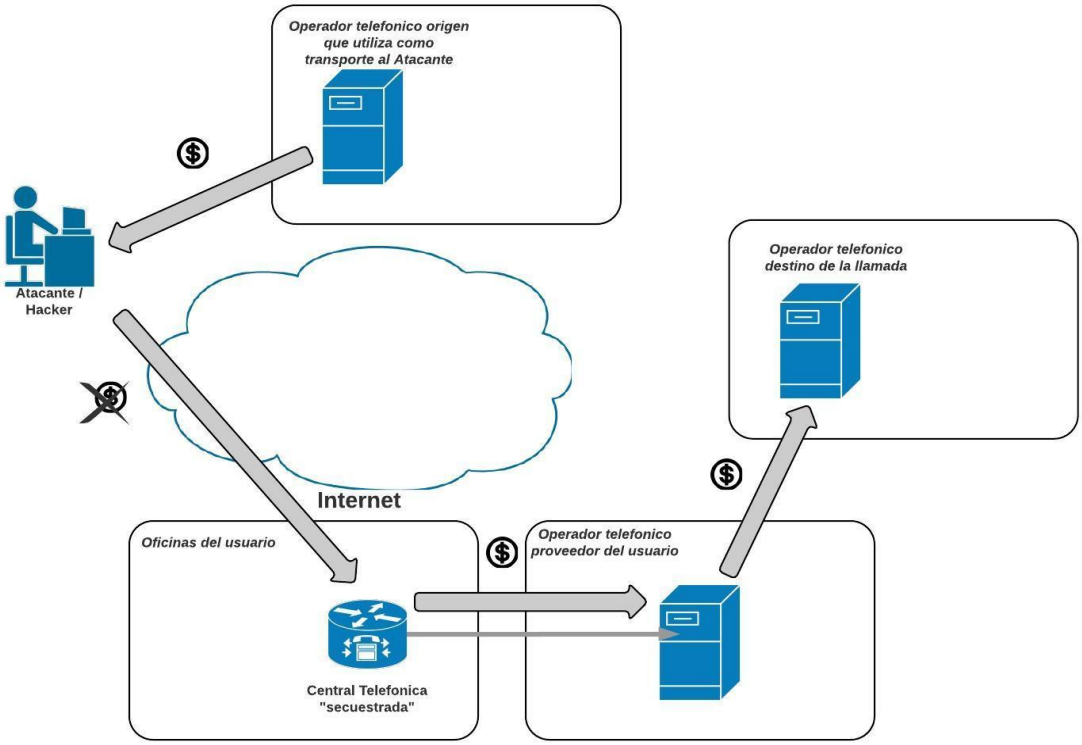
- **Secuestro o *hacking*** de la central telefónica de un usuario.

  En este escenario un atacante realiza una intrusión remota a una central telefónica de un usuario o abonado final. Las técnicas para lograr este objetivo son diversas, entre las cuales podemos encontrar las siguientes modalidades:

  1. Utilización de técnicas de fuerza bruta para adivinar contraseñas del la central telefónica del usuario;
  2. Explotación de malas configuraciones que permiten a intrusos generar llamadas a través de la central telefónica del usuario;
  3. Explotación configuraciones de fábrica que permiten tener acceso la central telefónica del usuario.

  El usuario no es consciente de lo que sucede con su equipamiento. Cuando un equipo es afectado, el atacante envía altos volúmenes de llamadas y, por lo general, a países cuyas tarifas son elevadas. El origen del tráfico telefónico por lo general es de operadores que no saben que el atacante ha cooptado maliciosamente un recurso no propio. El flujo de estas llamadas pueden representarse de la siguiente forma.

**Figura 6- Flujo de una llamada cursada por un secuestrador o *hacker***




Fuente: Elaboración propia (2016)

En este escenario de fraude y a diferencia del resto, el usuario final recibe facturación por parte de su operador telefónico por grandes sumas.

El I3 Forum (2014) identifica los siguientes beneficiarios y perdedores en este escenario:

¿Quién gana?

El intruso o hacker que vulnera el sistema telefónico del usuario y mediante esa maniobra que obtiene un servicio sin pago correspondiente.

¿Quién pierde?

El cliente o usuario cuyo equipamiento se vio afectado por el secuestro.

En ciertos casos el operador telefónico que da servicios al usuario vulnerado debe compartir la pérdida. En especial cuando los montos son elevados y el usuario se encuentra imposibilitado de afrontarlos.

- **Fraude sobre números internacionales con participación de ingresos (*revenue share*):**

Las tarifas de llamadas telefónicas a las distintas regiones o países del mundo no son todas iguales. Existen países que por su situación geográfica o regulatoria poseen valores mucho más altos. En el Anexo III puede verse una lista de costos expresada en segundos de comunicación para distintos geográficos. En esta se puede notar la gran dispersión de costos – y por lo tanto también de precios de venta – que existe. Por ejemplo, el Reino Unido posee un valor de 0.000038152 dólares estadounidenses por segundo, mientras que en otros países como Surinam (0.00562 dólares estadounidenses por segundo), Cuba (0.013125 dólares estadounidenses por segundo) o Senegal móvil (0.00545 dólares estadounidenses por segundo) el costo de la llamada es mas de cien veces el valor del mismo servicio al Reino Unido.

La existencia de destinos de tan alto valor genera la aparición de este escenario de fraude debido a las elevadas sumas que el defraudador puede generar en cortos intervalos de tiempo. Siguiendo el los mismos ejemplos anteriores, un fraude con numeración de Surinam genera 147 veces mas rápido el mismo dinero que un fraude con numeración del Reino Unido.

En este escenario el defraudador renta números a uno de los operadores telefónicos locales en alguno de estos países que presentan valores elevados en el precio de sus llamadas. El defraudador posee un acuerdo de participación en los ingresos con el operador, también denominado en inglés "*revenue share*". Mediante este acuerdo el defraudador recibirá parte de las ganancias que el operador local cobra por recibir llamadas desde el exterior a los números rentados. El escenario de fraude se completa con el defraudador generando tráfico telefónico internacional a estos números mediante alguno de los siguientes métodos:

- ❏ Secuestro o *hacking* de la central telefónica de un usuario.
- ❏ Robo o falsificación de tarjetas SIM de teléfonos móviles locales.
- ❏ Robo de tarjetas SIM de teléfonos móviles de extranjeros que posean itinerancia (*roaming*).
- ❏ Engaño a usuarios.
- ❏ Redirección de llamadas.

El I3 Fórum (2014) identifica los siguientes beneficiarios y perdedores en este escenario:

<u>¿Quién gana?</u>

El receptor de la llamada y dueño del número de internacional de alto valor.

El defraudador que comparte la ganancia obtenida por el receptor de la llamada.

<u>¿Quién pierde?</u>

Usuarios finales engañados en discar números de alto costo internacional.

Usuarios finales víctimas del secuestro de su central telefónica.

- Arbitraje

  El arbitraje telefónico puede formarse de varias formas. Una de estas sucede con la existencia de planes residenciales con tarifas planas. Dichos planes ofrecen al usuario una tarifa fija a cambio de llamadas ilimitados. Los planes de tarifas planas son generados y calculados teniendo en cuenta patrones normales de llamados telefónicos de usuarios promedio, tanto en volumen de llamadas como en sus destinos.

  Los defraudadores suelen investigar activamente el mercado residencial para encontrar estas ofertas comerciales. Cuando estos productos ofrecen deficiencias en su armado que los exponen a un arbitraje, los defraudadores los utilizan para generar llamadas por volumen o a destinos que exceden el racional comercial con el que fueron diseñados.

  El I3 Forum (2014) identifica los siguientes beneficiarios y perdedores en este escenario:

  ¿Quién gana?

  El defraudador que explota operaciones de compraventa que permiten arbitraje.

  ¿Quién pierde?

  La empresa telefónica que ofrece tarifas por debajo de valor de mercado o con planes de negocio que permiten arbitraje.

Además de los informes utilizados, diversas empresas de comunicaciones realizan publicaciones informando distintos escenarios donde un perpetrador de fraude puede realizar su actividad. La empresa Telsis (2015) resume algunos de los fraudes más comunes. A los anteriores listados agregan:

- **Fraude mediante teléfonos públicos**.
- **Wangiri**. El objetivo de este ardid es generar llamadas perdidas a celulares mostrando como origen números *premium* o internacionales. El receptor de la llamada es engañado en devolver el llamado a números que le generan una alta facturación. Por lo general el defraudador engaña por más tiempo a su víctima imponiendo una música que simula ser el tono de llamada al número discado.
- **Secuestro o *hacking* de teléfonos VoIP**. A la vez que las proveedoras de telefonía comienzan a ofrecer el servicio sobre redes de datos mediante tecnología VoIP se abren nuevas vulnerabilidades a la red de comunicaciones. Los dispositivos finales instalados en los usuarios pueden también pasar a ser secuestrados remotamente y sus datos utilizados para generar llamadas a través del proveedor.

En concordancia con lo expuesto, Karak, Jain y Muralidaran (2013) listan las siguientes taxonomías de fraude, identificando tanto a su autor como a su víctima.

**Cuadro 6 - Tipologías de fraude**

| Tipo de Fraude | Autor | Victima |
|---|---|---|
| Suscripción | Impostor haciéndose pasar por un cliente genuino | Cliente |
| Itinerancia (*roaming*) | Cliente | Operador Telefónico |
| Tarjetas de telefonía prepagas | Ingeniería interna, Terceros | Cliente |
| Servicios de Contenido | Terceros | Cliente |
| Secuestro de PBX | Terceros | Cliente |
| Servicios de Valor Agregado | Terceros (mediante discadores automáticos) | Cliente |
| Internos | Empleados | Operador Telefónico |
| *Auto dialers*(discadores automáticos) | Terceros, Hacker | Cliente |
| Estafas de números 0800 o similares | Terceros | Cliente |
| Fraude de interconexión | Terceros, Empleados, Proveedores | Cliente |
| Refiling | Terceros | Cliente |
| Clonación de tarjetas SIM | Terceros, Terrorismo | Operador Telefónico |

| | | |
|---|---|---|
| Hacking | Terceros | Operador Telefónico |

Fuente: “Evolving early combat systems in Next Generation telecom fraud: catch them young” (2013, p. 12)

### Conclusiones del apartado

Los ardides que utilizan los estafadores son variados y cambian con el tiempo y las tecnologías. También pueden poseer distintas complejidades, cantidades de actores y alcances geográficos varios. Algunos fraudes son sencillos y se basan en el simple robo de identidad de un abonado o la clonación de un chip de celular, pero otros pueden poseer procesos más complejos y requieren la conjunción de varios integrantes con el mismo objetivo de delinquir. Es primordial comprender que no existe un único patrón de fraude telefónico y que su detección requerirá de herramientas de análisis que permitan aprender dinámicamente.

Por otra parte, quienes cometan fraude a una empresa de telefonía pueden no ser solo sus clientes, sino también sus proveedores o hasta terceros que no poseen una relación comercial directa con la empresa. Los frentes a vigilar son muchos y los métodos de detección deben ser automatizables, pero al mismo tiempo deben arrojar un bajo número de falsos positivos que no degraden los recursos de la organización, y no dañen la relación con sus usuarios.

## III. 3 Modelación y detección del fraude telefónico

En este apartado se desarrollarán las técnicas usuales de detección del tráfico telefónico considerado fraudulento.

Johnson (1996) define el fraude en comunicaciones como una transmisión cualquiera de voz o datos a través de una red de telecomunicaciones donde el objetivo del originante es evadir o disminuir cargos legítimos. En la misma línea, Davis y Goyal (1993) definen fraude como la obtención de servicios no facturados y ganancias no merecidas durante una llamada. Ambas

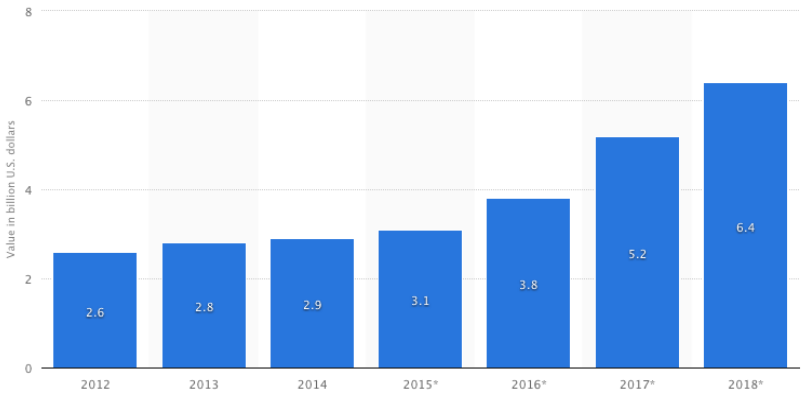
afirmaciones se centran en la intención de una ganancia monetaria en las transacciones realizadas por el perpetrador. Por lo tanto, el análisis de las transacciones telefónicas, su cliente origen relacionado y su costo/precio serán los objetos de análisis en este apartado.

### Comparativa con fraudes transaccionales en otras industrias

Antes de desarrollar las técnicas de modelación de fraude telefónico, se investigarán las técnicas en industrias más maduras pero con problemáticas similares; en especial el fraude de tarjetas de crédito a entidades bancarias. Dentro del fraude a dichas entidades se centrará en aquel que se da en compras no presenciales o por Internet, dominadas por las compras de comercio electrónico o comercio online. Algunas estadísticas de la industria ayudan a tener una dimensión económica del problema:

- La proveedora de servicios de consultoría PwC (2011) realizó una encuesta global y encontró que el 34% de las empresas encuestadas fueron víctimas de fraude bancario durante el año anterior. El crecimiento de este indicador con respecto a su anterior año fue del 30%.
- Nasdaq (2015) ofrece datos sobre la industria del fraude de tarjetas de crédito en EEUU: Cerca de 31.8 millones de usuarios sufrieron algún fraude en 2014, más de tres veces el número de casos sufridos en 2013. En su opinión, el fraude online o "no presente" es un gran problema en ese país. El 45% de los fraudes de 2014 cayeron en esta categoría, seguidos por el fraude de tarjetas falsas (37%) y luego por los casos de tarjetas robadas o perdidas (14%).
- El sitio online de estadísticas Statista (2016) visualizalas pérdidas en los EEUU por fraudes en tarjetas de crédito para el período 2012 a 2014 y su proyección hasta 2018.

**Gráfico 3 - Pérdidas por fraude en tarjetas de crédito en los EEUU**




Fuente: Sitio web Statista (2016)

- Rampton (2015), a través de su nota en la revista *Forbes*, interpreta sobre la próxima incorporación obligatoria en los EEUU de la tecnología de chip EMV[12] a las tarjetas de crédito resultará en una drástica reducción de fraudes por clonación o copia. Pero, por otro lado, este evento empujará a los estafadores a dirigir su atención al segmento online, donde no existe aún un proceso o tecnología estándar para combatir su crecimiento. Basándose en el axioma de que el fraude siempre sigue el camino del dinero, el aumento del comercio electrónico traerá aparejado también un aumento de los estafadores en ese ecosistema. La nota también advierte sobre el creciente riesgo que ofrecen las operaciones de *charge back* o reembolso, donde el usuario puede pedir la devolución de su dinero por la compra *online* de forma automática aún cuando tenga el bien comprado ya en su poder. El 86% de las operaciones de reembolso son fraudulentas.

[12]Acrónimo de "Europay MasterCard VISA".

Joyner (2011), perteneciente a la empresa SAS[13], presentó un informe relacionado con la temática donde informa que rara vez las instituciones bancarias monitorean el comportamiento de sus clientes a través de múltiples cuentas, canales y sistemas. Por lo general, estas corporaciones poseen sistemas antifraude que trabajan en compartimentos estancos o silos. Esta debilidad abre la puerta a escenarios donde el defraudador gana conocimiento de la información por medio de un determinado canal (una compra minorista presencial), pero utiliza este conocimiento para cometer fraude a través de otro canal distinto (mediante el sistema de *home banking*). Muy pocos bancos poseen sistemas que analizan en forma *cross* toda la institución y que pueden correlacionar el comportamiento del cliente a través de todos los productos y canales de contacto. El informe continúa afirmando sobre la necesidad real de estas instituciones de identificar patrones y a sus autores, pero también advierte sobre de la ausencia de modelos analíticos para establecer los correctos sistemas de defensa. Las necesidades -y sus problemáticas- que sufren estas instituciones se pueden resumir en las siguientes:

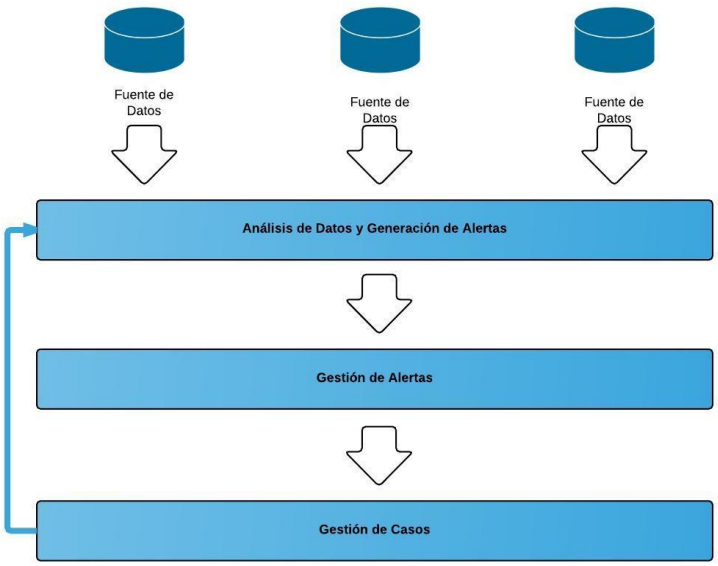
- Identificar fraude a través de toda la organización donde los sistemas de operaciones no suelen ser cooperativos intra o extra organizaciones.
- Monitorear cada transacción en tiempo real sin alienar a los clientes y proveedores generando procesos de verificación largos.
- Implementar reglas rigurosas para detectar fraude evitando falsos positivos (y sus costos relacionados de investigación).
- Unificar los procesos de gestión del fraude superando la disparidad de fuentes de datos y interfaces que dificultan la tarea.

[13] La empresa SAS provee herramientas para el acceso, gestión, análisis y reportería de datos con el propósito de toma de decisiones.

Es así como surge la necesidad de los bancos por una calificación (*scoring*) en tiempo real de todas las transacciones de tarjetas de crédito para lograr una detección más rápida y certera a escala global. El objetivo último es prevenir el fraude antes que éste ocurra, aún cuando los perpetuadores evolucionen sus métodos y oculten sus intenciones. Para esto, el citado informe de Joyner (2011) establece como requerimiento para una institución la incorporación a su base de conocimiento de datos de todos los sistemas transaccionales aún cuando sean de unidades de negocio distintas. Debe incluirse información de sectores como recursos humanos y auditoría, e incluir fuentes externas como bases de datos comerciales de criminales conocidos. Toda esta información integrada debe ser periódicamente validada y limpiada.

Conceptualmente el flujo de un proceso de detección temprana, con una integración de extremo a extremo, puede visualizarse en el siguiente gráfico

**Figura 7 - Flujo de proceso conceptual de un sistema de detección de fraude**




Fuente: SAS Group Forum (2011)

En este modelo, Joyner (2011) establece que cada transacción (apertura de una cuenta, otorgamiento de una tarjeta de crédito, acceso a un cajero automático, una llamada al *call center*, entre otros) sea analizada a través de un conjunto de reglas y modelos predictivos. En tiempo real, el sistema informático debe validar estas actividades del usuario contra la base de conocimiento global de la empresa con el objetivo de detectar comportamientos sospechosos. Adicionalmente, en forma diaria se debe completar con procesos masivos diferidos sobre todas las cuentas. El sistema informático realiza análisis sintáctico de los datos y actualiza la información principal de cada cliente. Con esta meta data, los registros son exhaustivamente vinculados basados en múltiples combinaciones de sus datos. Usando técnicas estadísticas, se identifican nuevas entidades de datos y éstas son colapsadas en nuevas vistas sobre la información.

Finalmente el sistema realiza agregación y priorización de las alertas provenientes de otros sistemas de fraude de la institución bancaria. Estas alertas son correlacionadas entre sí para generar una calificación global del riesgo de una cuenta o un grupo de cuentas relacionadas. Esta calificación es utilizada para redireccionar cada alerta al centro de investigación o soporte destinado a seguir el caso. Idealmente el sistema informático debe comunicarse automáticamente con otros sistemas del banco para realizar acciones automatizadas entre las que puede estar la paralización de una cuenta o la disminución de su crédito disponible.

Este sistema propuesto va más allá del simple y típico análisis sobre un cliente, y provee una visión holística de la actividad fraudulenta en la institución.

Otros estudios de interés donde puede encontrarse experiencia sobre comportamientos anómalos o ilegítimos basados en transacciones observadas pueden hallarse en las industria

de seguros, salud y finanzas. Específicamente en la industria de medicina, Yao (2014), publica una investigación sobre fraude a financiadores de salud en China. En esta clasifica los métodos para detección de fraude en dos grandes grupos. Aquellos de aprendizaje supervisado, donde se hace uso de información anterior sobre la variable dependiente (operación fraudulenta o legítima) para el entrenamiento y generación de patrones predictivos. Y por otro lado aquellos sin aprendizaje supervisado que no cuentan con un status predeterminado de las variables dependientes, por lo que extraen información de las variables predichas directamente. Otro trabajo en la misma industria es presentado por Yang (2006) que propone la identificación de fraude mediante la comparación con las vías clínicas (*medical pathways*) que son seguidas por los profesionales de la salud para generar un cierto diagnóstico o procedimiento médico. Yang (2006) propone que una institución médica operando normalmente debe, ante una determinada problemática específica, seguir una cierta cantidad de pasos secuenciales predeterminados. El abandono de esos comportamientos estandarizados permite a un sistema informático detectar fraude en las prestaciones. Este concepto de definir dentro de cada proceso, las conductas "normales" y penalizar las que están fuera de norma, es extensible a cualquier industria.

De lo expuesto hasta aquí en materia de lucha contra el fraude a entidades de otros segmentos de negocios se puede desprender que las prácticas recomendadas implican un monitoreo en tiempo real de cada transacción y una comparación contra múltiples patrones de comportamiento, tanto individuales del cliente como correlacionada entre todos los sistemas informáticos de un organización. También es importante la capacidad de contar con datos previos de tráfico anómalo y de tráfico limpio para entrenar los sistemas. Este acercamiento tiene muchas similitudes al tratamiento recomendado del fraude en la industria de telecomunicaciones, como se desarrollará a continuación.

## Propuestas de modelos de detección de fraude

Davis y Goyal (1993) reportan sobre lo insuficiente de aplicar umbrales uniformes para todos los usuarios del servicio telefónico. Este acercamiento al problema de detección de conductas anormales supone la existencia de un usuario promedio mítico. Su propuesta consiste en modelar cada usuario individualmente y permitir que su perfil de tráfico sea adaptativo a través del tiempo. Adicionalmente, reglas de generales de comportamiento de fraude[14] deben ser aplicadas para enriquecer el proceso. El componente analítico del sistema determina finalmente si las alarmas, luego de ser vistas en conjunto, dan suficiente evidencia para ser entregadas a personal humano para su revisión y seguimiento.

Hollmén (2000) considera en su disertación de doctorado que mediante el establecimiento de modelos de patrones de tráfico el fraude puede ser detectado proactivamente. Esta forma de trabajo no es nueva y se utiliza desde hace tiempo en la industria de la telefonía. Un escenario clásico y sencillo de detección de tráfico anómalo en redes de telefonía celular se enfoca en el análisis entre la relación tiempo y distancia a la que pueden realizarse dos llamadas consecutivas desde un mismo teléfono móvil. Se considera que bajo un comportamiento normal un usuario no puede generar una llamada en un lugar determinado de la ciudad y a los pocos minutos generar una nueva llamada en un lugar realmente alejado de la misma ciudad o en una ciudad vecina. Este sencillo método de detección de fraude se denomina "trampa de velocidad".

El citado autor propone la utilización de redes neuronales y modelos probabilísticos como herramientas para la prevención de conductas de fraude. Es importante notar que su enfoque sobre fraude se centra sobre redes de telefonía móvil, aunque muchos de los conceptos

[14] Ejemplo de regla: la verificación de llamadas a países de destino sospechoso o usualmente plausibles de fraude por su alto costo.

pueden ser ampliados a cualquier fraude telefónico: móvil, fijo o telefonía de datos sobre Internet. Para comenzar a analizar la problemática lo primero que realiza Hollmén (2000) es una compilación sobre distintas investigaciones publicadas sobre el tema y sintetiza estas en dos grandes metodologías de detección:

- Metodología de Análisis Absoluto: el modelo absoluto se basa en establecer escenarios de tráfico telefónico fraudulento y de tráfico telefónico honesto o normal. El tráfico telefónico entonces es encuadrado dentro de un escenario u otro.
- Metodología de Análisis Diferencial: el modelo diferencial se basa en detectar cambios repentinos en el comportamiento de las llamadas (aumento de la duración de la llamada, aumento de la cantidad de llamadas en horarios atípicos, entre otros).

En los siguientes gráficos de curvas de distribución probabilística se visualizan ambas metodologías. En el Análisis Absoluto, ilustrado en la gráfica izquierda, se deben modelar el comportamiento normal ($C_0$) y el comportamiento fraudulento o anómalo ($C_1$). En el Análisis Diferencial, ilustrado en la gráfica derecha, se construye sólo un modelo asumiendo el comportamiento normal; y todo desvío de éste es clasificado como fraudulento o anómalo. Las líneas de puntos en ambos gráficos indican los umbrales arbitrarios de decisión y las zonas de color indican las regiones donde se clasifica un evento como fraude.

**Gráfico 4–Comparación análisis absoluto versus análisis diferencial**


Fuente: "User profiling and classification for fraud detection in mobile communications networks" (2000)

Es así como todos los trabajos de investigación encontrados por Hollmén (2000) sobre detección de fraude se acercan al problema de una forma diferencial o de una forma absoluta. Las distintas variaciones dentro de cada una se deben a la representación del problema, la elección de modelos de clases, el grado de conocimiento disponible sobre fraudes conocidos y la cantidad de datos disponibles ejemplificadores de comportamientos normal y anormal. Por otro lado, el autor encuentra sorprendente el reducido marco teórico existente sobre modelos dinámicos aún cuando múltiples investigaciones afirman que el fraude es un fenómeno de comportamiento cambiante.

En orden de construir modelos de comportamiento normal y fraudulento, y de poder determinar la capacidad real de diagnóstico de los modelos construidos, es requerimiento poseer registros de llamadas que exhiben ambas conductas. En la práctica, conseguir registros normales es relativamente fácil, por lo que la construcción de modelos a partir de estos datos suelen dominar los sistemas antifraude. Los registros de actividad anómala son más escasos y su recolección requiere de trabajo humano manual y extenso. Para la recolección de datos Hollmén (2000) concibe dos posibilidades:

- Mediante cobros impugnados. Dado que la valorización del tráfico de cada servicio telefónico es enviado mensualmente a su correspondiente cliente se presupone que aquellas facturas que contengan llamadas anómalas serán rechazadas por éste. De esta forma es posible construir, manualmente, los dos conjuntos de datos basándose en la impugnación o no impugnación de consumos por parte del usuario final.
- Mediante detección de fraude sencillo o básico. Esta propuesta consiste en separar llamadas de cuentas que tuvieron algún comportamiento de fraude detectado mediante una forma básica (ejemplo: llamadas de muy corta duración durante un intervalo muy reducido de tiempo). Una importante característica de este método es que no separa individualmente las llamadas anómalas de las normales. El conjunto de registros denominado fraudulento contiene una mezcla de llamadas normales y llamadas adulteradas.

La otra decisión clave para el diseño del sistema de detección de fraude es la elección del método de clasificación y perfilado *(profiling)* de usuarios. Existen varios posibles criterios y Hollmén (2000) recopila los más emblemáticos:

- **Redes probabilísticas.** Permiten una eficiente descripción de densidades probabilísticas multivariadas. De interés particular son las redes bayesianas que permiten una representación como grafos acíclicos dirigidos. Esta representación gráfica facilita su entendimiento y manipulación. El método asume ciertos supuestos o técnicas de trabajo:
    - Independencia condicional entre las variables.

    - Decisión sobre la distribución de probabilidades de cada variable de la red (por ejemplo: gaussiana para variables continuas y multinomial para variables discretas).
    - Utilización del algoritmo Esperanza-Maximización (algoritmo EM) para encontrar estimadores de máxima verosimilitud de parámetros en aquellos modelos probabilísticos que dependen de variables no observables. El algoritmo realiza iteraciones hasta encontrar alguno de los mapeos posibles entre las distribuciones ocultas y las mediciones observadas.

- **Mapas auto-organizados (SOM)**: Esta tipología de red neuronal artificial es entrenada usando aprendizaje no supervisado para producir una representación discreta del espacio de las muestras de entrada, llamado mapa. Los mapas auto-organizados son diferentes de otras redes neuronales artificiales, en el sentido que éstos usan una función de vecindad para preservar las propiedades topológicas del espacio de entrada. Es el método de redes basado en aprendizaje competitivo no supervisado más utilizados.

- **Métodos LVQ (Learning Vector Quantization)**. Pueden ser entendidos como un caso especial de redes neuronales artificiales. Son métodos de aprendizaje adaptativo basados en los mapas auto-organizativos (SOM). Poseen la ventaja de utilizar un número fijo y relativamente bajo de prototipos para aproximar las funciones de densidad de probabilidad de las distintas clases.

En concordancia con lo expuesto anteriormente, Tawashi (2010) informa que:

- La detección de fraude telefónico es una disciplina en constante evolución. Cuando una forma de detección de fraude se encuentra implementada, los estafadores telefónicos cambian sus tácticas rápidamente y desarrollan nuevas formas de fraude.
- La detección de nuevas metodologías de fraude posee la complejidad adicional de que sus técnicas de detección nunca son públicamente difundidas por las empresas. Esto se debe a que su exposición también llegaría a los estafadores y podrían generar más rápidamente formas de evadirlas.
- Cuando una empresa telefónica sufre de fraude telefónico nunca lo informa por el temor de generar prensa negativa entre sus clientes. Empresas que publican en mercados de valores poseen un aversión extra en difundir públicamente estos eventos.
- La constante proliferación de nuevas tecnologías (Internet, mayor poder computacional a menor costo, herramientas libres, documentos online, entre otros) permite que el fraude telefónico sea realizado por personas inexpertas y con recursos cada vez más asequibles.

Con el foco en el fraude al usuario final y cómo decidir si una cierta llamada telefónica es fraudulenta o no, Fawcett y Provost (1998) afirman que la detección mediante la clasificación de llamadas individuales no es suficiente. El contexto es crítico en este análisis, dado que una llamada potencialmente sospechosa para un usuario, podría no serla para otro. Asimismo, usuarios legítimos realizan ocasionalmente llamadas que pueden parecer sospechosas por ser atípicas para su conducta promedio. En síntesis, la decisión sobre la existencia de fraude debe basarse en un análisis de conductas individuales de cada usuario. En esa misma línea, los autores proponen la creación de indicadores que permitan diferenciar el tráfico telefónico normal de un usuario individual del tráfico impostado que podría generar un estafador en su nombre.

Fawcett y Provost (1998) plantean el uso de técnicas de inteligencia artificial y aprendizaje automático (*machine learning*) para la construcción de reglas con factores de certeza que analicen cada llamada telefónica generada. La construcción de estas reglas se realizaría mediante el análisis del tráfico telefónico durante un intervalo de tiempo (por ejemplo, 30 días) sobre cuentas de usuarios sin fraude. Durante ese tiempo el sistema a construir clasificaría y aprendería los perfiles de tráfico corriente posible. En base a estas reglas generadas se podría diseñar un detector de fraude que compare el tráfico telefónico en tiempo real contra los umbrales de tolerancia fijados por estas reglas. Las pruebas de campos realizadas mediante esta metodología tuvieron un 92% (+/- 0.5%) de certeza en la detección.

Los investigadores Gupta, Pahwa y Arora (2014) concuerdan con el uso de herramientas de minería de datos (*data mining*), pero proponen un acercamiento distinto a la detección sin utilizar técnicas de aprendizaje y construcción de clasificadores. Su propuesta se basa en métodos de detección de valores atípicos (*outliers*) basados en la suma de coeficientes similares. La ventaja principal que agrega es la independencia del conocimiento de las funciones de distribución de probabilidades del objeto de análisis. Barnett y Lewis (1994) definen a un valor *outlier* como una observación que parece desviarse marcadamente de los otros miembros de la muestra en la cual ésta ocurre. La aplicación de esta herramienta por parte de los investigadores arrojó un resultado de un 90% de certeza en la clasificación de llamadas en fraudulentas como en genuinas (con un 4% de Falsos Positivos y un 6% de Falsos Negativos).

### El crecimiento del poder computacional

Los métodos, tecnologías y paradigmas descriptos anteriormente poseen una ventaja adicional que experimenta la industria de la tecnología en general. El constante abaratamiento del poder computacional y el constante aumento del mismo dan ventajas únicas a cualquier

proceso que se basa fuertemente sobre procesos informatizados. McAfee y Brynjolfsson (2014) opinan que la humanidad esta acercándose a un nuevo punto de inflexión productivo similar a los ocasionados en las anteriores revoluciones industriales, pero esta vez producido por la inteligencia artificial, las redes de comunicaciones, los avances en poder de procesamiento y la digitalización de casi toda la información producida.

Los autores opinan que la denominada ley de Moore[15] se seguirá manteniendo por el futuro próximo, haciendo que cada vez se puedan obtener equipamientos mas baratos y, a la vez, con capacidades computacionales mas poderosas. Asimismo, la creciente interacción de los dispositivos en lo que se conoce como Internet de las Cosas (IoT[16] por sus siglas en inglés) permitirá que se generé un crecimiento exponencial de información digital que puede ser compartida, iterada e interpretada en tiempo real por sistemas informáticos. Por otro lado, predicen la automatización de una gran cantidad de tareas cognitivas que hoy en día son ocupadas por trabajadores humanos.

Otras fuentes, entra las que se pueden citar a Satell (2016) y Sydell (2015), predicen similares tendencias en las predicciones realizadas por Moore, por lo cual cualquier algoritmo que se plantee hoy en día, cual complejo que sea, con el tiempo podrá ser mas sencillamente implementado y por equipamiento cada vez mas barato.

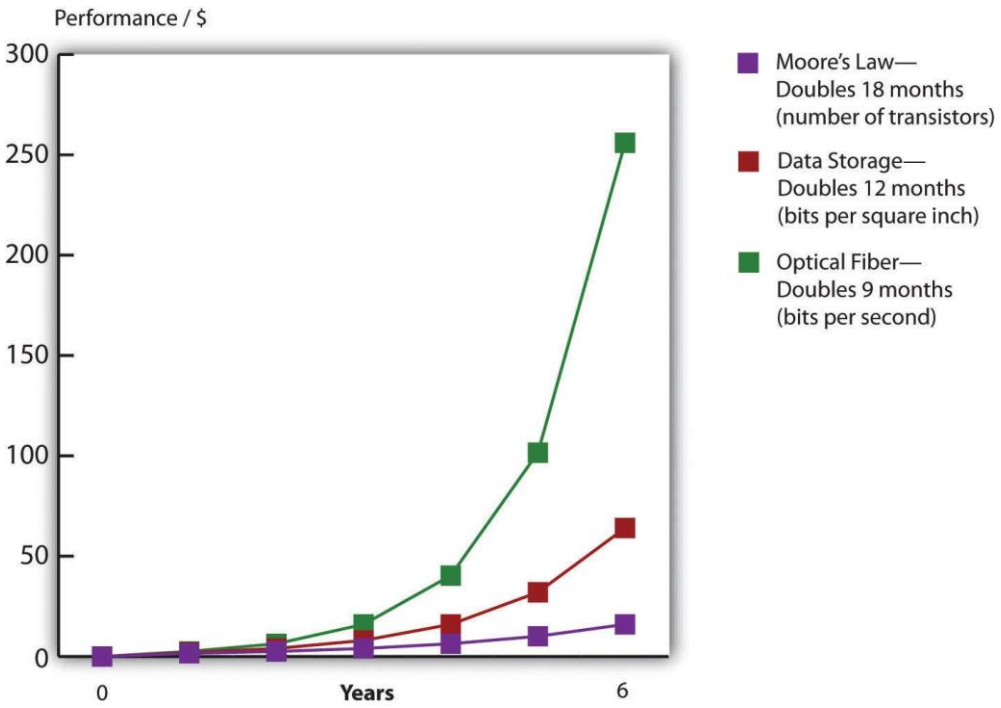
Este mismo paradigma puede aplicarse a otros componentes de la tecnología como la capacidad de almacenamiento y la velocidad de los vínculos de comunicaciones. A

[15]La **Ley de Moore,** expresada por Gordon Moore, afirma que aproximadamente cada dos años se duplica el número de transistores en un microprocesador. Es una ley de comprobación empírica e implica que la potencia computacional posee un crecimiento constante en el tiempo.

[16]**IoT (Internet of Things).** La internet de las cosas es la tendencia a la interconexión digital de objetos cotidianos a través de Internet, por lo cual con el correr del tiempo se conectarían a Internet más "cosas u objetos" que personas.

continuación se gráfica el crecimiento de la eficiencia de la capacidad computacional, el espacio de almacenamiento y la capacidad de la fibra óptica:

**Gráfico 5 – Evolución de la Ley de Moore**




Fuente: presentación para accionistas de Amazon.com por Jeff Bezos.(2006)

De forma complementaria, existe consenso sobre la afirmación que la humanidad atraviesa desde la última década una "Edad de la Información". McAfee y Brynjolfsson (2014), Birkinshaw (2014), Razin (2016), y otros, explican sobre el pasaje de la sociedad industrial del siglo XX a la sociedad de la información de este siglo, y predicen fuertes cambios sociales y en las relaciones de trabajo. Particularmente ponen foco en la necesidad de la aparición de perfiles laborales que analicen el creciente volumen de datos digitales que se generan en un número siempre creciente.

## El crecimiento de la disponibilidad de información

La mayoría de las teorías propuestas de modelos de comportamiento se basan en el procesamiento de información pasada o en curso para generar predicciones futuras. La tarea imprescindible de construir sistemas que posean auto aprendizaje, se comprueba ante la evidencia que los volúmenes de datos disponibles son gigantes y no harán más que crecer en el futuro.

Bae Brandtzæg (2013) advierte sobre la sobre abundancia de información creada. La cantidad de datos disponibles en Internet aumenta diariamente, dado que cada persona produce y distribuye información constante sobre sus actividades. Pero la generación de nuevos datos no solo proviene de acciones activas, como compartir preferencias en redes sociales o blogs, sino de también incluye acciones pasivas como desplazarse a través de la ciudad con el *smartphone* prendido, el generar una compra mediante una tarjeta de crédito o la simple visita de paginas web. Según Bae Brandtzæg (2013) el 90% de la información disponible en 2013 había sido creada en los anteriores dos años.

Marr (2015) recopila algunos datos de interés que muestran los volúmenes de datos que se generaron en 2015:

- Cada minuto se generaron 300 horas de nuevos videos en la plataforma YouTube.
- Cada segundo se generaron 40.000 búsquedas en el buscador Google.
- Mil millones de personas usaron Facebook en un mismo día.
- Los usuarios de Facebook enviaron, en promedio, 31 millones de mensajes por minuto.
- Se generaron ventas globales de *smartphones* por 1400 millones de unidades.

- Se predice que para el año 2020 se generarán 1.7 megabytes de información por segundo por cada ser humano del planeta.

Es en esta cantidad de información donde las empresas deben comenzar a buscar valor. Por un lado es importante entender el relacionamiento de las distintas fuentes de información (estructurada y no estructurada) entre sí y por otro desarrollar las herramientas que permitan hacerlo con la menor intervención humana.

### Conclusiones del apartado

Como conclusión, se puede afirmar que el fraude telefónico es dinámico y que las metodologías para enfrentarlo deben también ser dinámicas, preferentemente basadas en sistemas estadísticos que detecten comportamientos anómalos o atípicos. Por la gran cantidad de transacciones que se generan es imposible respaldarse en personal humano para identificar una conducta criminal contra el servicio que proveen. Los procesos a implementar que velen por la seguridad de la empresa deben encontrarse automatizados y en constante ajuste. Un umbral de decisión muy alto a la hora de alterar a operadores humanos sobre una actividad ilegal, puede devenir en pérdidas millonarias en períodos cortos de tiempo. Por el contrario, un umbral de decisión muy bajo, puede generar falsos positivos e inundar a los operadores de la auditoría con demasiados casos a procesar. Los falsos positivos también pueden generar molestia en los usuarios genuinos que ven su servicio interrumpido erróneamente.

A continuación se destacan los conceptos principales del apartado:

- Las formas de fraude telefónico son dinámicas. La aparición de nuevas tecnologías de comunicaciones introduce nuevos riesgos de fraude y nuevos escenarios.

- El fraude telefónico puede ser detectado mediante modelos de comportamiento normal vs comportamientos anómalos. La dificultad se centra en definir qué es un comportamiento normal. También en definir los umbrales de decisión.
- La creación de perfiles de conducta es necesaria. Es posible que la forma más óptima de crearlos sea bajando al nivel de perfiles de conducta por usuario. Las transacciones pueden ser agrupadas y a la vez enriquecidas con *metadata*[17].
- Una de las tareas más complejas al momento de implementar un sistema de detección de fraude es el entrenamiento de su algoritmo. Es posible la elección de un aprendizaje supervisado o no supervisado.
- La aplicación de técnicas de aprendizaje automático, redes neuronales y minería de datos producen los mejores resultados de detección y la menor cantidad de falsos positivos.
- El poder computacional crece y se abarata en el tiempo en una relación exponencial. Por lo tanto, algoritmos cada vez más complejos -que diez años atrás solo podrían haber sido corridos en supercomputadoras- están al alcance de las empresas y los particulares.

- Existe una creciente tendencia a generar cada vez mayor información digital y desde diversos orígenes. Esta abundancia de datos permite alimentar estos algoritmos en tiempo real con mejor información, y por lo tanto, les permiten tomar decisiones mas avanzadas y certeras. Por otro lado, la abundancia de datos también trae aparejada una gran dificultad de análisis. La inmensidad del volumen de datos provoca confusión cuando se desea analizarlos, provocando que datos superfluos escondan datos importantes.

[17] Datos que contienen datos sobre otros datos.

### III. 4 Buenas prácticas en los procesos anti fraude

No existe en la legislación local y no se ha encontrado en otras internacionales un cuerpo unificado de normas que deba seguir un operador telefónico para evitar ser víctima de fraude. El Estado y/o los órganos reguladores dejan esas decisiones de implementación a la industria de telecomunicaciones. Esta posición no es extensible para cualquier industria. Por ejemplo, en La Argentina la industria financiera debe cumplir con la Ley 25246 sobre Prevención de Lavado de Dinero y por lo tanto debe "recabar de sus clientes, requirentes o aportantes, documentos que prueben fehacientemente su identidad, personería jurídica, domicilio y demás datos que en cada caso se estipule, para realizar cualquier tipo de actividad de las que tienen por objeto" (Ley 25.246, artículo 21, inciso a).

La industria de las telecomunicaciones ha creado, con el tiempo, distintos foros, cámaras y organismos privados donde se nuclean sus empresas para debatir y colaborar en la lucha con el fraude en sus negocios. Algunos de ellos son:

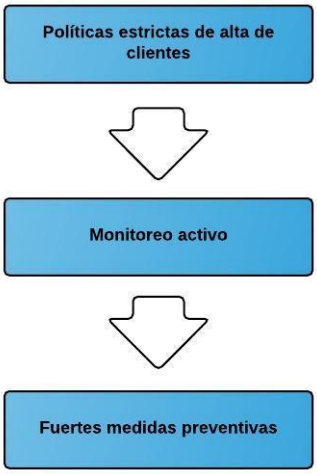
- El comité "Telecommunications Fraud Prevention Committee" perteneciente al Alliance for Telecommunications Industry Solutions (ATIS), el cual ha presentado al ente regulador Federal Communication Committee (FCC) de EEUU distintas recomendaciones y comentarios sobre reglamentaciones anti-fraude
- La Telecommunications Risk Management Association (TRMA) que funciona como foro de la industria para gestión del riesgo. Permite a profesionales cooperar, comprender y compartir mejores prácticas relacionada con incobrables.

- Fraud Watch International especializado en fraudes de Internet en general.
- Telecommunications UK Fraud Forum (TUFF) el cual posee entre sus metas el generar un ambiente de cooperación entre sus miembros y otros foros similares dentro del Reino Unido y fuera de él. También buscar generar documentación y dar a conocer herramientas y métodos tangibles que permiten a la industria manejar el fraude de forma más efectiva. Este foro colabora y se integra con foros locales de otros industrias y con la National Fraud Authority.

En estas organizaciones y otros actores privados se han encontrado diversos publicaciones, *white papers*, exposiciones en congresos de la industria e investigaciones donde se exponen recomendaciones o buenas prácticas recomendadas para el segmento investigado.

La empresa Visa (2009) publica un documento de buenas prácticas a seguir para operadores de telefonía de servicios prepagos y comunica que "entre las principales industrias seleccionadas por defraudadores se encuentra la industria de las telecomunicaciones, en partícula la industria de la telefonía móvil prepaga". En el documento describe las buenas prácticas para reducir el fraude de Cliente No Presente (aquel que sucede de forma remota) las cuales pueden dividirse en tres partes continuas

**Figura 8 - Proceso teórico de buenas prácticas propuesto por VISA**




Fuente: Elaboración propia (2016)

1. **Políticas estrictas de alta de clientes**. Durante el proceso de admisión de un nuevo usuario se deben requerir de datos mínimos mandatorios. Es necesario incluir datos clave como nombre, número celular, dirección de correo electrónico (validada), fecha de nacimiento y todo aquel que permita identificar al nuevo usuario. Además, se deben incluir métodos de autenticación de segundo nivel sobre los datos presentados, como el envío de un código de confirmación al número de celular o a la dirección de correo electrónico. También se recomienda la publicación en la página web del operador de los reglamentos propios y normativa local con que se combatirá y sancionará el fraude.

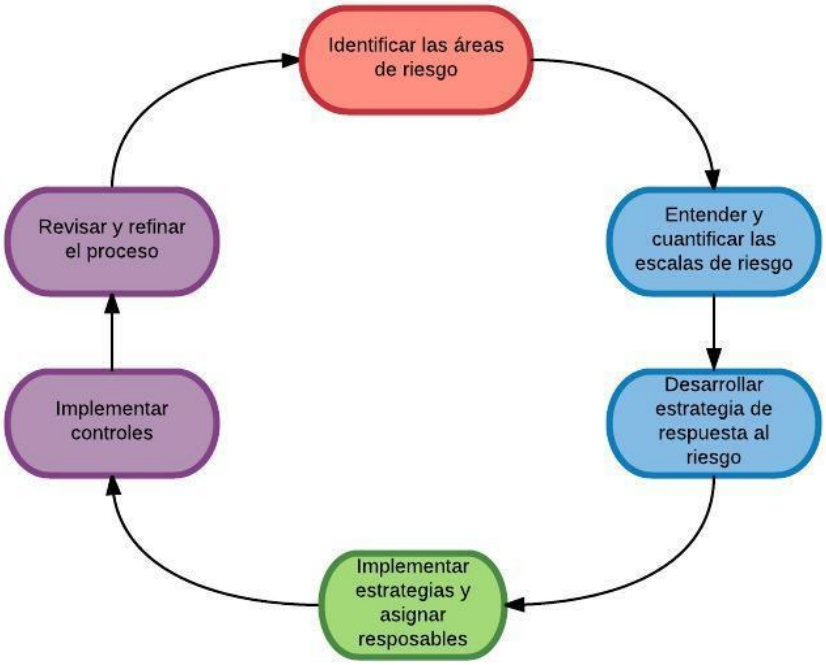
2. **Monitorear activamente las cuentas de los clientes para identificar actividades sospechosas.** Este proceso debe incluir, entre otras, las siguientes actividades:
    a. Generar criterios estrictos de chequeo sobre las transacciones comerciales y operativas de todos los clientes (ejemplo: trampas de velocidad).

b. Generar listas blancas y listas negras de clientes. Los operadores de telefonía deben mantener listas propias de sus clientes genuinos históricos. Las listas blancas poseen el objetivo de evitar molestias a usuarios verdaderos estables. Sus transacciones deben ser procesadas por filtros de riesgo más permisivos o poseer umbrales de alarma más altos. De forma similar las listas negras debes poseer información de clientes y atributos encontrados en operaciones fraudulentas pasadas. En estas listas se deben encontrar número de documentos, direcciones IP, números de tarjetas de crédito, direcciones físicas, números telefónicos, direcciones de correo electrónico y todo dato vinculado con un escenario de fraude anterior.

3. **Tomar medidas preventivas.** Estas deben ser fuertes y decididas contra aquellas características de tráfico telefónico o clientes sospechosos.
    a. Cierre o suspensión de cuentas preventivo. Toda cuenta o cliente que dispare los procesos de detección debe ser rápidamente suspendida. Un equipo 7x24 debe velar por este cumplimiento.
    b. Incorporación a listas negras. El cierre de una cuenta debe realimentar el universo de listas negras que posee la organización con los dato del fraude sufrido.
    c. Cooperación en la industria. Dentro de los límites de la legislación local, los operadores telefónicos deben compartir proactivamente su información de patrones de tráfico y listas negras. La industria local en general obtendrá un beneficio evitando que un determinado defraudador pueda reincidir en otro operador.

El instituto de formación profesional de contabilidad del Reino Unido, CIMA (2008), explica las motivaciones del fraude, su prevención temprana, su detección y sus posteriores respuestas. Le instituto establece como primer paso la gestión de riesgo sobre cada escenario de fraude posible. En este contexto la gestión de riesgo de fraude es tratado como un subconjunto del riesgo operativo donde los errores o eventos tienen su génesis en la intención deliberada de obtener un beneficio. El proceso a seguir para cada potencial escenario puede visualizarse en el siguiente cuadro

**Figura 9 - Flujo de trabajo para gestión del riesgo**




Fuente: Elaboración propia (2016)

El proceso propuesto propone la creación de grupos de gestión del riesgo que puedan recolectar todos los escenarios potenciales de riesgo, asignarles una probabilidad asociada e identificar el potencial impacto para la organización. De esta evaluación, los mandos medios

de la organización deben adjudicar estrategias  a cada riesgo encontrado. Algunas de las estrategias posibles son:

- Retención del riesgo (aceptar riesgos bajos).
- Evitación riesgo (descontinuar productos o servicios demasiado riesgosos).
- Reducción del riesgo (implementar mecanismos de control).
- Transferencia del riesgo  (generar contratos o establecer seguros).

Definida cada estrategia para cada riesgo, estas deben ser comunicadas a los responsables de su implementación. El camino elegido para la minimización del fraude muy posiblemente generará nuevos controles o la modificación de ya existentes. El equipo de riesgo es el encargado de monitorear la efectividad de las acciones ejecutadas. El proceso es un ciclo iterativo, donde nuevamente deben estudiarse los riesgos de fraude luego de la aplicación de los pasos anteriores. El objetivo ulterior debe ser convertir el análisis de riesgo en parte de la cultura organizacional.

En otro aspecto, es interesante observar el dato presentado por Karak, Jain y Muralidaran (2013) sobre el fraude interno. Según sus investigaciones, en la industria de las telecomunicaciones las estafas con origen interno solo representan el 8% de los incidentes, pero en el impacto en la pérdida de utilidad es del 40%. Para combatir esta fuente es necesario agregar otros disparadores a los procesos. Karak, Jain y Muralidaran (2013) agregan la siguiente lista de prácticas:

- Evitar centralizar demasiada autoridad en un solo empleado.
- Evitar la falta de controles y chequeos.

- Diseñar correctamente los sistemas.
- Investigar cualquier renuncia repentina de un empleado clave.
- Investigar los cambios de personalidad repentinos de un empleado o su negativa a delegar tareas.
- Investigar las mejoras financieras de un empleado.
- Sospechar del trabajo fuera de hora sin buenas razones.
- Sospechar de la resistencia de un empleado a ser transferido a otros roles.

Draz (2010) opina sobre la importancia de los controles y las auditorías internas periódicas, para lo cual levanta los siguientes puntos de interés:

- **División de funciones**. Es imperativa la segregación de tareas relacionadas con la custodia, autorización y control de origen de los documentos.
- **Auditoria interna**. Donde los procesos de control interno no pueden ser pensados como estáticos y donde se recomienda un acercamiento “de arriba hacia abajo” con la formación de grupos de trabajo en cada área, pero liderados por el departamento de auditoría de la empresa.
- **Comunicación**. Los procesos de comunicación son tan importantes como los de auditoría. Todos los interesados deben estar al tanto cuando algo está "roto”. Las empresas deben definir un proceso de comunicación que informe a todos aquellos que merecen estar enterados que a ocurrido un fraude en la organización.

- **Aprender de las fallas**. Todo evento de fraude debe poseer un profunda evaluación posterior. De esta evaluación deben aparecer lecciones aprendidas y acciones correctivas sobre las piezas del proceso que fallaron.

### Conclusiones del apartado

Los fraudes más importantes poseen origen interno, tanto como elemento colaborador o en solitario. Por lo tanto, los procesos de fraude deben estar ligados a los procesos de auditoría interna. La separación de funciones y el establecimiento de controles duplicados, impiden la formación de potenciales riesgos internos.

Debido a la multiplicidad de posibles orígenes de fraude y la limitación de recursos que las organizaciones poseen, se debe aplicar gestión del riesgo de forma iterativa. Todos los posibles expuestos deben ser nominados y se les debe relacionar su probabilidad de ocurrencia junto con su nivel de impacto. Un grupo de trabajo debe analizar cada riesgo y priorizar su atención.

Una herramienta vital para los operadores telefónicos de un determinado mercado debe ser la colaboración con sus pares. La formación de grupos de trabajo, cámaras y foros con representantes de todas las organizaciones de la industria permiten intercambiar conocimiento, generar mejores prácticas unificadas y colaborar en la generación de nueva legislación sobre el tema.

## III. 5 Conclusiones del Marco Teórico

- El estudio del fraude de este sector es de importancia actual y futura. Los números de eventos, y su impacto en las utilidades, demuestran que existen claros beneficios de invertir recursos en desarrollar técnicas para minimizar el expuesto propio de la actividad.
- Contrario a la percepción inicial, la industria tradicional de las telecomunicaciones, con sus productos clásicos de telefonía fija y telefonía móvil, posee todavía mucho tiempo por delante. Los números de facturación que maneja el sector indican que, aún no creciendo en las dimensiones de otros sectores informáticos más modernos, todavía hay demanda a ser satisfecha en el futuro cercano y mediano.
- Los escenarios de fraude se reproducen en todas las empresas del mundo y son conocidos, pero con nuevas tecnologías aparecen nuevos escenarios. Quienes cometen fraude son más creativos e innovadores que los agentes que trabajan por la seguridad de los operadores telefónicos. La innovación debe ser constante para no quedar atrás en la lucha contra el fraude.
- En el mismo sentido, ante un fraude de naturaleza dinámica, es ventajoso informatizar los sistemas de detección temprana. Para ello, es indispensable poder definir modelos de comportamiento de tráfico anómalo y tráfico normal. Debida la complejidad de establecer un comportamiento típico se debería trabajar con perfiles por usuario. Parte de la dificultad radica en encontrar al imaginario "cliente modelo". Técnicas de aprendizaje supervisado versos técnicas de aprendizaje no supervisado deben ser evaluadas según los datos disponibles en cada organización.

- Para la clasificación y creación de perfiles se pueden disponer de muchas metodologías, entre las que se encuentran: redes bayesianas, redes neuronales

artificiales, mapas autogenerados, detección de valores atípicos, entre otros. La inclusión del contexto en el que se da cada llamada y el enriquecimiento con datos desde todos los sectores de la organización permite detectar fraudes más complejos.

- En la denominada era del conocimiento los volúmenes de datos que las empresas disponen serán crecientes año a año. La correcta identificación de cual información es importante para la empresa y el relacionamiento de los datos entre sí, son críticos para la evolución de los sistemas antifraudes. La tecnología acompaña ese crecimiento brindando mayores capacidades de almacenamiento y mayores velocidades de transmisión de estos. A medida que estos volúmenes de datos sigan su aumente esperado, deberán aparecer herramientas y perfiles laborales que los puedan modelizar e interpretar.
- Es necesario la formación de un área dedicada, entrenada y especializada para combatir las estafas originadas por los criminales de la industria telefónica. Esta área debe colaborar con Auditoría Interna para curar los procesos y agregar los controles necesarios. El área de fraude debe contar con personal con conocimientos en minería de datos, negocio de telecomunicaciones, inteligencia artificial y estadísticas.
- La industria telefónica debe buscar estandarizar y generar regulaciones locales (y de ser posibles internacionales) que la ayuden contra el fraude.
- La creación de cámaras y foros permite compartir conocimiento, prácticas e información sobre defraudadores. Quienes cometen fraude a una empresa un día, serán los que cometen mañana a otra. El poseer bases de datos colaborativas entre todos los jugadores de la industria minimiza la repetición de la defraudación. Se encontró que países de Europa y los Estados Unidos existen varias entidades que cumplen esta función.

A través del presente Marco Teórico se han analizado los aportes de diferentes autores que fueron considerados de interés y que resultan indispensables para el desarrollo de esta tesis.

En el siguiente capitulo – Marco investigativo – se presentará el trabajo de campo que permitirá conocer la realidad práctica y ampliar los factores relevantes que componen los procesos de gestión del fraude en la industria de comunicaciones.

# IV. MARCO INVESTIGATIVO

El presente Capítulo se encuentra enmarcado en un conjunto de acciones de campo destinadas a describir y analizar el problema planteado, a través de procedimientos específicos que incluirán las técnicas de observación y la recolección de datos. Las técnicas que se utilizarán para construir el presente Marco Investigativo pretenden triangular información obtenida del campo a los fines de poder acercar una visión lo más completa posible del tema bajo investigación, a saber:

1. **Análisis de un caso:** Para profundizar mejor la investigación, se procedió a estudiar el funcionamiento de la empresa argentina NET, que brinda servicios consultoría y análisis de tráfico de telefonía. Dicha empresa no brinda servicio de telefonía en sí, sino que las empresas del rubro subcontratan en ella tareas de análisis de su tráfico. Estos análisis pueden ser de diversas índoles, desde análisis del correcto enrutamiento de las llamadas hasta la correcta elección del cuadro tarifario utilizado. En especial, se abordó -con ellos- como brindan servicios de prevención de fraude telefónico y detalles sobre un proyecto ejemplificador.

2. **Entrevistas a informantes-clave**: Se realizaron tres entrevistas a empresarios locales del sector de telefonía. Se propuso realizar entrevistas presenciales con un formulario inicial semi-estructurado y una duración aproximada de una hora cada una, aunque -en algunos casos- se extendió más allá de lo esperado. El resultado de las entrevistas fue volcado en la investigación y arrojó detalles sobre las prácticas actuales implementadas en las empresas de telefonía para minimizar su expuesto a los fraudes.

3. **Encuestas:** En el marco del evento del sector LAWC se distribuyó -en la Mesa de Entradas- una encuesta estructurada. LAWC es un evento de importancia industrial, donde participan representantes de todas las áreas de la industria de telecomunicaciones, así como operadores de distintas envergaduras, proveedores de telefonía móvil, inalámbrica, Internet y soluciones de telefonía VoIP[18], entre otros.

La investigación pretende, por un lado contrastar con la práctica aquellos conocimientos teóricos mostrados en el Marco Teórico y -por otro- entender las buenas políticas que existen en la industria que -tal vez- no hayan sido analizadas por los referentes teóricos escogidos. Sabiendo que es un industria que -rara vez- colabora comunitariamente, resulta muy posible, que existan casos de éxito o procedimientos implementados que solo se conozcan puertas adentro, y que solamente -mediante entrevistas directas- puedan salir a la luz. El poder entrar en contacto cercano con algunos referentes del sector permitió entender estas prácticas *ad hoc* implementadas. Por otro lado la observación personal del funcionamiento de la empresa NET permitió encontrar detalles más precisos tal vez no comunicados por los encuestados o referentes.

## IV. 1 Análisis de un caso: Empresa NET

Para profundizar mejor la investigación, se procedió a estudiar el funcionamiento de la empresa NET, que brinda servicios consultoría y análisis de tráfico de telefonía. La empresa es de capitales íntegramente argentinos y la mayoría de sus clientes son locales, con algunas excepciones regionales. Los datos vertidos en el presente apartado fueron obtenidos de las

[18] **VoIP** (Voz sobre protocolo de internet) es un conjunto de recursos y protocolos que hacen posible la señal de voz viaje a través de Internet en formato de datos.

entrevistas con su socio principal, su gerente comercial y un ingeniero que estuvo asignado a un proyecto de análisis de procesos.

### Descripción general de la empresa y sus servicios

NET no presta servicios de telefonía de forma directa, sino que brinda servicios profesionales las empresas del sector de telecomunicaciones. Estos servicios pueden ser de diversa índole y ser acordados -caso a caso- para cada cliente, aunque -por lo general- contienen las siguientes tareas:

- Informes de eficiencia de costos en la elección de proveedores.
- Diseño e implementación del LCR[19] de la empresa.
- Análisis del correcto enrutamiento de las llamadas.
- Análisis sobre la correcta elección del cuadro tarifario utilizado para sus abonados.
- Control de calidad de procesos relacionados con el negocio de telefonía.
- Administración de escenarios de Co-Billing y CPP[20] (*Calling Party Pays*).
- Control de fraudes y abusos sobre la red.
- Aseguramiento de ingresos del sector de telefonía.
- Análisis de rentabilidad del sector de telefonía.

La empresa posee consultores propios especializados en la industria los cuales son asignados con dedicación exclusiva a cada cliente. La mayoría de los empleados -pasados o presentes-

[19] **LCR (Least Cost Routing):** Proceso manual o automático mediante el cual un operador telefónico decide caminos de conmutación para sus llamadas basado en costos. Este proceso posee como resultado una lista de destinos telefónicos (países, ciudades, otros) con sus posibles operadores telefónicos de terminación ordenados por costo.

[20] **CPP (Calling Party Pays o Abonado Llamante Paga)**: Fórmula tarifaria por la cual quien origina la llamada paga el costo total de la comunicación. En La Argentina rige para las llamadas realizadas desde la red de telefonía fija hacia la red de telefonía móvil y fue implementado por el decreto N° 92/1997 (B.O. 31/01/97) para incentivar el desarrollo del, en ese momento, incipiente mercado de la telefonía móvil.

tienen relación con el mundo de informática, comunicaciones o ingeniería. Algunos –también- poseen perfiles orientados a gestión de procesos.

Dentro de los clientes que contrataron los servicios de NET en los últimos años se pueden encontrar operadores de telefonía locales como así –también- operadores internacionales, tales como:

- British Telecom (división Argentina)
- Metrotel (CPS Comunicaciones SA)
- Cablevisión Argentina SA
- Crossfone Argentina (DSR Comunicaciones SA)

Otras empresas de menor envergadura han contratado servicios de NET para la gestión integral de su unidad de negocios de telefonía. Según lo mencionado en el Marco Teórico, en el camino a la convergencia de servicios de voz y datos, cada vez más proveedores de Internet también ofrecen servicios de telefonía o de televisión paga. Por otro lado, aquellos que, tradicionalmente vendían exclusivamente servicios de televisión o de telefonía, ahora buscan también completar su ofrecimiento comercial con servicios de Internet. En el sector de telecomunicaciones, a esta tendencia convergente se le denomina *triple play*, y consiste en el empaquetamiento de servicios y contenidos audiovisuales (voz, banda ancha y televisión) dentro de la misma oferta comercial. Debido a esta tendencia comercial, pequeños operadores -que antes solo brindaban servicios de televisión e Internet por cable- ahora se ven forzados a ofrecer servicios de telefonía a sus clientes. Acorde con lo expuesto, no siempre este ofrecimiento es beneficioso para los operadores de pequeño tamaño que encuentran en el agregado de este servicio más un problema que la fuente de nuevos ingresos. Para aquellos cableoperadores, cooperativas de servicios de Internet o proveedores de Internet que no

poseen gran escala se suman a sus problemáticas operativas diarias nuevos desafíos. Algunos de ellos pueden ser:

- Incorporación de nuevo conocimiento técnico para la implementación de los proyectos de telefonía y su posterior mantenimiento.
- Incorporación de nuevo conocimiento para brindar soporte a los usuarios del nuevo servicio brindado.
- Generar acuerdos comerciales con otros operadores telefónicos para el encaminamiento de sus llamados.
- Analizar la estructura de costos de la unidad de negocios.
- Capacidad de generar planes comerciales que incluyan al nuevo servicio.
- Evitar el fraude técnico y comercial.
- Gestionar la nueva infraestructura de servicios.
- Generar la correcta valorización y facturación de los nuevos servicios.

Para estas empresas pequeñas de comunicaciones, desde NET se ofrecen desde servicios consultivos y de tercerización de funciones hasta la gestión completa de su división de telefonía. Se les provee tanto recursos humanos capacitados como herramientas tecnológicas especializadas para gestionar la nueva unidad de negocio. Muchas de las herramientas de software con que cuenta NET han sido desarrolladas por un equipo de programadores propios y sintetizan la experiencia de casi una década en el mercado. Algunas de las aplicaciones de software con que cuenta la empresa son:

- Aplicación para generación de LCR.
- Aplicación para análisis de perfiles de fraude.

- Aplicación de gestión de cargos de CPP con las operadores móviles locales (Claro, Personal, Nextel y Movistar).
- Aplicación para el seguimiento de acuerdos bilaterales con otros operadores telefónicos.
- Aplicación para la valorización de llamadas realizadas con operadores de telefonía argentina dentro del marco del convenio de interconexión (Telefónica de Argentina y Telecom Argentina)

Como se mencionó anteriormente, estas aplicaciones han sido construidas por NET y son ofrecidas en modalidad de software como servicio (*SaaS*, por sus siglas en inglés) dentro del contrato de trabajo que establecen con sus clientes. De esta forma, los clientes no deben cargar con los costos de capital de la compra de equipamiento y licencias.

En el último tiempo –también- se comenzó a proveer la plataforma de servicios de telefonía misma. Con la consolidación de la tecnología VoIP es posible brindar servicio telefónico usando la conectividad de Internet del usuario final sin importar la tecnología subyacente. De esta forma, NET ya ha comenzado a ofrecer una plataforma de servicios en la nube desde la cual sus clientes pueden ofrecer el servicio de telefonía a sus usuarios de Internet. Lo interesante de este producto es que permite a los pequeños operadores salir a ofrecer el servicio de forma inmediata con un inversión relativamente pequeña. Puntualmente en nuestro país existe un gran número de pequeños proveedores de Internet por medio de radiofrecuencia en banda no licenciada (2.4 gigahertz y 5.8 gigahertz) que brindan servicio en localidades del interior. Estos potenciales clientes necesitan de una plataforma de servicio como el que ofrece NET para poder completar su oferta comercial. A estos pequeños proveedores les sería imposible adquirir -como inversión de capital- todos los componentes

necesarios para brindar telefonía y, más aún, la experiencia necesaria para poder operar el negocio. Por último, estos proveedores domésticos, por su poco conocimiento en la materia, se verían fuertemente expuestos a muchos escenarios de fraude ante los cuales carecen de herramientas para defenderse.

Otro de los beneficios de subcontratar con NET es su conocimiento del marco regulatorio local argentino. Como todo negocio, las normas que regulan la actividad son variadas y dispersas. No existe en el país un cuerpo unificado de todas las leyes que regulan la actividad y, por ende, se requiere de la experiencia personal acumulada para entender qué obligaciones se deben cumplir, qué tributos se deben pagar y cuales son los beneficios que se pueden solicitar al Estado. El presidente de NET, Javier Zucconi, posee gran experiencia en este tema y es él quien, por lo general, brinda ese asesoramiento a los clientes.

Respecto a la gestión del fraude los técnicos de NET realizan un monitoreo proactivo de las llamadas de sus clientes. Si bien el servicio de monitoreo está implementado en la actualidad sólo en horarios de lunes a viernes, en esencia es posible extenderlo a una operación 7x24 si alguno de sus clientes lo solicitara así. El análisis de perfiles de fraude se realiza mediante medios estadísticos básicos, dado que la herramienta de software para hacerlo es de desarrollo propio y no posee todas las funcionalidades encontradas en herramientas de explotación de datos de marcas líderes. Según las opiniones de los empleados de NET el software actual cubre con las necesidades normales que necesita su clientela, pero admiten que existe lugar para mejoras.

Descripción de un proyecto de interés

Dentro de los casos de éxito manejados por NET se encontró uno de interés y con relación directa con el trabajo de esta tesis. El proyecto, de alcance regional, consistió en revisar y redefinir los procesos de aseguramiento de ingresos y gestión del fraude en Telefónica. La envergadura del proyecto incluyó no solo a Argentina, sino –también- las operaciones de Perú, Ecuador y Brasil. La adjudicación fue por licitación pública y fue ganada por la firma sueca Ericsson, quien integró luego a NET por su experiencia comprobada en la industria. Ericsson se enfocó en los aspectos más generales de la consultoría y descargó en NET aspectos más detallados relacionados con el negocio de la telefonía. El aporte de equipamiento de hardware y licencias de software corrió por parte de Ericsson.

Objetivos del proyecto:

- Mejorar los márgenes mediante la prevención de pérdidas financieras debido al fraude.
- Mejorar la experiencia de usuario impidiendo que defraudadores hagan uso de sus cuentas o abusen de sus servicios.
- Mejorar herramientas para monitorear la posibilidad de fraude 7x24.
- Unificar los procesos de gestión de fraude.

Desarrollo del proyecto

El primer paso en el proyecto fue definir las reglas de negocio y sus distintos umbrales. Esto formó parte de un trabajo de investigación donde se estudiaron casos anteriores de fraudes específicos que sufrió Telefónica. Fue necesaria la participación de representantes de distintos sectores de la empresa, entre los que se encontraron: Legales, Facturación, Comercial y Operaciones. Uno de los mensajes más importantes comunicados durante las

sesiones de trabajo fue que el fraude era un problema de todas las áreas y de la empresa, en general. El entregable de este paso, que tuvo una duración cercana a un mes, fue un documento que modelaba los procesos de la organización donde se encontraban los "puntos de dolor" en los cuales podría generarse fraude.

El proyecto incluyó equipar a la empresa con el software de gestión de fraude de **cVidya**. Este provee motores de detección de tráfico altamente efectivo, sistema de alarmas y sistema de manejo de casos con interfaces altamente intuitivas. De hecho, una de las ventajas remarcadas sobre la herramienta de software fue su *interface* web dado que desde cualquier navegador es posible utilizarla para obtener reportes, generar nuevas reglas de negocio y utilizar sus herramientas de investigación. Esto permitió que el equipo de personas que controla el fraude pueda trabajar virtualmente desde cualquier lugar geográfico con solo poseer acceso a Internet y una computadora portátil.

Adicionalmente, la nueva plataforma debió integrarse con sistemas de la empresa ya existentes para obtener información con la cual alimentar el sistema antifraude. Entre ellos se encontraron:

- Balances de cuentas de abonados prepagos.
- Eventos de cargas de crédito en cuentas prepagas.
- Registros de las transacciones de llamadas o *Call Detail Records* (CDR[21]).
- Plataformas de servicio: *Softswitches*, centrales de conmutación, otros.
- CRM de la empresa para la obtención de los detalles de los abonados.
- Otros sistemas de manejo de riesgo, gestión de cobranza y facturación.

[21]**CDR (Call Detail Record)**: Registro de una llamada telefónica que contiene información sobre la misma (numero del llamante, numero del receptor, duración de la llamada, día y hora de la llamada, valorización y otros).

Desde el punto de vista de arquitectura de software, la plataforma de **cVidya** se basa en el *framework* de software Hadoop[22], que permite la creación de aplicaciones distribuidas en múltiples nodos (en teoría miles de ellos) y procesar petabytes de información. Este diseño es el que habilita el procesamiento en tiempo real del extenso tráfico de llamada de Telefónica en tiempo real.

La herramienta, una vez configurada y parametrizada, comenzó a generar alarmas que informan sobre tráfico que puede estar en violación con las reglas de negocio decididas.

Una vez puesto en funcionamiento la nueva herramienta, establecidos los nuevos procesos de negocio y asignados responsables para cada tarea, se implementó una fase de realimentación periódica entre las notificaciones que se generaban y la existencia de fraude verdaderamente. Dado que Telefónica ya poseía una herramienta anterior de control de fraude se realizó un paralelo de los resultados de ambos sistemas. El estudio de estos casos permitió detectar la incidencia de falsos positivos y falsos negativos, ajustando los umbrales de decisión y creando, de ser necesarios, nuevas reglas de negocio. Esto resultó además en la vinculación de otras fuentes de datos no incorporadas en el diseño original.

Otro foco importante en el aspecto de fraude estuvo relacionado con los canales de ventas. Al igual que la mayoría de las industrias el análisis de las condiciones de crédito de un suscriptor, verificación de su identidad y seguimiento de sus gastos es crítico. En este aspecto el manejo de este canal resultó específicamente sensible en virtud que agregar más validaciones o endurecer los requerimientos para la adopción de nuevos abonados, puede perturbar negativamente la cadena de facturación. En contraposición, reglas de negocio laxas

[22]**Hadoop** es un entorno de software que soporta aplicaciones distribuidas bajo una licencia libre. Permite a las aplicaciones trabajar con miles de nodos y petabytes de datos.

o servicios mal dimensionados pueden representar incrementos falsos de facturación o disminución del ingreso promedio por usuario (ARPU). El proyecto incluyó estudios sobre el proceso comercial a fin de mitigar los siguientes escenarios:

- Contratación de usuarios con mala calificación crediticia
- Contratación de usuarios ficticios.
- Reactivación de usuarios existentes.
- Descomposición de paquetes de servicios.
- Abuso de políticas de crédito.
- Abuso de políticas de servicio.

El trabajo investigativo abarcó el relevamiento de todos los planes comerciales, en especial sus precios y lógica. Con esta información se realizaron tableros de control y reportes que analizan toda la cadena de valor, permitiendo encontrar "filtraciones" y discrepancias.

Resultados y beneficios del proyecto

Se calcula que la inversión original fue recuperada dentro del año y medio de iniciadas las operaciones del nuevo sistema. Los nuevos procesos fueron adoptados con éxito para los países contratados.

Con el uso de las nuevas prácticas implementadas y la nueva herramienta de gestión de fraude se detectaron y detuvieron eventos de los siguientes escenarios de fraude:

- Fraude originado por *bypass* de llamadas.
- Fraude a usuarios por *callback*.

- Intentos de *hacking* utilizando DTMF[23]
- Intentos de intrusión a centrales de telefonía de usuarios.
- Generación de llamadas de larga distancia "montadas" sobre llamadas nacionales.
- Transferencias de llamadas ilegales con destino números internacionales.
- Llamadas anormales desde números de origen desconocidos o con formatos incorrectos.
- Fraude de suscripción y fraude de *roaming*.
- Distinción de patrones de fraude en general.

El proceso fue diseñado para poseer un monitoreo 7x24 con un equipo de guardia pasiva para los horarios nocturnos. La herramienta de gestión de fraude contacta por medio de correos electrónicos a los operadores de guardia según un esquema de escalamiento definido. Varios responsables fueron incorporados en esta lista de escalamiento, incluido (como última salvaguarda) el vicepresidente de Finanzas.

Por otro lado, también existieron mejoras en la experiencia de usuario, en especial por la mejora de la tasa de falsos positivos en la detección de fraude de suscripción, evitándose la suspensión errónea de clientes inocentes. Como beneficio secundario, la disminución de falsos positivos, permitió ahorro de horas hombre dentro del área de operaciones en la empresa de telefonía.

[23]**DTMF** (Dual-Tone Multi-Frequency) sistema de marcación analógico de números de destino entre el equipo terminal y la central telefónica. Cada número discado es la combinación de dos tonos.

Conclusiones del análisis del caso: Empresa NET

Empresas como la relevada poseen un enorme potencial de negocios local y, posiblemente, en la región. La realidad política de 2016 ha liberado el otorgamiento de licencias de servicios de telefonía, y muchos pequeños proveedores de Internet se están volcando a dar este servicio en pueblos del interior de La Argentina. Según lo relatado por Javier Zucconi de NET existen cientos de estos pequeños ISPs[24] con carteras de clientes de entre 50 a 500 abonados, que por lo general poseen infraestructuras precarias o son emprendimientos Pyme. Estas empresas se verían ampliamente beneficiadas tercerizando la gestión técnico-comercial de su oferta de telefonía. Por otro lado, la escasa experiencia que poseen los hace víctimas fáciles de defraudadores.

Finalmente, y como se pudo ver, el realizar *outsourcing* o subcontratar especialistas externos para la gestión de riesgo de fraude, no es un patrimonio exclusivo de empresas pequeñas. Grandes empresas se ven también beneficiadas de este aporte profesional, en especial aquellas donde la burocracia es tan grande, que es necesaria una cabeza única que pueda ver la totalidad del problema e implementar los cambios organizacionales y tecnológicos requeridos.

## IV. 2 Entrevistas con informantes-clave

Se consideró de gran importancia para esta tesis el recolectar la opinión de algunos expertos en el tema que tienen o han tenido funciones de decisión en la industria de la telefonía, en especial en sectores de operaciones, finanzas o comercial, donde la convivencia con la potencialidad del fraude es un hecho diario.

[24] **ISP**: Internet Service Provider

Es así como, con el propósito de buscar conceptos principalmente inferibles de la experiencia que brinda la realidad práctica, se han entrevistado a algunos expertos con una serie de preguntas semi-estructuradas, las cuales son detallan en el Anexo I.

Del resultado de estas entrevistas se han podido extraer varios puntos de relevancia:

### El fraude es sintomático de la industria analizada

Uno de los entrevistados llegó a expresar, con ironía, una frase muy descriptiva al respecto: "En este momento nos están intentando hacer fraude y en este momento también. Y dentro de un rato nuevamente nos estarán intentando hacer fraude y puede que además lo logren" (Montes, entrevista personal, 8 de agosto de 2016).

Todos los entrevistados fueron categóricos al momento de indicar que sus empresas debían convivir con el fraude diariamente. La hipótesis con que trabajan no se basa en la potencialidad del fraude, sino en qué momento o estadio podrán detectarlo y cuánta será la pérdida relacionada antes de detenerlo. Los intentos de fraude son inherentes a la industria, como lo son el robo de tarjetas de crédito a la industria del banco. Se trabaja para evitar que los defraudadores destruyan la rentabilidad de la empresa, pero es imposible erradicarlos completamente dado que existe una literal legión de nuevos atacantes que se renueva cada día.

Un punto remarcado fue que, en el mundo interconectado actual, el origen del fraude pocas veces es local. Esto dificulta aún más el trabajo de las áreas operativas porque, aun cuando detecten quien intenta estafarlos, muchas veces su procedencia física escapa la jurisdicción local. Algunos escenarios de fraude son tan complejos por la multiplicidad de actores y cantidad de países que intervienen que llevarlos antes las autoridades correspondientes podría

demandar recursos de tiempo y dinero que no están a disposición de los encuestados o de sus empresas. Este dato dejó ver también una realidad: la mayoría de los defraudadores nunca se ven forzados a pagar por sus acciones y esto hace tremendamente atractiva la actividad.

### Las herramientas utilizadas son insuficientes

La mayoría de las herramientas y procesos que describieron los encuestados son desarrollos propios y usualmente denominados "hogareños" o *in-house*. Nacieron de la necesidad al encontrarse con el problema y no viceversa. Sin ir más lejos, en uno de los casos relatados la primera iteración de la herramienta de software implementada fue una planilla de Microsoft Excel. Posteriores iteraciones fueron construidas utilizando lenguajes de programación más generalistas, pero igualmente utilizando recursos internos de las empresas. Y, lamentablemente, durante el desarrollo de estas no se pudo contar con conocimientos profesionales relacionados a estadísticas, redes neuronales, aprendizaje automático u otros paradigmas relacionados. Finalmente, ninguno de los representantes pudo equipar su empresa con las tecnologías *World class* que les hubieran facilitado enormemente su tarea. Tampoco ninguno recibió asistencia externa de empresas consultoras especializadas o de sus casas matrices de existir estas.

Un concepto mencionado por un experto fue que el costo de la inversión (en bienes, licencias u horas hombre) para combatir el fraude no podía ser mayor a las pérdidas que el fraude mismo pueda ocasionar o al volumen de dinero que esa unidad de negocio movilice. Es una afirmación muy sabia, pero choca con una realidad: Es posible que un fraude produzca más costos que la facturación del área de negocio. Para entender esta contradicción resulta importante comprender que en el negocio de la operadora telefónica muchas de las llamadas que realizan sus abonados no terminan en su propia red sino en redes de terceros pertenecientes a otros operadores. Estas llamadas deben ser –entonces- entregadas por

interconexiones ya acordadas entre ambos operadores. Este tráfico telefónico es pagado por el operador que recibió la llamada original cuando la entrega al operador de destino. Las acuerdos de interconexiones, por lo general, funcionan con acuerdos de crédito y en forma post pago. Por lo tanto, ante un escenario de fraude, el monto del costo podría incrementarse enormemente en caso que las llamadas generadas tengan como destino otros operadores, en especial, si el fraude es suficientemente amplio en duración y a destinos de alto valor. Es así, como se llega a que el monto máximo de un fraude puede ser muy superior a la facturación mensual de la línea de productos y puede no tener un límite si no es detectado a tiempo o si los proveedores no detienen el tráfico que el operador atacado les entrega. Se está ante una realidad donde los procesos antifraude pueden literalmente evitar la quiebra de una organización y nunca deben ser minimizados.

### Los montos de los fraudes son grandes

Siguiendo el punto anterior los ejemplos de fraudes detectados no son despreciables. Se citaron fraudes de algunos miles de pesos argentinos a decenas de miles de dólares estadounidenses.

Se definió como el costo del fraude a aquel dinero que la empresa de telefonía debe terminar erogando a sus proveedores para cubrir el tráfico telefónico, y que no tendrá una facturación relacionada a un cliente. No se incluyeron los costos internos. Fueron relatados distintos ejemplos donde esto sucedió:

- En un ejemplo de fraude de suscripción el cliente nunca realmente pensó en pagar su factura. El fraude se dio ante un nuevo cliente que solicitó dos tramas de telefonía

E1[25] en un domicilio residencial. El operador, que estaba recién iniciando su operación en el país, entregó el servicio sin verificar fehacientemente la identidad del cliente, ni verificar su capacidad crediticia. Tampoco pensó jamás que el cliente podría obrar de mala fe por lo cual no denegó preventivamente su tráfico telefónico a destinos no convencionales (Antártida, Inmarsat[26], islas del pacífico, otros), ni tampoco realizó un monitoreo crítico de su actividad. Al final del día, al momento de pagar la factura del primer periodo el cliente desapareció. La empresa de telefonía intentó dar con su paradero, pero debido a que sus datos eran falsos jamás pudo cobrar por el servicio prestado. Finalmente debió abonar a sus proveedores la totalidad del tráfico que les entregó a través de sus interconexiones. La pérdida para la empresa fue grande, pero dejó valiosas enseñanzas.

- Otro ejemplo relatado se dio debido a un cliente verdadero, pero cuya falta de estándares adecuados en materia de seguridad informática en su infraestructura de telefonía devino en que ésta fuera usada por terceros para generar tráfico de llamadas a destinos de alto precio. Según lo relatado, el cliente en cuestión era una pequeña empresa de la ciudad argentina de Mendoza que había subcontratado la implementación de su central telefónica VoIP. El profesional que realizó el trabajo no realizó las configuraciones correctas para que la central telefónica no sea secuestrada remotamente desde Internet. A los meses de estar en servicio el cliente, su central telefónica comenzó a generar llamadas originadas desde China con destino países del continente africano. Esto sucedió durante un fin de semana, cuando la empresa telefónica no poseía ningún operador realizando un monitoreo proactivo. Al encontrarse el día lunes con un consumo de cerca de veinte mil dólares

[25]**Trama digital E1:** Formato de transmisión digital de telefonía donde por un solo par cables de cobre se entrega 32 canales de voz

[26]**Inmarsat** es una red de telefonía satelital con cobertura global. La utilización de tecnología dependiente de satélites geoestacionarios hace que las comunicaciones hacia y desde esas estaciones de teléfono posean un precio elevado.

estadounidenses el cliente fue bloqueado. Al intentar los responsables comerciales cobrar el servicio, el cliente afirmó que no podía jamás pagar esa suma, y que solo podrían hacerlo mediante un proceso de litigio y posterior quiebra. El resultado final fue que la operadora tuvo que afrontar el costo de la totalidad de las llamadas.

De los dos casos elegidos se puede visualizar que la posición de la empresa de telefonía siempre fue débil frente al fraude, y que solo la implementación de procesos muy prolijos puede impedir que parte de su utilidad se vea disminuida por costos relacionados con desfalcos de terceros.

### La complejidad de encontrar al perpetrador del fraude

Sea cual sea el origen del fraude –desde *hacking* hasta fraude de suscripción- los entrevistados describieron una realidad donde detenerlo es complejo. Si detener a los defraudadores es difícil encontrarlos también lo es, y mas aún, el lograr que la justicia los procese por sus delitos. El aspecto internacional del negocio hace que muchas veces victima, operador telefónico y delincuente se encuentren en países distintos. La realidad de las jurisdicciones y vacíos del derecho tornan este asunto de una complejidad que paraliza directamente cualquier intento legal. Por lo tanto, quienes brindaron esta información, confiesan que en la mayoría de los casos las empresas absorben el fraude, y capitalizan el evento para ajustar sus procesos y sistemas. En algunas ocasiones la imposibilidad de detener un tipo de fraude causa que determinados servicios deban ser ajustados o modificados para poder seguir siendo ofrecidos.

## La industria telefónica no es colaborativa

Parecería evidente en la realidad del siglo XXI que la colaboración es el camino para la mejora y la generación de nuevos y mejores servicios. Desde las aplicaciones que dependen de *crowdsourcing*[27] hasta la mayoría de los más conocidos sistemas operativos dependen de la colaboración masiva. Todo lo contrario fue lo recolectado desde las entrevistas con los especialistas elegidos. Ninguno posee conocimiento de foros locales donde sea posible reunirse periódicamente para discutir de temas de interés como el estado del arte de tecnología antifraude. Uno de los expertos participó en un evento sobre el tema años atrás en Brasil y explicó que el mercado de ese país posee una dimensión tanto mayor al local que ha producido este tipo de reunión de notables de la temática. No poseía conocimiento del mismo tipo de foros en otros países de la región y dudaba de su existencia. El resto definitivamente ignoraba de la existencia de eventos similares. Además de faltar congregaciones de interesados en la actividad privada, las entrevistados afirmaron que tampoco existían áreas de gobierno donde recurrir en busca de información, consejo o normativa.

De lo recolectado, parece entenderse que no existen acuerdos de colaboración, ni el interés de formar bases de datos o repositorios de información centralizados. El acercamiento a la problemática del fraude desde la experiencia independiente de cada operador parece forzarlos a tener que invertir tiempo resolviendo el mismo problema en cada empresa. Los entrevistados mostraron interés en la existencia de una "lista negra" donde se pudiera consultar y colaborar sobre datos relacionados con:

- Personas que han realizado fraudes de suscripción.

[27]**Crowdsourcing**: paradigma donde se utiliza la colaboración de muchas personas para la resolución de un problema particular o para generar conocimiento nuevo. Ejemplos actuales incluyen la aplicación de transito Waze o la enciclopedia online Wikipedia.

- Países o regiones que suelen ser el destino de las llamadas fraudulentas.
- Direcciones IP conocidas como ori de fraude.
- Otros datos sobre patrones de fraude.

Otro dato repetido en todos los informates-clave fue la inexistencia de regulación local o ayuda sobre el tema. Consideran que ninguna de las leyes de telecomunicaciones actuales o en tratamiento posee relación, siquiera tangencial, con el fraude en la industria de telefonía.

### La adopción de tecnologías de punta

Uno de los especialistas dejó el segmento de las telecomunicaciones hace 3 años y se encuentra explorando el incipiente sector de las herramientas cognitivas, en especial IBM Watson[28]. A su entender, deviene necesario utilizar herramientas de inteligencia artificial en el marco de cualquier unidad antifraude (telefónico, bancario, crédito, entre otros). En uno de los proyectos actuales con el Estado Argentino, dichas tecnologías se piensan aplicar para ciberseguridad nacional, donde el entrecruzamiento de datos desde varios orígenes heterogéneos (llamadas de celulares, tráfico de Internet, movimientos bancarios, correos electrónicos, movimientos migratorios en las fronteras y otros) permitirá prevenir ataques terroristas. En su opinión estas mismas herramientas deben ser aplicadas a la industria del fraude incorporando no solamente los datos propios del negocio sino información contextual que permita a la inteligencia artificial aprender y encontrar patrones donde los humanos sencillamente no podrían. Al contrario de los restantes entrevistados, este especialista poseía la visión más futurista o de innovación tecnológica, y sus recomendaciones siempre incluyeron solución orientadas a la utilización de *big data*, procesamiento distribuido en

[28]**IBM Watson** es una aplicación de inteligencia artificial diseñada para el procesamiento de lenguajes naturales, la recuperación de información, el razonamiento automático, y el aprendizaje automático.

arquitecturas tipo *Hadoop*, inteligencia artificial, interfaces con máquinas a través de lenguaje natural y otras paradigmas de última hora.

Los restantes entrevistados fueron más conservadores e imaginaban en el futuro el continuar utilizando herramientas estadísticas sencillas basadas en consumos promedios, destinos de llamadas históricamente problemáticos, patrones de llamadas atípicos y otros medios basados en fórmulas matemáticas directas.

### El fraude es un problema de toda la organización

Existió consenso total en los entrevistados acerca de la importancia de alinear y concientizar a la organización entera, o al menos a quienes poseen roles de decisión, sobre el riesgo de no implementar políticas contra los defraudadores. De las charlas quedó claro que con solo la participación de las áreas técnicas es imposible combatir eficazmente esta problemática. Se recomendó la existencia de grupos de trabajo con representantes de finanzas, legales, operaciones y tecnología que posean reuniones periódicas para revisar los eventos sufridos en el último período, el impacto relacionado con la implementación de nuevos productos comerciales, los posibles expuestos que podrían aparejar adoptar nuevas tecnologías, los posibles expuestos que podrían traer cambios organizaciones y el estado del arte en la materia.

### El control del fraude y su tercerización

Sobre la posibilidad de subcontratar el control de la actividad de fraude no existió un consenso. Dos de los entrevistados lo vieron como una decisión peligrosa debido a lo sensible del tema. La posición fue de cautela ante la posibilidad de confiar una gran cantidad de información interna a terceros, aún cuando las suficientes salvaguardas fueran concebidas y

puestas en marcha. La visión que dieron del estudio del fraude lo acerca a un análisis de P&L[29] llamada por llamada, por lo que debería ser necesario compartir datos de costos, facturación, clientes, proveedores y otros. Aún cuando los suficientes acuerdos de confidencialidad fueran firmados el riesgo de transmitir esta información abriría otros caminos hacia el fraude anteriormente inexistentes. Si se expresaron positivamente sobre un control externo de ciertas tareas como en análisis de las perfiles de uso y/o patrones de tráfico telefónico.

El tercer entrevistado consideró que así como muchas veces se subcontrata recursos humanos, facturación o cobranzas, no es diametralmente distinto el realizar *outsourcing* a una empresa especializadas en la temática. También consideró que esto podría funcionar como una suerte de seguro, donde la empresa que brinda el servicio podría tener penalidad o compartir el costo ante el evento de un fraude que no fue detectado por ellos.

### Mejoras sugeridas por los encuestados

Los entrevistados no dieron aportes específicos sobre que se debería modificar en los proceso de fraude. De forma tangencial, uno de los expertos, comentó que veía el futuro de esas tareas basándose en modelos de autoaprendizaje y con poca interacción humana, especialmente cuando el precio de esos motores de análisis por inteligencia artificial disminuye con el tiempo y su poderío computacional sigue creciendo de acuerdo a la ley de Moore[30].

[29]**P&L:** Profit and Loss Statement, pérdidas y ganancias.
[30]La **Ley de Moore** expresa que aproximadamente cada dos años se duplica el número de transistores en un microprocesador. Es una ley de comprobación empírica e implica que la potencia computacional crece constante en el tiempo.

## Conclusiones de las entrevistas

Finalmente, como resultado de las entrevistas a los especialistas, se observa que los algunos de conceptos aprendidos en el Marco Teórico, existen en las organizaciones representadas.

Todos los escenarios de fraude descritos de forma teórica fueron experimentados en mayor o menor medida por las entidades telefónicas, y se corroboró que los montos asociados son importantes en las finanzas de estas. Todas las empresas del sector poseen algún tipo de sector para evitar ser víctimas de este delito. En algunos casos se encontró que existía mayor formalización de un área con estas funciones, y en otros que la función estaba diseminada en distintas cabezas de la organización, pero todos eran profundamente conscientes del riesgo de no asignar recursos a la actividad. Todos informaron que poseían esta función dentro de la organización.

El aspecto más importante relevado fue la insuficiencia de madurez de procesos, la falta de estándares de la industria y la poca inversión en herramientas de software modernas a la altura del problema. Casi todo lo implementado por las empresas representadas fue hecho por el personal propio interno de forma reactiva ante el problema y con poco estudio teórico avanzado. Por ejemplo, el estudio de los patrones de tráfico que representan un fraude fue realizado por personal de IT o comercial y no por personal con formación en estadísticas o ciencia de datos.  En este sentido, es posible inferir que las organizaciones del sector se beneficiarán enormemente por el agregado de procesos realizados por profesionales en la materia y herramienta de software que implementen paradigmas computacionales de inteligencia artificial, cognitivos o basados en modelos estadísticos.

La información de los profesionales participantes es descrita en el Anexo II.

## IV. 3 Encuestas a representantes de la industria

Descripción y metodología empleada

La encuesta fue realizada en forma presencial durante el evento anual Latin America Wholesale Congress (LAWC) 2015 celebrado entre los días 11 y 12 de noviembre en el hotel Sheraton Libertador. El congreso LAWC fue elegido por ser un evento de gran importancia en la industria donde –anualmente- participan representantes de todas las áreas del sector de telecomunicaciones, entre los que se encuentran operadores de distintos tamaños, proveedores de telefonía móvil, telefonía inalámbrica y telefonía VoIP, proveedores de Internet mediante distintas tecnologías, proveedores de software para la actividad, proveedores de equipamiento, clientes, gobierno y otros.

Resulta importante notar que es un encuentro de la actividad privada y, principalmente, corporativa. Generalmente existe baja presencia académica o representación del sector gobierno. Quienes concurren buscan presentar sus productos y servicios, o bien adquirirlos. El objetivo principal es entablar relaciones y estudiar la posibilidad de hacer negocios. También, se realizan alianzas estratégicas y reuniones donde operadores de telefonía acuerdan intercambios mutuos de tráfico de llamadas en los denominados “acuerdos bilaterales”. Por lo general, quienes participan poseen cargos de gerente o ejecutivos comerciales, aunque puede encontrarse representantes de áreas de tecnología, IT o comunicaciones. Además, el evento es repetido en otros países de Latinoamérica en otras fechas del año, pero quienes concurren a la instancia local del evento suelen también hacerlo a las otras instancias regionales. Por lo que se pudo apreciar en persona, el público del evento poseía procedencia variada, mayoritariamente desde los países de la región.

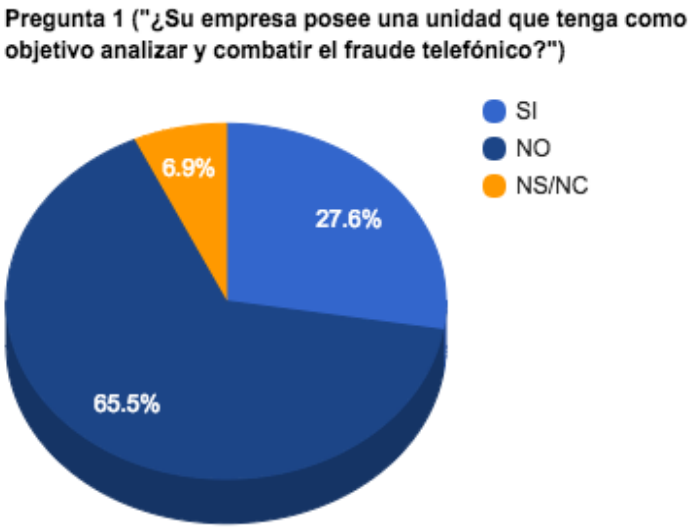
Las encuestas fueron dejadas para ser completadas en el área de registración y acreditación (horario 9AM). Fueron completadas y devueltas 29 hojas. Las preguntas elegidas tuvieron como objetivo entender variables que representan el tamaño de la empresa, su compromiso con la disminución del fraude y que técnicas implementan para perseguir ese objetivo. Asimismo, se intentó que esas variables, al ser correlacionadas pudieran generar información extra sobre las políticas que implementan las empresas.

Con las encuestas obtenidas, se realizó una matriz en Google *Spreads sheet* y se procedió a generar resultados estadísticos. Las preguntas y la matriz de resultados se incluyen en el Anexo I.

*Análisis de los resultados de las encuestas*

Utilizando las respuestas a la primera pregunta puede observarse que la mayoría de las empresas no poseía un área destinada al análisis del fraude. Solo el 27.67% de los encuestados confirmó que su empresa contaba con dicha división mientras que el 65.5% respondió por la negativa. El resto (2 encuestados) manifestó no tener conocimiento. El resultado permite entender que resultaba relativamente inusual, en el momento de la encuesta, que las empresas de telecomunicaciones destinaran recursos específicos para esta actividad y por lo tanto reutilizaban recursos (humanos y físicos) de otras áreas. Algo similar se recolectó durante las entrevistas a los informantes-clave donde los expertos declararon que aquellos que diseñaban y programaban las herramientas eran parte del personal existen del área de IT.

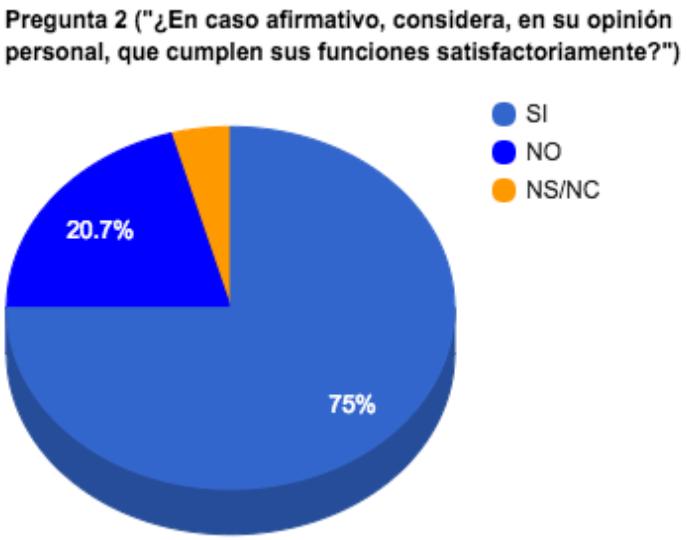
**Gráfico 6 - Presencia de áreas especializadas de antifraude en las organizaciones**




*Fuente: elaboración propia (2016)*

Asimismo, pocos de los representantes de las empresas parecían estar satisfechos con el resultado obtenido de esas áreas, lo que se infiere del contundente 75% que representa a aquellos encuestados que se inclinaron por la negativa en la segunda pregunta, mientras que solamente el 20.7% se mostró satisfecho.

**Gráfico 7 - Nivel de satisfacción con las áreas antifraude**




*Fuente: elaboración propia (2016)*

La tercera pregunta intentó encontrar cuáles son las pérdidas que sufrían las empresas ocasionadas por estafas vinculadas con el servicio telefónico. Los resultados obtenidos deben ser entendidos a la luz de dos limitaciones: La falta de conocimiento del encuestado sobre el número real de perdidas y la decisión del encuestado de transmitir esta información sensible, aún bajo el paraguas del anonimato. Los resultados obtenidos se reproducen a continuación.

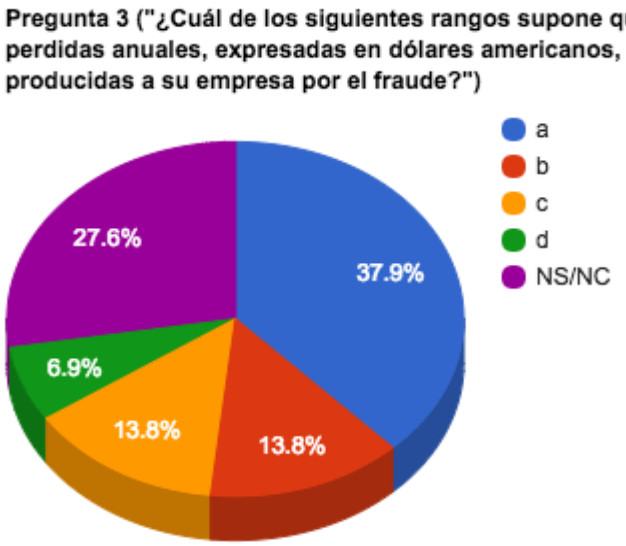
**Cuadro 7 - Pérdidas anuales (estimadas) ocasionadas por fraudes**

| Resultados pregunta 3 | % |
|---|---|
| **a: 0 a 100.000** | 37.93% |
| **b: 100.000 a 500.000** | 13.79% |
| **c: 500.000 a 1.000.000** | 13.79% |
| **d: mas de 1.000.000** | 6.90% |
| **NS/NC** | 27.59% |

*Fuente: elaboración propia (2016)*

A primera, vista los resultados podrían interpretarse afirmando que los montos de las perdidas ocasionados por defraudaciones fueron mas reducidos que grandes, pero esto no contempla cuanto impactó el monto de las perdidas en la facturación total de la empresa, y así para poder medir la relación facturación-perdida.

**Gráfico 8 - Perdidas anuales (estimadas) ocasionadas por fraudes**




*Fuente: elaboración propia (2016)*

Para que sea más enriquecedor el análisis de la información, las respuestas obtenidas pueden ser re-ordenadas de la siguiente forma para intentar llegar a una nueva hipótesis binaria:

**a**. Quedarse solo con aquellas encuestas que donde alguna de las opciones fue elegida, o sea descartando a quienes no contestaron por ningún rango.

**b**. Interpretar a quienes respondieron con el rango inferior (0 a 100.000 dólares estadounidenses) como "pueden no haber tenido fraude" dado que este rango contiene al cero, o sea el no se presentó ningún fraude.

**c.** Sumariar los restantes tres rangos e interpretarlos como "han tenido algún fraude".

De esta forma los mismos datos pueden verse como a continuación:

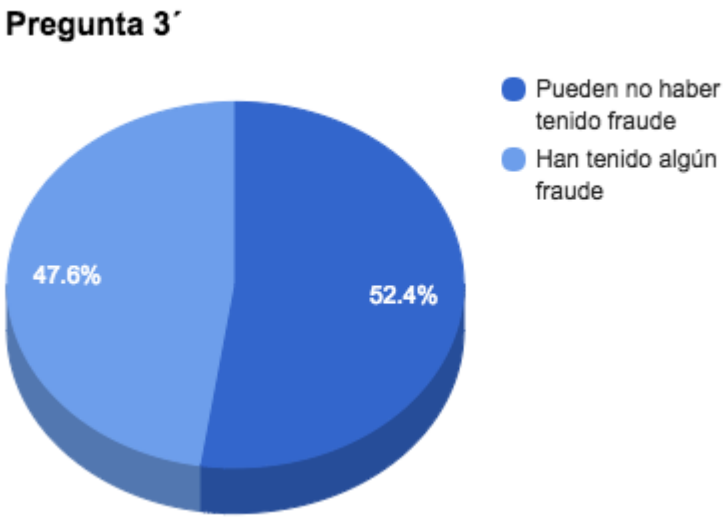
**Cuadro 8 - Presencia de fraude telefónico en las empresas**

| Resultados pregunta 3´ | % |
|---|---|
| **Pueden no haber tenido fraude** | 52.38% |
| **Han tenido algún fraude** | 47.62% |

*Fuente: elaboración propia (2016)*

Donde casi la mitad de los encuestados (47.62%) afirmó la hipótesis que tuvieron al menos un fraude anual, demostrando que el fraude es presente en la industria.

**Gráfico 9 - Presencia de fraude telefónico en las empresas**




*Fuente: elaboración propia (2016)*

La cuarta pregunta buscó encontrar cuál es el volumen de dinero que facturan las empresas provenientes de la unidad de negocios de telefonía. Las mismas limitaciones de la pregunta anterior aplican en esta (falta de información y temor sobre la divulgación de información sensitiva), pero por lo observado en mayor medida. El número de encuestados que dejó esta

pregunta en blanco fue del 62.1% (frente al 27.6% de la pregunta anterior). Se debe agregar que puede ser complejo decidir que conceptos son los relacionados con el servicio de telefonía en si, dado que muchos operadores venden sus servicios de Internet, telefonía y televisión en un mismo paquete.

Obviamente, aquellos que contestaron que su empresa sufría mayores pérdidas anuales también indicaron que estas compañías poseían mayores ingresos relacionados al área, por lo cual el nivel de fraude proporcional acompaña al nivel de facturación de la unidad de negocio.

**Gráfico 10 - Facturación anual (estimada) para la unidad de telefonía**


*Fuente: elaboración propia (2016)*

Prosiguiendo con los datos de esta pregunta, y eliminando del análisis estadístico aquellas encuestas donde no se contestó por alguna de las opciones, se pueden re-ordenar los resultados de las encuestas de la siguiente forma, donde se extrae que existía presencia de

empresas de tamaño pequeño y grande mayoritariamente. A la luz de los resultados es posible que las escalas de facturación -arbitrariamente elegidas- puedan haber distorsionado, o guiado, las respuestas.

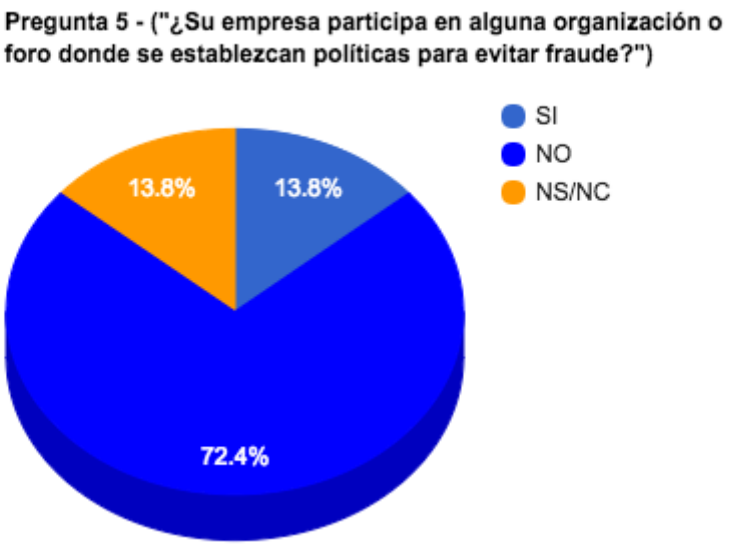
**Cuadro 9 - Facturación anual (estimada) declarada para la unidad de telefonía**

| Pregunta 4' | % |
|---|---|
| **a: 0 a 500.000** | 45.46% |
| **b: 500.000 a 1.000.000** | 18.18% |
| **c: 1.000.000 a 5.000.000** | 9.09% |
| **d: mas de 5.000.000** | 27.27% |

*Fuente: elaboración propia (2016)*

Un dato interesante, que también fue analizado en el Marco Teórico y durante las entrevistas a los informantes-clave, es la baja presencia de foros o agrupaciones de interés relacionadas con el fenómeno del fraude en telefonía. Si bien fueron detectadas tales comunidades en los Estados Unidos y Europa durante la investigación teórica, no se encontraron presencias similares locales o regionales. En concordancia a esta tendencia la encuesta brindó como dato que solo el 13.8% de las empresas participaba en tales foros, mientras que el restante 72.4% no lo hacía. Una cierta cantidad, no menor, de encuestados directamente no respondió esta pregunta, indicando que no tenía conocimiento sobre esa información. Es posible que el conocimiento de esta información no sea corriente dentro de las organizaciones.

**Gráfico 11 - Participación en agrupaciones de interés**




Fuente: elaboración propia (2016)

Existe la posibilidad de realizar un análisis más profundo de las respuestas a la quinta pregunta. Si se considera solamente aquellas encuestas donde se respondió en la primera pregunta que la empresa contaba con un área especializada en fraude (8 empresas respondieron de forma positiva), entonces el 37.5% de ellas participaba en agrupaciones creadas para esta temática, lo que muestra que existía correlación entre la presencia de personal especializado y la participación en agrupaciones de interés.

**Gráfico 12 - Participación en agrupaciones de interés de las empresas que poseen áreas especializadas**


Fuente: elaboración propia (2016)

De forma similar, es posible quedarse solo con las encuestas donde la respuesta a la cuarta pregunta ("*¿Cuál de los siguientes rangos supone en que se encuentra, expresada en dólares americanos, la facturación de su empresa anual para la unidad de telefonía?*") se indicó el tope de escala para la facturación del área de telefonía (respuesta "*d*"). Se puede inferir que estas encuestas representan a empresas de mayor tamaño, dado que su facturación es mucho mayor que las otras. Siendo así, es esclarecedor notar que el 50% de estas empresas de mayor tamaño participaban en foros sobre el tema investigado, lo cual parece un resultado lógico dado que seguramente poseían más recursos para invertir.

Otro corte en la matriz de datos de interés surge de, nuevamente, mantener el subconjunto de aquellas encuestas donde la respuesta a la cuarta pregunta el representante indicó el tope de escala, pero verificar en estas la presencia de una unidad especializada para el tratamiento del fraude (pregunta 1 con valor afirmativo). Realizando lo dicho, se encuentra que el 100% de las empresas que declararon las facturaciones más altas, poseen unidades operativas

especializadas. Esto también posee coherencia, dado que empresas más grandes, al poseer más recursos (y más riesgos) podían asignar personal y equipamiento específicos para esa tarea. Nuevamente, el factor volumen de facturación como *proxy* para entender tamaño parece indicar mayor madurez en el combate contra el fraude.

Prosiguiendo con el análisis cuantitativo de la sexta pregunta, esta estuvo enfocada a averiguar la posición de las empresas sobre el cuidado preventivo de sus usuarios. Lamentablemente la mayoría de las empresas (86.2%) respondieron negativamente a esta respuesta, indicando que dejaban a los clientes la implementación de buenas prácticas de cuidar de su infraestructura de telefonía. Esto no es una decisión sabia, pues como se vio en apartados anteriores, gran cantidad de los fraudes se originan por secuestro (*hacking*) del equipamiento de los clientes, quienes al usualmente no poseer conocimiento técnico avanzado en la materia, son vulnerados fácilmente por los atacantes. No parece existir diferencia si se realiza una segmentación de información por tamaño de empresa.

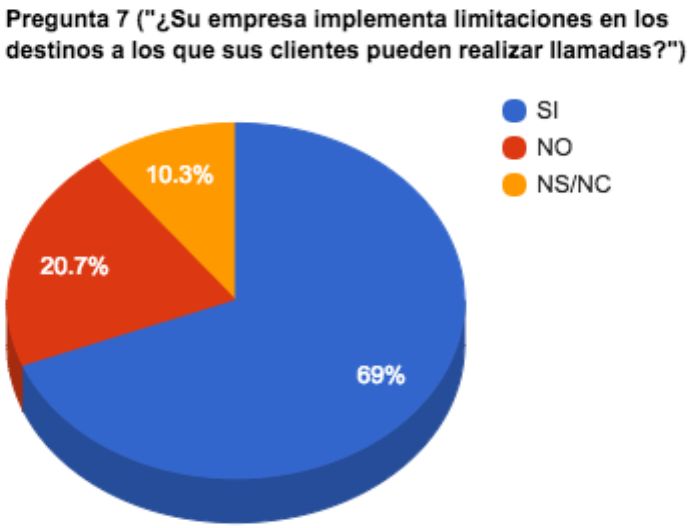
**Gráfico 13 - Presencia de procesos para evitar proactivamente el secuestro del equipamiento telefónico de los usuarios**


Fuente: elaboración propia (2016)

La pregunta séptima también fue orientada a conocer las medidas que toma el operador telefónico para protegerse, tanto a él como al cliente, del fraude que pueda originarse desde el lado cliente. De las entrevistas a los informantes-clave, y de la propia experiencia, se conoce que aquellos destinos donde la tarifa de la llamada es mas alta es a la vez más atractiva para los defraudadores, dado que con menor número de llamadas pueden generar mayor rentabilidad ilegítima. Esta realidad es conocida por las operadoras telefónicas y por lo tanto suelen limitar la posibilidad que los usuarios generen llamadas a estos destinos, al menos sin previa gestión individual, y el consiguiente proceso de verificación sobre la veracidad de la necesidad y la posición crediticia del usuario.

Del análisis de las respuestas obtenidas es claro que esta política preventiva era ampliamente compartida (69%) en todas las empresas, sin importar su tamaño. La limitación de destinos inusuales es una práctica común en la industria.

**Gráfico 14 - Presencia de limitaciones en cuanto a destinos habilitados.**




Fuente: elaboración propia (2016)

Con el objeto de recabar información sobre el fraude por suscripción, y recordando que es aquel donde el cliente falsea su identidad con el objetivo de no pagar la factura de servicios, se generó la octava pregunta, en la que se preguntó –directamente- por este escenario, el cual es plenamente conocido en la industria.

La gran mayoría de las encuestas reflejaron conocimiento y confianza en el proceso de alta de nuevos clientes, mostrando que las empresas estabna al corriente de los riesgos relacionados con la falsificación de identidad y asignaban recursos a implementar procesos para minimizarlos.

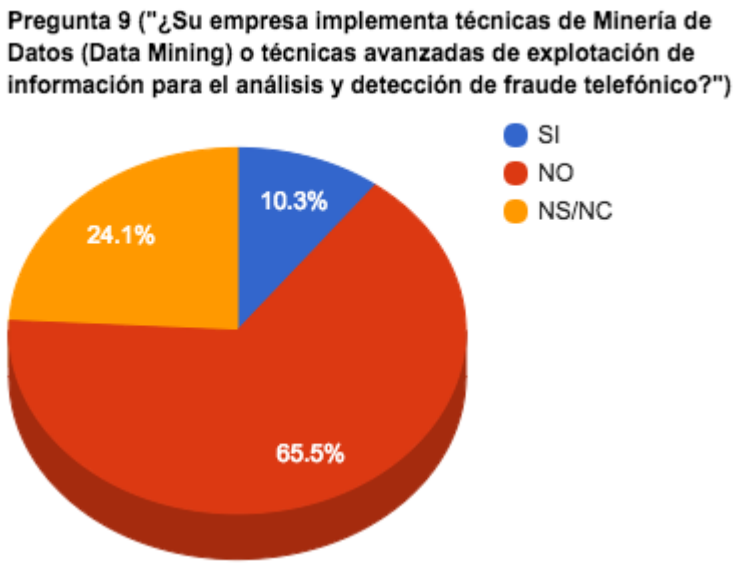
**Gráfico 15 - Presencia de procesos para la detección del fraude de suscripción**


Fuente: elaboración propia (2016)

Finalmente, la novena y última pregunta se orientó a entender si existe conocimiento sobre implementaciones de herramientas antifraude que utilicen técnicas avanzadas de estadística, minería de datos, redes neuronales u otras tecnologías que aprovechen los grandes volúmenes de información que genera diariamente una empresa de telecomunicaciones. Se encontró que la gran mayoría declaró que no eran utilizadas en su organización o desconocían sobre su

existencia (representando el 89.7% de las encuestas si se toman quienes contestaron de forma negativa y quienes no contestaron esa pregunta)

**Gráfico 16 - Presencia de técnicas estadísticas en el análisis y detección de fraude**




Fuente: elaboración propia (2016)

*Conclusiones de las encuestas*

A partir de las encuestas realizadas, se ha llegado a las siguientes conclusiones:

- Pocas empresas de telecomunicaciones poseían áreas especializadas para el análisis, prevención y combate del fraude. Por lo general, sólo aquellas que tenían mayor tamaño, poseían la madurez para alocar recursos dedicados a estas tareas. Las empresas de telefonía más pequeñas (por ejemplo, los cableoperadores del interior) no han podido acceder a este lujo, pero potencialmente podrían realizar un *outsourcing* de esta función y obtener beneficios similares sin inversión de capital.

- La insatisfacción con las tareas del área encargada de la gestión del fraude representa la necesidad de mejorar esta función. También, representa la oportunidad de poder ofrecer servicios de consultoría profesional u *outsourcing* de este trabajo. La generación de buenas prácticas generalizadas y compartidas podría beneficiar fácilmente a la industria.
- La mayoría de las empresas declararon tener ocurrencias de fraude por algún valor.
- Al momento de la encuesta no existían o no se conocían por parte de los encuestados grupos de interés, foros o cámaras focalizadas en el fraude que den participación a los actores de la industria local o regional. Aquellas empresas que contestaron de forma positiva respecto a su participación en esos grupos en su mayoría fueron empresas de gran tamaño y es posible que tuvieran participación a través de sus casas matrices.
- Casi todas las empresas demostraron consciencia de la necesidad de limitar proactivamente a qué países pueden comunicarse sus abonados, implementando "listas negras" que incluyan los destinos de mayor costo, y por lo general, menos comunes para las comunicaciones del usuario típico.
- Asimismo, la mayoría de las empresas mostraron tener implementados procesos para verificar la identidad de los abonados y su capacidad crediticia.
- Por último, las herramientas informáticas que transmitieron usar la gran mayoría de los representantes encuestados no hacía uso de las tecnologías recientes que les podrían brindar mayor eficiencia y valor agregado.

## IV. 4 Conclusiones del Marco Investigativo

- El fraude posee un impacto grande en la industria y es uno de los factores que más vulnera la utilidad de las empresas. Aún así, su gestión no siempre posee los recursos necesarios o la visión estratégica adecuada para utilizarlos.
- Existe una clara tendencia en las empresas a resolver los problemas de fraude puertas adentro, con baja colaboración entre los actores del segmento. La cooperación es tan pequeña que los perpetradores pueden mover su conducta delictiva de operador telefónico a operador telefónico sin sufrir las consecuencias. Esto ha generado un negocio permanente donde gran cantidad de personas viven del fraude a la industria de la telefonía. La falta de foros o grupos donde la temática sea tratada no hace más que demostrar la falta de cooperación.
- Las herramientas informáticas que se utilizan en las empresas son de elaboración propia, producidas de forma reactiva a los eventos sufridos. No se encontró que para desarrollarlas se incorporaran perfiles con experiencia en el tema, sino que las técnicas fueron evolucionando siguiendo al problema, pero nunca intentando predecirlo. El personal que suele implementar estas herramientas es IT, pero no es el totalmente indicado, por no tener una visión global del negocio.
- Siguiendo con las herramientas, pocas tiene una evolución mayor a predecir el consumo total del usuario por adelantado e implementar un corte predictivo. La otra técnica utilizada es el bloque preventivo de países que posean tarifas de telefonía alta.
- No se destinan recursos especializados al análisis y/o prevención del fraude. Los recursos provienen “prestados” de otras áreas, y por lo general, solo luego de un evento de fraude, que fuerza a que esta realidad sea atendida con prioridad.
- Existe espacio para ofrecer este servicio de forma consultiva, brindando tanto servicios profesionales como tecnología. Aún las empresas de mayor tamaño que ya

tienen áreas especializadas lo hacen. Es posible que para las empresas medianas y pequeñas la cultura de externalizar funciones no sea tan presente.

En el presente Marco Investigativo se han expuesto las técnicas de recolección de datos de campo utilizadas. En el siguiente capítulo, se expondrán las conclusiones del trabajo realizado, las propuestas y los aportes para futuras investigaciones.

# V. CONCLUSIONES GENERALES, PROPUESTAS Y APORTES PARA FUTURAS INVESTIGACIONES

El presente trabajo pretendió, por un lado, analizar el estado del arte en cuanto a tecnologías informáticas referidas al análisis del fraude en la industria de la telefonía, en especial aquellas que incorporan modelos ayudados por técnicas de minería de datos y/o modelos probabilísticos que se apalanquen en la creciente potencia computacional existente. Por otro lado, buscó entender cuáles son los procesos que implementan las empresas para rescatar sus mejores prácticas, compilarlas y, a la vez, ofrecer optimizaciones, agregando las antedichas herramientas de última generación.

Con tal fin, además de realizar un análisis del pensamiento de distintos autores a través de sus publicaciones, se realizó un revelamiento en campo del tema, utilizándose varios métodos de recolección que permitieron generar una razonable descripción de los usos y costumbres locales. La integración de estas etapas permitió llegar a las conclusiones, propuestas y aportes para futuras investigaciones que se desarrollan en los siguientes aparados.

## V.1 Conclusiones

*Respecto del estado del arte en tecnologías y prácticas*

Vivimos un periodo de gran actividad productiva, apalancada por la vertiginosa aparición diaria de nuevas tecnologías. Ciertas tecnologías que podrían parecer no alcanzables por los próximos siglos están al filo de ser una realidad comercial accesible al público general: impresión 3D, traducción en vivo, automóviles auto-manejados, ciber-vigilancia y sistemas

informáticos que son capaces de entender el lenguaje humano y ofrecer respuestas. La lista podría continuar, aunque -ante este escenario- deviene difícil creer que actividades tan metodológicas e históricas como el fraude no puedan ser fácilmente solucionadas por sistemas inteligentes.

La mayoría de las fuentes utilizadas durante el Marco Teórico coinciden en la tendencia que existe en el reemplazo de tareas rutinarias humanas por algoritmos cada vez más eficientes, dejando la participación humana el diseño yla interpretación avanzada del resultado de estos algoritmos. El abaratamiento progresivo del poder computacional, el ancho de banda en la conectividad a Internet y el almacenamiento de datos, permiten generar nuevos algoritmos cada vez más eficientes y económicos. En la misma dirección, la colaboración en diversos aspectos: datos e información, códigos de lenguaje de programación reutilizables, servicios en la nube gratuitos, entre otros, permite apalancar muchos procesos y enriquecerlos con bajas inversiones iniciales.

Por otro lado, es importante recordar que existe un incremento exponencial en la generación de datos. En primera medida, los dispositivos que generan datos se han visto multiplicados, desde los equipos personales como *smartphones* y televisores, hasta el equipamiento profesional de redes generan crecientes volúmenes de información. Por otro lado, los usuarios –también- poseen más canales de comunicación por donde generar nuevos datos; finalmente, todos estos datos suelen ser compartidos, transmitidos y almacenados. Toda esta abundancia de información permite censar -mediante nuevas herramientas- el comportamiento de las personas y -de estas observaciones- es posible crear modelos para predecir sus actos futuros. En relación a esta investigación, el comportamiento a identificar y predecir es el fraude.

En relación con esto último, se descubrió la importancia de monitorear el comportamiento de los usuarios a través de los múltiples canales y sistemas a través de los cuales éstos interactúan con la empresa. Por ejemplo, y solo considerando los procesos de atención al cliente, los usuarios pueden consultar con el operador mediante la web, pueden llamar al *call center* de la empresa, visitando puntos de servicio presenciales y –hasta- mediante comunicaciones por Whatsapp. La optimización de procesos debe tener en cuenta estas diferencias. Las implementaciones que ven cada canal de contacto como "silos" desarrollados al rededor de un canal especifico o reglas de negocio especificas no permitirán tener la visión completa de la problemática, tanto en la industria de la telefonía o en cualquier otra, ya sea para la gestión del fraude o para otras gestiones criticas.

Se han investigado distintas técnicas de detección de conductas anormales. Muchas se basan en la definición de un "usuario promedio" (o un "proveedor promedio", dependiendo el escenario de fraude a detectar) y luego la comparación de los datos contra este patrón. Las actividades que se alejan de esta media pueden ser calificadas como anormales o, en este caso, como fraudulentas. Por el contrario, otras técnicas definen patrones típicos de fraude y buscan comparar los datos contra estos patrones. Si la actividad observada se parece a este patrón es posible considerarla como fraudulenta. La mayoría coincide en que es imposible determinar la legitimidad o no de una llamada telefónica de forma individual y -solo entendiendo comportamientos en el tiempo- es posible clasificar al abonado como un defraudador o no.

También, se han encontrado diversas herramientas de software que permiten hacer minería de datos sobre los grandes conjuntos de datos que poseen las empresas. La capacidad de almacenamiento y creación de *datawarehouses* permiten analizar los datos existentes y

encontrar patrones. El hallazgo de patrones de conductas permiten rediseñar los modelos para mejorar su eficiencia de detección. Cuando los conjuntos de datos son más ricos, heterogéneos y poseedores de información periódicamente actualizada resulta posible encontrar patrones más complejos.

Un dato de importancia fue la baja representatividad en el material teórico encontrado de modelos dinámicos. El poseer sistemas cuyos modelos son independientes del conocimiento de la función de distribución del objeto de análisis simplifica y reduce los tiempos de investigación humano. Se ha visto que existe un incipiente número de aplicaciones de *Real Time Decision* (RTD) que pueden ser la base de sistemas completamente automatizables, requiriendo poco o ningún esfuerzo manual para la construcción y mantenimiento de sus modelos predictivos. Estas soluciones, en contraste con las soluciones clásicas de obtención de patrones como la minería de datos, permiten aprender de cada transacción con el cliente y/o proveedor y, automáticamente, actualizar sus modelos predictivos en tiempo real.

Al contrario de técnicas analíticas como reglas de negocio estáticas, minería de datos o estadísticas, estos sistemas de RTD permiten mejorar la velocidad de respuesta general de la organización mediante la observación de los flujos en el tiempo de las interacciones individuales de cada cliente y/o proveedor. El aprendizaje basado en cada interacción y la capacidad de ajuste de procesos en tiempo real, permite tomar el mejor curso de acción en cada nueva oportunidad. La implementación de este tipo de paradigma no solo reduce el costo administrativo, sino que también elimina la demora en el ciclo de: hallazgo de nuevos datos - desarrollo o mejora del modelo predictivo - puesta en producción del nuevo modelo.

Una de las mayores dificultadas en todas las técnicas investigadas es el entrenamiento inicial de los sistemas de gestión del fraude. La dificultad se centra en poder asegurar con absoluta seguridad que un cierto tráfico de llamadas es carente de acciones presentes o futuras de fraude.

En contraste de los que se analizó en el Marco Teórico, la herramientas informáticas relevadas en campo no acompañan al estado del arte. La mayoría fueron desarrollos propietarios, realizados sin la colaboración del resto de la industria y atendiendo solo a las problemáticas internas. También, fueron pocos los que pudieron visualizar el poder de paradigmas de inteligencia artificial para el aprendizaje y catalogación del tráfico de llamadas. De similar forma, los sistemas informáticos encontrados no poseían ninguna realimentación en tiempo real de los nuevos datos generados. Los modelos predictivos básicos desarrollados por los sectores informáticos eran estáticos en el tiempo y no poseían auto-aprendizaje, necesitando de una nueva iteración manual para detectar un escenario nuevo de fraude. De esta forma, los modelos creados se encuentran destinados a quedarse siempre rezagados ante las innovaciones e inventivas de los defraudadores.

Otro punto a mencionar es que fueron pocas las empresas que exploraron o tenían pensado explorar en servicios tercerizados que ofrecieran herramientas de gestión de fraude en modalidad de servicio. Si bien es cierto que lo datos requeridos para su detección son -muchas veces- sensibles y otras directamente privados, un subconjunto de la información, correctamente pre-procesada para minorizar su contenido podría ser externalizado a empresas que brinden servicios de detección de fraude. La ventaja de convertir costos de inversión en investigación y desarrollo, versus costos operativos, ayudaría enormemente a las empresas del sector.

Es claro, que uno de los principales impedimentos que encuentran las empresas cuando intentan detectar el fraude se refiere a la variedad de escenarios y sub-escenarios posibles. Esto se acentúa, por un lado, por la rapidez con que aparecen nuevas técnicas, y por otro, porque –además- los defraudadores también se ven beneficiados por el abaratamiento de la tecnología de comunicaciones. Sin recursos dedicados para la inversión en herramientas de software *World class* o en la formación de un equipo propio para la creación interna de estos sistemas, es una misión difícil la detección certera – y temprana – del fraude.

Los encargados de generar sistemas antifraude dejaron ver que entendían el diseño de estas herramientas desde el paradigma clásico de la programación, o sea el modelar matemáticamente el problema en cuestión y posteriormente formular una programa solución que posea una serie de propiedades que permitan resolverlo. En contraposición, la aproximación propuesta parte de un conjunto de datos de entrada suficientemente significativo (llamadas fraudulentas y llamadas no fraudulentas) y su objetivo es conseguir que aprenda automáticamente las propiedades deseadas y generé el sistema de clasificación fraude/no-fraude por si mismo.

*Respecto a la incidencia del fraude en la industria telefónica*

Existen dos afirmaciones importantes a verificar en esta investigación.

La primera se refería a verificar si el problema analizado era significativo en el presente y si lo sería siendo en el futuro cercano. Esta hipótesis es importante porque condicionaría cualquier inversión de tiempo o capital en desarrollar prácticas o herramientas para la solución del dilema.

Tanto en la investigación práctica como la teórica se pudo apreciar que la incidencia del fraude sobre las utilidades de las empresas de comunicaciones es grande. Se pudieron determinar la veracidad de las siguientes afirmaciones:

- No distingue tamaños de empresas. Lo sufren tanto empresas pequeñas como grandes. Tanto aquellas que se dedican exclusivamente a brindar servicios de telefonía, como aquellas que solo lo brindan como valor agregado a otro servicio.
- No distingue países. El impacto es global y por lo general una misma ocurrencia de fraude puede afectar más de un país y organización al mismo tiempo.
- No es un problema que decrezca en el tiempo. Todo lo contrario, posee un aumento en valor absoluto de perdidas, y también en la cantidad de organizaciones que lo sufren.
- Es agnóstico a la tecnología de base que se utilice para prestar el servicio. Es posible que lo sufran tanto empresas que brindan telefonía fija tradicional mediante circuitos TDM[31], empresas que brindan el servicio mediante paquetes de datos a través de Internet o empresas de telefonía móvil. Todas ellas poseen vulnerabilidades generales y especificas que las hacen victimas de las redes de defraudadores.
- Las organizaciones se encuentran mal equipadas para combatir el fraude. Todas son consientes de su existencia, pero por lo general no dedican recursos necesarios en relación al impacto que les ocasiona.

La segunda de las afirmaciones compete a la continuidad de la industria y los servicios que presta. En los servicios de comunicaciones existe gran volatilidad y escepticismo respecto a

[31]**TDM (Time Division Multiplexing):** técnica que permite la transmisión de señales digitales donde el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).

que negocios seguirán prestándose dentro de cinco o diez años. La innovación constante se ha acelerado en la última década, apareciendo –recurrentemente- tecnologías de comunicaciones que desplazan a tecnologías anteriores. Cabe recordar que una tecnología relativamente reciente como el correo electrónico oscila entre el crecimiento vegetativo y el estancamiento de su base de usuarios.

Esta situación de cambio acelerado, hace preguntar sobre el futuro del servicio telefónico tal como se brinda hoy en día. De la investigación puede desprenderse lo siguiente:

- El servicio de telefonía fija esta en contracción, pero la telefonía móvil aún tiene crecimiento.
- Existen nuevas tecnologías de base que permiten brindar un servicio similar, pero adaptándose a los nuevos usuarios (Skype y Google Voice, entre otros.).
- La longevidad de la telefonía ha ocasionado que se encuentre enraizada en muchos aspectos de la vida cotidiana (sistemas de bomberos, policía, oficinas corporativas, otros.) y su sustitución no será una tarea corta.
- En relación con lo anterior y debido a las décadas en actividad de la telefonía, es una de las pocas tecnologías de comunicaciones con estándares maduros y ampliamente adoptados a nivel global.

En síntesis, la problemática posee un gran impacto actual en la actividad de las organizaciones y se estima que lo seguirá teniendo en el futuro cercano. Por ende, se sustenta la necesidad de esta investigación y la posterior asignación de recursos para mejorarla. Como comentario final, resulta importante notar que lo investigado para la industria de las

telecomunicaciones puede ser adaptado a otros procesos informatizados de otras industrias que sufran el mismo flagelo:

- Banca minorista.
- Tarjetas de crédito.
- Financiamiento de salud y medicamentos.
- Seguros.
- Ciberseguridad nacional.
- Otros

## V.2 Propuestas

*Buenas prácticas en materia de procesos*

Los procesos internos de altas, bajas y modificaciones de los usuarios - y de sus servicios - serán siempre específicos de cada organización aunque -luego de lo investigado- se pueden proponer algunas características que deben ser consideradas a la hora de su implementación:

1. Existencia de validaciones extensivas sobre la identidad del abonado al menos durante las siguientes interacciones entre este y la empresa de servicios:

    a. Alta de un nuevo cliente. Es el momento más sensible y donde mayor foco debe ponerse en verificar la verdadera identidad del potencial nuevo usuario de servicio.

b. Consultas técnicas sobre el servicio. La información técnica sobre el servicio puede ser peligrosa en manos de estafadores profesionales. El brindarla debe estar precedida de la validación de la identidad cliente.
c. Cambios técnicos del servicio. Aún más críticos que la consulta de detalles técnicos sobre servicios, son las solicitudes de cambios sobre estos detalles.
d. Modificación de datos personales y/o de facturación. Los cambios de datos básicos del cliente deben ser cuidadosamente alterados y solo valiéndose de buenas pruebas de acreditación de la veracidad del cliente.

La validación debe intentar agrupar la mayor cantidad de datos que permitan validar la identidad real del cliente. Datos clásicos como número de documento, identificador tributario (CUIT), nombre/apellido, edad, dirección de residencia y otros, pueden no ser suficientes por encontrarse fácilmente online mediante exploración sencilla en un motor de búsqueda (Google, Bing, Yahoo, otros). En la era de la información, resulta posible utilizar métodos complementarios que agreguen la utilización del *home banking*, la mayoría de las empresas orienta a sus clientes a la compra, pago y gestión de los servicios de forma remota. Lo canales adicionan veracidad al resultado del proceso. Algunos de los posibles son:

- Validación de la identidad en redes sociales (Linkedin, Twitter, Facebook, etc.).
- Utilización de servicios de terceros. (Ejemplo: Clave Fiscal de AFIP).
- Utilización de micro-pagos reembolsables con tarjetas de crédito.

Un dato de importancia a ser considerado es el incremento de la gestión de trámites remotos. Al igual que los bancos intentan llevar a sus usuarios apara la autogestión o gestión no presencial pueden ser variados: a través de Internet, mediante mensajes SMS, terminales de autoservicio en lugares públicos o semipúblicos, llamadas telefónicas, otros. En todos ellos el usuario no interactúa físicamente con un representante de la empresa sino que lo hace a través de alguna tecnología de comunicación. Entendiendo que este paradigma es una tendencia general, los procesos de validación de identidad deben ser ajustados para poder interactuar con clientes que tal vez nunca visten presencialmente oficinas del operador.

2. Investigación de la capacidad crediticia del cliente. La segunda pieza clave en un proceso comercial es la validación crediticia de la persona física o empresa que contratará los servicios. Por lo general existen servicios privados que brindan esa información (quebrantos, cheques rechazados, juicios, etc.) y estos deben ser incorporados como un paso dentro del camino crítico del proceso. Es de vital importancia poder mesurar el riesgo de incobrabilidad que posee cada cliente, y este deberá tener una relación con el máximo crédito en servicios que se le permita consumir dentro de un periodo de facturación.

3. Implementación de una mesa de operaciones destinada a la gestión de fraudes. Se recomienda la existencia de una mesa de operaciones que atienda las alertas generadas por las herramientas que controlan el tráfico de llamadas y predicen la probabilidad de fraude. El proceso de gestión debe incluir, indefectiblemente, un equipo que tenga asignada esta tarea. Es posible que la empresa no posea la envergadura para solventar un equipo de operaciones destinado a dicho fin, por ende esta función deberá ser

sumada a otra mesa de operaciones ya existente. Esta función puede ser agregada a las funciones del SOC[32], el NOC[33], o del centro de atención al cliente.

En relación con lo que se relevó en el Marco Investigativo, se tomó conocimiento que -si bien los intentos de fraude pueden ocurrir en cualquier momento- los atacantes tienen especial predilección por horarios no convencionales. Dado que poseen conocimiento que las empresas poseen menos personal en horarios de fines de semana o madrugadas, suelen concentrar sus ataques en esos momentos. Por lo tanto, es imprescindible que el área que posea delegada la función de recepción de alertas posea operadores 7x24.

4. Generación de un listado de escalamientos claros ante alertas de fraudes. Los sistemas de alertas deben notificar a la Mesa de operaciones instantáneamente, pero esta debe poseer un proceso claro por el cual escalar hacia arriba cualquier escenario que no se claro o que genere dudas sobre la decisión a tomar. Los incidentes no deben poder terminar en puntos muertos donde ningún área de la organización lo tome para sí. Por otro lado, el proceso de escalamiento debe poseer tiempos máximos donde, ante la inactividad del incidente reportado por una determinada cantidad de tiempo, este sea escalado a un nivel superior de forma automática.

[32]**SOC** (Security Operations Center). El SOC o Centro de Control de Seguridad es un equipo centralizado de personas responsable por la seguridad informática de la empresa.
[33]**NOC** (Network Operation Center). El NOC o Centro de Control de la Red es el equipo de personas responsable de monitorizar las redes de una empresa, en búsqueda de alarmas, patrones o condiciones que requieran atención humana con el objetivo de mantener los servicios siempre en condiciones de funcionamiento óptimas.

5. Auditoria internas y controles. Tal como se vio en el Marco Teórico muchos escenarios de fraude requieren connivencia de sectores internos en las empresas de telefonía.

   - Los sectores comerciales deciden el precio al que se venden los servicios a los clientes. Estos pueden vender a precios mas baratos si poseen arreglos personales con la parte compradora.
   - Los sectores técnicos poseen acceso a las plataformas de servicio. Estos pueden brindar servicios que nunca serán facturados, alterar registros, generar altas fraudulentas, reasignar cobros de un cliente a otro y otra variedad de acciones que de no mediar su acción un defraudador externo no podría acceder.
   - Los sectores de producto o compra de destinos telefónicos. Estos habitualmente arreglan con otros operadores interconexiones por las cuales enviar llamadas. En sus manos recae la autoridad para arreglar precios, cantidades, tiempos, calidades y condiciones. Dentro de esta área bien pueden generarse arreglos que perjudican a la organización.
   - Otros sectores como facturación o administración que están dentro del proceso facturación-cobranza también pueden verse envueltos en procesos de fraude.

   Los sectores citados y cualquier otro donde el proceso puede ser corrompido, deben poseer auditorias recurrentes, abarcando tanto el diseño del proceso en sí como muestras aleatorias de ocurrencias del proceso mismo. Aquellos puntos del proceso que sean críticos, como la carga de precios, deben poseer dobles o triples chequeos por operadores distintos. Por otro lado, es crítica la separación de

funciones y roles, donde una misma persona no debe poseer atribuciones sobre distintas partes del proceso que estén destinadas ser elementos control. Desde el plano de la seguridad informática, cada empleado debe poseer credenciales de autenticación fuertes que eviten la falsificación de la identidad.

*Buenas prácticas en materia de herramientas informáticas*

Toda empresa del sector de comunicaciones que brinde servicios con costos y facturación variable debe poseer la plena conciencia que puede sufrir intentos de defraudación. Aún cuando venda sus servicios en modalidad de tarifa plana muy probablemente sus costos no serán solamente fijos, sino que tendrán una fuerte incidencia variable de la cantidad de tráfico telefónico que sus usuarios cursen mensualmente. Se cual fuere el escenario es una necesidad la implementación de herramientas informáticas que consoliden la totalidad de información de sus clientes y que apliquen análisis de patrones.

De lo relevado en el Marco Investigativo se entiende que existen algunas prácticas comunes en casi todos los operadores telefónicos y que deben ser implementadas por la totalidad del sector:

- *Limitación de aquellos destinos (países, regiones, tipos de numeración, otros) que por su alta tarifa por minuto son atractivos para los delincuentes:* Dado que los defraudadores saben que tarde o temprano serán detectados, su preferencia se encuentra en aquellos destinos donde, por el alto valor de la tarifa, puedan generar mayor margen en la menor cantidad de tiempo. Por esta razón, y como se vio en el Marco Investigativo, las empresas de comunicaciones suelen restringir de facto a sus usuarios la posibilidad de comunicarse con estos destinos. Solo ante un pedido

expreso del abonado estos destinos deberían ser habilitados. Estas solicitudes de habilitación deben quedar registrados en los sistemas del operador y a disponibilidad de los sistemas informáticos de análisis de patrones que se discutirán más adelante. En el Anexo IV se incluyen los destinos que se recomienda no permitir comunicaciones debido a estar comúnmente asociados a escenarios de fraude.

- Límites de crédito: Cada usuarios debe poseer un límite máximo de crédito máximo disponible en cada período de facturación. En servicios que son postpagos el pago del servicio al finalizar el período se basa en la confianza que el cliente finalmente pagará lo adeudado por su consumo. Se recomienda entonces el implementar límites de crédito a cada cuenta y el bloqueo del servicio al traspasar ese umbral. El límite particular de cada usuario puede ser distinto dependiendo de varios factores:

    - Historial de pagos y tiempo de permanencia como cliente de la empresa.
    - Depósitos o avales que sirvan como garantía de pago.
    - Envergadura económica-financiera comprobable del cliente.
    - Otros servicios contratados por el cliente.
    - Otros.

  De la misma forma, el umbral máximo crediticio puede variar de forma negativa si se tienen en cuenta problemas recurrentes de pagos, conductas sospechosas en cuanto al uso del servicio, informes negativos de posición crediticia, patrones de conductas de llamadas a destinos inusuales, otros.

Finalmente, el límite debe ser evaluado de forma predictiva. Sabiendo cual es el consumo de servicio por hora de cada cliente, es posible predecir la tendencia que tendrá en el periodo total de facturación. Si la tendencia indica que el umbral de dinero a pagar se cumplirá mucho antes de alcanzar el período completo, deben existir alertas a la mesa de operaciones para que hagan seguimiento de la conducta anómala.

Asimismo, deben incorporarse las siguientes técnicas:

- Resguardo de los registros de comunicaciones (CDR). En su nivel más básico toda llamada genera un registro con información que puede variar según la tecnología subyacente que utiliza el operador. Estos registros deben poseer la máxima información posible y deben ser guardados por el mayor tiempo posible. Los registros de las llamadas son un activo valioso para las empresas y es recomendable la generación de resguardos redundantes.

- Generación de un *data warehouse*[34] que contenga toda la información de los clientes. No solamente los CDR son información valiosa para la prevención del fraude sino que todo dato estructurado proveniente de todos los sistemas de información de la empresa. Entre los posibles sistemas de interés se encuentran:

    - Sistemas de atención al cliente o de incidencias.
    - Comunicaciones de clientes mediante redes sociales de la empresa.

[34]**Datawarehouse**: Colección de datos integrada, no volátil y variable en el tiempo, que ayuda a la toma de decisiones en la entidad en la que se utiliza.

- Registros de comunicaciones de clientes mediante llamadas telefónicas o correos electrónicos.
- CRM (*Customer Relationship Manager*).
- Bitácoras de equipamiento de comunicaciones y telefonía.
- Sistemas de facturación, software de gestión o ERP[35].
- Cuentas de crédito o balances de clientes
- Otros.

Todos estos datos deben ser reunidos y relacionados en un almacenamiento centralizado de la empresa que sea la base sobre la cual construir los modelos predictivos de conductas y de detección de patrones.

- Implementación de modelos probabilísticos. Tal como se abordó en el Marco Teórico, existen diversas técnicas que permiten diferenciar el tráfico normal de un cliente verdadero o hacia un proveedor honesto, del tráfico anómalo producto de un fraude. Los atributos básicos de una llamada telefónica: duración, numero de destino, número de origen, tiempo de establecimiento, categoría de la llamada, país de origen, país de destino, y otros, pueden –y deben- ser recombinados y enriquecidos con otras fuentes de datos.

  Un ejemplo sencillo puede brindarse sobre el escenario de fraude *Blueboxing* o secuestro de llamadas por parte de un proveedor. Como se recordará, este escenario tenia la particularidad de ser generado por un proveedor (o sea otro operador telefónico) al cual se le entrega una serie de llamadas que tienen en común un

[35]**ERP** (Enterprise Resource Planning) sistemas que integran y manejan los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.

determinado destino. El proveedor fraudulento toma un cierto porcentaje de las llamadas y en vez de entregarlas a los destinatarios finales verdaderos las deriva a una locución falsa. Estas llamadas son cobradas, pero no poseen costo para el operador que decide producir el fraude.

Este escenario es muchas veces difícil de detectar, en especial porque es disfrazado mediante alguna decisión aleatoria sobre las llamadas en las que se produce el engaño. Pero puede no ser tan complejo encontrarlo si para la detección de este patrón se integra la herramienta de reclamos de clientes. Entendiéndose que las llamadas secuestradas resultarán una molestia para el usuario originante, este muy posiblemente reclame a su operador. En este caso, la herramienta de reclamos debe contribuir con sus datos estructurados al sistema de antifraude para poder construir la detección de ese modelo de comportamiento anómalo y de esa forma lograr una descripción amplia del comportamiento del cliente o del proveedor. De igual forma puede prevenirse el escenario de Falso establecimiento de llamadas (FAS), también originado por proveedores fraudulentos y también de difícil detección por mecanismos manuales.

En síntesis, los datos recolectados desde todos los sistemas de la organización deben ser utilizados en conjunción para entender cuales son los patrones de conducta de un defraudador y en base a ellos definir sistemas de detección, tanto basados en métodos probabilísticos predefinidos o basados en sistemas de autoaprendizaje.

- Análisis financiero: El análisis financiero de la unidad de negocios de telefonía debe hacerse agrupando o cortando el universo de datos por distintas características. Se

recomiendan algunas básicas, pero es posible también ampliarse a otras que reflejen la realidad de la compañía, como líneas de producto o días específicos de importancia del año (Navidad, Día de la Madre, otros.). Por lo tanto, es indispensable generar un tablero de comando o reportes periódicos que muestren la rentabilidad a los siguientes niveles.

1. Unidad completa de negocio. Considerando la facturación total de los clientes versus los costos directos de la unidad de negocio (costos de llamadas, personal directo involucrado, infraestructura directa asociada, costos fijos directos de enlaces de datos, costos fijos directos de interconexiones de telefonía, otros).

2. Producto comercial. Realizando la agrupación de la facturación por cada producto. La asignación de costos por productos puede ser compleja y necesitar un exhaustivo análisis, pero permite entender que productos son rentables y cuales no lo son.

3. Destino. Este es uno de los reportes mas importantes debido a que numerosas perdidas se dan por motivos de precios mal asignados a ciertos destinos del mundo. El escenario de fraude derivado de un arbitraje de precios puede ser detectado mediante reportes que incorporen la facturación directa de tráfico telefónico agrupado por destino versus los costos directos asociados.

4. Cliente. Es el nivel mas especifico de análisis y muestra la rentabilidad de cada cliente. Para empresas grandes verificar la rentabilidad de cada cliente de

forma individual es imposible, pero si es posible ver la rentabilidad de aquellos que posean los mayores volúmenes de facturación o los mayores volúmenes de tráfico de llamadas telefónicas. También es posible estudiar *outlayers*, o sea aquellos que tuvieron los peores rendimientos o aquellos que tuvieron rendimientos excepcionalmente grandes.

Los reportes anteriores pueden ser mejorados realizando comparaciones entre períodos o segmentando por tipos de clientes. El racional detrás de la recomendación se centra en poseer información financiera en tiempo real que ayude a encontrar los desvíos producidos por el fraude.

- Realimentación a sistemas comerciales y operativos. La integración de todos los sistemas de información y el desarrollo de una herramienta de software automatizada para la detección del fraude, debe permitir la retroalimentación con los sistemas de originales. Algunas de las posibles retroalimentaciones posibles se exploran a continuación, pero dependerán los sistemas que cada empresa posea y la posibilidad de adaptación de estos:

    - Retroalimentación a sistemas comerciales o de relacionamiento con el cliente: Aquellas cuentas comerciales que han sido relacionadas con comportamientos comprobables de una actividad defraudatoria deben poseer un marca en el los sistemas de atención al cliente, CRM y/o cualquier otro sistema que involucre el contacto con el cliente.

- Retroalimentación a sistemas técnicos: La implementación de esta retroalimentación dependerá fuertemente de la tecnología subyacente mediante la cual el operador entregue su servicio. En infraestructuras basadas en tecnología VoIP o de conmutación de paquetes debe existir una retroalimentación a los *softswitches*[36] donde se les informe datos que impidan la generación de nuevas comunicaciones desde el origen el origen del fraude (dirección IP, usuarios/contraseñas, proveedor utilizado, otros) o hacia el destino del fraude (destinos de llamadas usados frecuentemente para fraudes, números telefónicos relacionados con fraudes, otros.). En infraestructuras basadas en establecimiento de circuitos similares estrategias deben implementarse retroalimentando hacia las centrales intermedias de conmutación, bases de dato de itinerancia (*roaming*), bases de datos de portabilidad, otros.

- Retroalimentación a sistemas de validación crediticia: Aquellas cuentas comerciales que han sido relacionadas con comportamientos comprobables de una actividad defraudadora deben poseer un impacto en el sistema de *scoring* que permita decidir el límite de crédito que se le asigna a cada cliente. El calificador negativo que impactará en el sistema de *scoring* debe poseer una relación directa con las razones, magnitud y consecuencias del fraude. Dicho de otra forma, un fraude de una magnitud menor y por razones ajenas al cliente, debería impactar en menor manera, que un fraude más mayor magnitud ocasionado por negligencia técnica del cliente.

[36]**Softswitch:** Dispositivo central en una red de comunicaciones basada en tecnología VoIP que conecta llamadas telefónicas entre sí.

- Registros de actividades. Con la finalidad de poder realizar auditorías internas es vital que toda acción realizada por los empleados en los sistemas de la empresa posea un registro correspondiente. Algunas de las acciones que deben ser resguardadas con información de día y hora, persona y acción realizada son:

    - Cambios de precios de venta en listas de precios a clientes.
    - Cambios de precios de compra a proveedores.
    - Cambios en las definiciones de productos.
    - Cambios técnicos/operativos en las plataformas de servicio.
    - Cargas de créditos o modificaciones en el balance de una cuenta.
    - Otros.

    Estos registros deben también alimentar el *datawarehouse* de la compañía y ser considerados dentro del los datos que analizan las herramientas de gestión del fraude.

*Buenas prácticas en materia de colaboración*

Aún contando con los mejores procesos y las mejores herramientas informáticas, existe mucho para ganar en la colaboración. Es creciente la aparición de paradigmas técnicos o de negocios que se basan en la cooperación por un lado, y en la segmentación de un problema grande en muchos pequeños para ser solucionado colaborativamente (desde Wikipedia hasta Kickstarter) por otro. La premisa detrás del éxito de estos proyectos se basa la sinergia que se logra cuando muchos individuos contribuyen de forma organizadas tras una misma meta. Durante la investigación se encontró que este pensamiento tiene baja ocurrencia en el ámbito de las telecomunicaciones, donde poco o nada se transmite entre los actores.

En La Argentina, existen diversos ámbitos ya existentes que pueden ampliarse generando comisiones, subcomisiones o grupos de trabajo en las cuales estos temas pueden ser tratados. Entre ellos se pudieron encontrar:

1. CATIP (Cámara Argentina de Telefonía IP). Nuclea a prestadores de servicios de telefonía recientes que han desarrollado su servicio bajo la tecnología VoIP.
2. CABASE (Cámara Argentina de Internet). Nuclea a diversos actores que brindan servicio relacionado con Internet, desde desarrollo de software hasta proveedores de acceso a Internet.
3. CICOMRA (Cámara de Informática y Comunicaciones de La República Argentina). Cama. Organiza una de las exposiciones mas antigua del medio: EXPO COMM.

- Implementación de listas negras compartidas: Distintos datos sobre fraudes o intentos de fraudes en progreso pueden ser compartidos entre las organizaciones que facilitarían la protección general de todos los miembros. La información compartida puede generar listas negras comerciales (CUIT o DNI de infractores conocidos) o técnicas (direcciones IP, números telefónicos, proveedores) que pueden ser consultadas en tiempo real en los procesos de las organizaciones. En el caso aparecer un potencial cliente o una potencial comunicación dentro de estas listas negras, el nivel de sospecha de la misma dentro del proceso de aceptación puede ser modificado de acorde con el mismo dato. Las listas negras pueden ser generadas y consultadas de forma automatizada y sistémica, donde todos los miembros participantes comparten sus datos en ellas desde sus sistemas de información y a la vez consultan sobre los datos aportados por los restantes miembros.

Sistemas de RTD pueden tomar ventaja de estos datos para cancelar, en la mitad de un proceso de alta, a un nuevo cliente riesgoso o hasta el detener el establecimiento de una llamada que se ha confirmado es procedente de un defraudador.

- Reuniones periódicas de discusión. Se recomienda incorporar grupos de investigación sobre la temática en aquellas entidades locales ya existentes que aglutinan a los referentes de la industria de las comunicaciones.
- Generación de buenas prácticas compartidas. Aquellas agrupaciones donde se discuta la problemática del fraude deben publicar recurrentemente sus descubrimientos en forma de buenas prácticas. El conocimiento ganado no debe ser ocultado puertas adentro, dado que el problema de uno es el problema de todos. Si las correctas prácticas son implementadas por todos los operadores, el fraude dejará de ser una conducta atractiva para aquellos que viven de ella.

### V.3 Aportes para futuras investigaciones

A partir de lo aprendido en la presente tesis de investigación se dejan recomendaciones de potenciales temas que pueden resultar de interés para futuros investigadores y/o proyectos comerciales:

- Determinar otros puntos de dolor en los procesos mencionados en las buenas prácticas que puedan disminuir su exposición al fraude. Construir matrices de riesgo para cada proceso puntual.

- Proponer sistemas de auditoría interna que disminuyan los fraudes internos.

- Investigar, compilar y comparar las herramientas informáticas *World class* que brinden gestión del fraude.
- Realizar estudios de campo cuantitativos que permitan determinar que destinos geográficos son los mas propensos a ser utilizados en escenarios de fraude.
- Extrapolar las conclusiones aprendidas sobre modelos probabilísticos a otros sectores.
- Completar la investigación con el marco jurídico local y/o regional. En el plano local se están generando muchas propuestas de cambios a la legislación de comunicaciones que podrían tener alto impacto en el sector.
- Generar una estándar de intercambio único para precios de destinos de telefonía. Durante el marco investigativo se pudo ver que el proceso de intercambio de tarifas entre operadores no posee nada cercano a un estándar. Generalmente los cambios de tarifas se informan mediante correos electrónicos y en formato libre de planillas de cálculo Microsoft Excel.

# BIBLIOGRAFÍA

## Libros:


- Barnett, V. y Lewis, T. (1994). *Outliers in statistical data*. (3ra ed.) EEUU: John Wiley and Sons.
- Ben-Gal, I. (2010). *Data mining and knowledge discovery handbook*. (2da ed.). Capítulo 7: Outlier detection. EEUU: Springer.
- Dodd, A. Z. (2012). *The essential guide to telecommunications*. (5ta. ed.). EEUU: Prentice Hall.
- McAfee, A. y Brynjolfsson, E. (2014). *The second machine age*. EEUU: W. W. Norton & Company.
- Wheen, A. (2011). *How modern telecommunications evolved from telegraph to the Internet*. EEUU: Springer Praxis.


## Tesis e investigaciones:


- Bolton, R. y Hand, D. (2002). *Statistical fraud detection: a review*. Tesis doctoral. Institute of Mathematical Statistics, Ohio, EEUU.
- Hollmén, J. (2000). *User profiling and classification for fraud detection in mobile communications networks*. Tesis posgrado. University of Technology, Helsinki, Finlandia.
- Isomäki, Markus. (1999).*Security in the traditional telecommunications networks and in the Internet.* Tesis posgrado. Helsinki University of Technology, Helsinki, Finlandia.

- Tawashi, H. A. (2010). *Detecting fraud in cellular telephone Networks.*Tesis de grado. University of Gaza (Faculty of Commerce), Gaza, Israel.
- Yao, Y. (2014). *Detection of health insurance fraud with discrete choice*. Tesis de grado. Peking University, School of Economics, Pekín, República Popular China.Recuperado de http://econ.pku.edu.cn/upload/file/20140619/20140619144287188718.pdf el día 23/05/2016.


Revistas:


- Gupta, D. Pahwa, P y Arora, R. (2014). An analysis of telecommunication fraud using outlier detection model based on similar coefficient sum. *International Journal of Soft Computing and Engineering*. 4 (marzo de 2014)
- Rampton, J. (2015). How online fraud is a growing trend. *Revista Forbes*. Abril de 2015.
- Yang, W. (2006). A process-mining framework for the detection of healthcare fraud and abuse. *Expert Systems with Applications* 31 (2006) 56-68. Editorial Elsevier.
- Zhang, C. Sun, J.Zhu, X. y Fang, Y.(08/2010). Privacy and security for online social networks: challenges and opportunities. *Revista IEEE Network* julio/agosto de 2010. Recuperado de http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/seg2011/social-2.pdf l día 20/05/2016


Páginas web:


- Bae Brandtzæg, P. (22/05/2013). *Big Data, for better or worse: 90% of world's data generated over last two years*. ScienceDaily. Recuperado de http://www.sciencedaily.com/releases/2013/05/130522085217.htm el día 19/05/2016.

- Birkinshaw, J. (06/2014). *Beyond the Information Age*. Wired. Recuperado de http://www.wired.com/insights/2014/06/beyond-information-age/ el día 20/06/2016.
- Burton, J. (2005). *The communications/information productivity revolution*. Recuperado de https://www.scribd.com/document/35141318/Telecom-Revolution-White-Paper el día 06/05/2016.
- Castells, M. (08/09/2014). *The impact of the Internet on society: a global perspective.* MIT Technology Review. Recuperado de https://www.technologyreview.com/s/530566/the-impact-of-the-internet-on-society-a-global-perspective/ el día 21/05/2014.
- CIMA. (2008). *Fraud risk management. a guide to good practice*. Recuperado dehttp://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf el día 19/06/2016.
- CTIA. (2014). *Annual wireless industry survey*. Cellular Telephone Industries Association. Recuperado de http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey el día 01/05/2016.
- Draz, D. (28/03/2011). *Fraud prevention: improving internal controls*. CSO. Recuperado de http://www.csoonline.com/article/2127917/fraud-prevention/fraud-prevention--improving-internal-controls.html el día 26/06/2016.
- ENACOM. (2013). *Estadísticas e indicadores de Telecomunicaciones Argentina. Serie 2008 - 2012*. Ente Nacional de Comunicaciones. Recuperado de http://www.enacom.gob.ar/multimedia/noticias/archivos/201409/archivo_20140901035233_1056.pdf el día 07/05/2016.
- Ferro, G. (05/01/2016). *The future of collaboration is asynchronous*. Recuperado de http://packetpushers.net/future-collaboration-asynchronous/ el día 16/05/2016.

- Gunatilaka, D. *A survey of privacy and security issues in social networks*. Recuperado de http://www.cs.wustl.edu/~jain/cse571-11/ftp/social/index.html el día 20/05/2016.
- Hollingsworth, T. (12/01/2016). *My thoughts on the death of IP telephony*. Recuperado dehttps://networkingnerd.net/2016/01/12/my-thoughts-on-the-death-of-ip-telephony/ el día 05/05/2016.
- Howells, I., Scharf-Katz, V. y Stapleton, P. (2014). *Telecom fraud 101: fraud types, fraud methods, & fraud technology*. Argyle Data. Recuperado de http://www.argyledata.com/files/Telecom-Fraud-101-eBook.pdf el día 12/06/2016.
- Marr, B. (30/09/2015). *Big data: 20 mind-boggling facts everyone must read*. Forbes.Recuperado de http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#6aec894a6c1d el día 15/05/2016.
- Nasdaq. (16/09/2015). *Credit card fraud and ID theft statistics*. Nasdaq. Recuperado de http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388 el día 29/05/2016.
- PwC. (2011). *Cybercrime: protecting against the growing threat global economic crime survey – PWC Global Economic*. Price Waterhouse Cooper. Recuperado de http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf el día 01/05/2016.
- Radicati Group, Inc. (2015). *Email statistics report, 2015-2019*. Recuperado de http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf el día 19/05/2016.
- Razin, E. (04/05/2016). *From the industrial age to the information age: where have all the factories gone?*. Forbes.Recuperado de http://www.forbes.com/sites/elyrazin/2016/05/04/from-the-industrial-age-to-the-information-age-where-have-all-the-factories-gone/#2fb165b35c51 el día 20/06/2016.

- Satell, G. (24/02/2016). *How IBM plans to innovate past Moore's Law*. Forbes. Recuperado de http://www.forbes.com/sites/gregsatell/2016/02/24/how-ibm-plans-to-innovate-past-moores-law/#59f51d6f71fd el día 20/06/2016.
- Singhal, N. (28/08/2010). *Phone numbers are dead; they just don't know it yet*. Recuperado de https://techcrunch.com/2010/08/28/phone-numbers-dead/ el día 25/04/2016.
- Spencer, M. (08/2009).*America loses its landlines"*. The Economist. Agosto de 2009. Recuperado de http://www.economist.com/node/14214847l el día 28/05/2016.
- Statista. (2016). *Value of payment card fraud losses in the United States from 2012 to 2018.*Recuperado de http://www.statista.com/statistics/419628/payment-card-fraud-losses-usa-by-type/ el día 25/05/2016.
- Sydell,L. (20/042015). *At 50 years old, the challenge to keep up with Moore's Law*. Recuperado de http://www.npr.org/sections/alltechconsidered/2015/04/20/400988928/at-50-years-old-the-challenge-to-keep-up-with-moore-s-law el día 20/06/2016.
- Telsis. (2015). *Protecting against the next generation of telephony fraud*. Telsis. Recuperado de http://www.telsis.com/whitepaper/1590-1379-01-Telephony-Fraud-White-Paper.pdf el día 03/06/2016.
- Visa. (2009). *Telecommunication industry global fraud prevention and best practices for Visa merchants*. Recuperado de http://www.visa.ca/merchant/resources/fraud-fighting/pdf/telecommunication-industry-global-Fraud-Prevention.pdfl el día 18/06/2016.
- White, R. (2016). *Should IP telephony die?*. Recuperado de http://ntwrk.guru/percentage-driven/ el día 05/05/2016.

- Yager II, K R. (11/2011). *The line is dead: the future of telephone, cable and wireless communications*. Recuperado dehttp://www.morrisanderson.com/images/uploads/documents/The_line_is_dead_Yager_Sept_2011.pdf el día 12/06/2016.


Otros:


- Davis, A. B. y Goyal, S. K. (1993). “Management of cellular fraud: Knowledge-based detection, classification and prevention”. Reporte presentado en el 13º International Conference on Artificial Intelligence, Expert Systems and Natural Language. Avignon, Francia.
- Fawcett, Tom y Provost, Foster. (1998). “Automated Design of User Profiling for Fraud Detection”. Reporte WS-98-07 de la American Association for Artificial Intelligence.
- I3 Forum. (2014). "Fraud classification and recommendations on dispute handling within the wholesale telecom industry". Reporte presentado en el I3 Forum de 2014.
- Joyner, Ellen. (2011). “Enterprise-wide Fraud Management”. Paper 029-2011. SAS Institute Inc. North Carolina, EEUU. Presentado en el SAS Group Forum 2011. Las Vegas, Nevada, EEUU.
- Karak, Souvik, Jain,Sanket y Muralidaran, Vijay. (2013). “Evolving early combat systems in Next Generation telecom fraud: catch them young”. Publicación para IBM. Recuperado de http://www.academia.edu/ el día 20/06/2016.

# ANEXOS

## Anexo I: Encuesta a representantes de la industria

**La presente encuesta debe realizarse de corrido y es de carácter totalmente anónimo. La información relevada será utilizada como información para una Tesis de posgrado de la Universidad de Palermo.**

**En las preguntas que posean respuesta por SI o por NO, dibuje un círculo sobre su respuesta. En las preguntas que posean varios valores de respuesta, dibuje un círculo sobre su opción elegida.**

---

1. ¿Su empresa posee una unidad que tenga como objetivo analizar y combatir el fraude telefónico? SI/NO

2. ¿En caso afirmativo, considera, en su opinión personal, que cumplen sus funciones satisfactoriamente? SI/NO

3. ¿Cuál de los siguientes rangos supone que son las pérdidas anuales, expresadas en dólares americanos, producidas a su empresa por el fraude?:

a. 0 a 100.000

b. 100.000 a 500.000

c. 500.000 a 1.000.000

d. mas de 1.000.000

4. ¿Cuál de los siguientes rangos supone que se encuentra, expresadas en dólares americanos, la facturación de su empresa anual para la unidad de telefonía?:

a. 0 a 500.000

b. 500.000 a 1.000.000

c. 1.000.000 a 5.000.000

d. mas de 5.000.000

5. ¿Su empresa participa en alguna organización o foro donde se establezcan políticas para evitar fraude? SI/NO

6. ¿Su empresa implementa protecciones o políticas que evitan el hacking (secuestro) del servicio telefónico a sus clientes? SI/NO

7. ¿Su empresa implementa limitaciones en los destinos a los que sus clientes pueden realizar llamadas? SI/NO

8. ¿Considera que su empresa posee procesos eficientes para controlar el fraude de suscripción (aquel donde un nuevo usuario falsea su identidad con la intención premeditada de no pagar luego el servicio)? SI/NO

9. ¿Su empresa implementa técnicas de Minería de Datos (Data Mining) y técnicas avanzadas de explotación de información para el análisis y detección de fraude telefónico? SI/NO

10. Si posee sugerencias sobre posibles políticas para la prevención o detección de fraude telefónico puede describirlas a continuación

## Cuadro 10 - Matriz de respuestas de la encuesta

| Preguntas | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *¿Su empresa posee una unidad que tenga como objetivo analizar y combatir el fraude telefónico?* | NO | SI | SI | NO | NO | NO | NO | NO | SI | NO | NO | NO | NO | SI | NO | NO | NO | NO | N/C | SI | SI | NO | NO | SI | NO | NO | SI | NO | N/C |
| *¿En caso afirmativo, considera, en su opinión personal, que cumplen sus funciones satisfactoriamente?* | N/A | SI | SI | N/A | N/A | N/A | N/A | N/A | NO | N/A | N/A | N/A | N/A | SI | N/A | N/A | N/A | N/A | N/A | SI | SI | N/A | N/A | NO | N/A | N/A | SI | N/A | N/A |
| *¿Cuál de los siguientes rangos supone que son las perdidas anuales, expresadas en dólares americanos, producidas a su empresa por el fraude?* | N/C | d | c | a | a | b | a | N/C | c | b | a | N/C | N/C | c | a | a | N/C | b | N/C | d | N/C | a | a | b | N/C | a | c | a | a |
| *¿Cuál de los siguientes rangos supone que se encuentra, expresadas en dólares americanos, la facturacion de su empresa anual para la unidad de telefonia?* | N/C | d | N/C | N/C | N/C | N/C | a | N/C | N/C | c | a | N/C | N/C | d | a | a | N/C | b | N/C | d | N/C | a | N/C | N/C | N/C | b | N/C | N/C | N/C |
| *¿Su empresa participa en alguna organización o foro donde se establezcan políticas para evitar fraude?* | N/C | SI | NO | NO | NO | NO | NO | N/C | SI | NO | NO | NO | N/C | NO | NO | NO | N/C | NO | NO | NO | SI | NO | SI | NO | NO | NO | NO | NO | NO |
| *¿Su empresa implementa protecciones o políticas que evitan el hacking (secuestro) del servicio telefónico a sus clientes?* | NO | NO | NO | NO | NO | SI | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | NO | SI | NO | NO | SI | NO | NO | SI |
| *¿Su empresa implementa limitaciones en los destinos a los que sus clientes pueden realizar llamadas?* | SI | SI | SI | N/C | SI | SI | NO | SI | SI | SI | SI | N/C | NO | SI | SI | SI | N/C | NO | SI | SI | NO | SI | SI | SI | NO | SI | SI | NO | SI |
| *¿Considera que su empresa posee procesos eficientes para controlar el fraude de suscripción (aquel donde un nuevo usuario falsea su identidad con la intencion premeditada de no pagar luego el servicio)?* | SI | SI | SI | N/C | SI | N/C | NO | SI | SI | NO | NO | NO | SI | SI | NO | NO | SI | NO | SI | SI | SI | SI | SI | SI | SI | SI | SI | NO | NO |
| *¿Su empresa implementa técnicas de Minería de Datos (Data Mining) o técnicas avanzadas de explotación de información para el análisis y detección de fraude telefónico?* | NO | SI | NO | NO | N/C | NO | N/C | NO | SI | NO | NO | NO | NO | NO | N/C | NO | N/C | NO | NO | NO | SI | NO | NO | NO | N/C | NO | NO | N/C | N/C |
| *Si posee sugerencias sobre posibles políticas para la prevención o detección de fraude telefónico puede describirlas a continuación* | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C | N/C |

Fuente: elaboración propia (2016)

## ANEXO II: Guía de entrevistas a informantes-clave

El detalle de los entrevistados, sus profesiones y conocimientos sobre la temática de la tesis se muestran en el siguiente cuadro:

**Cuadro 11 -Resumen de entrevistas a informantes-clave**

| Nombre | Posición | Empresa | Ciudad | Fecha Entrevista | Duración | Modo de realización |
|---|---|---|---|---|---|---|
| **Néstor Montés** | Gerente de IT | Telefónica ABC | Ciudad de Buenos Aires | 03/08/2016 | 2 horas | Presencial |
| **Mariano Cento** | VP Ventas | Biactiva | Ciudad de Buenos Aires | 28/07/2016 | 45 min | Presencial |
| **German Suleta** | Gerente Comercial | Alvis SA | Ciudad de Buenos Aires | 11/08/2016 | 1 hora | Presencial |

Fuente: Elaboración Propia (2016)

Preguntas semi-estructuradas utilizadas durante las entrevistas:

1. ¿En su actividad como ejecutivo de cuentas de una empresa de telefonía que casos de fraude telefónico recuerda?
2. ¿Sabe cómo se resolvieron finalmente estos casos? ¿Se encontraron a los perpetradores? ¿Las pérdidas ocasionadas a la empresa fueron revertidas? ¿tiene información de los montos involucrados?

3. ¿Tuvieron que discontinuar ciertos servicios o modificarlos a raíz de la potencialidad a fraude que tenían?

4. ¿Si pudiera decidir sobre las políticas antifraude de su empresa qué haría?

5. ¿Posee conocimiento de grupos, cámaras o foros de interés locales o regionales?

6. ¿Considera que poseen las herramientas para afrontar fraude? ¿Tercerizarían ese servicio?

## ANEXO III: Lista de costos mayorista de telefonía

La siguiente lista de costos fue la utilizada por el operador de telefonía Crossfone Argentina SA durante 2015. Ella refleja cual es el valor que debe pagar por cada segundo de conversación telefónica a distintos países o redes del mundo.

### Cuadro 12 -Tarifas mayoristas de telefonía

| Destino | Tarifa [USD] |
|---|---|
| ALEMANIA | 0.00034 |
| ALEMANIA E-PLUS MOVIL | 0.00386 |
| ALEMANIA E-PLUS MOVIL | 0.00386 |
| ALEMANIA E-PLUS MOVIL | 0.00386 |
| ALEMANIA SHARED COST | 0.00024 |
| ALEMANIA SHARED COST | 0.00024 |
| ALEMANIA SHARED COST | 0.00024 |
| ALEMANIA SHARED COST | 0.000258333 |
| ALEMANIA SHARED COST | 0.00026 |
| ALEMANIA SHARED COST | 0.00026 |
| ALEMANIA T-MOBILE MOVIL | 0.00175 |
| ALEMANIA T-MOBILE MOVIL | 0.00175 |
| ALGERIA | 0.000969132 |
| AUSTRALIA | 0.000134505 |
| AUSTRALIA METRO | 0.000125341 |
| AUSTRALIA METRO | 0.00013 |
| AUSTRALIA MOBILE | 0.00036 |
| AUSTRALIA OPTUS MOBILE | 0.00036 |
| AUSTRALIA OPTUS MOBILE | 0.000363611 |
| AUSTRALIA TELSTRA MOBILE | 0.000363948 |
| AUSTRIA | 0.001721192 |
| AUSTRIA T-MOBILE MOBILE | 0.00351888 |
| BAHAMAS | 0.000642553 |
| BARBADOS | 0.00181 |
| BELGICA - PROXIMUS MOVIL | 0.00048 |
| BELGIUM BELGACOM-M MOBILE | 0.00023523 |
| BELGIUM PROXIMUS | 0.00124 |
| BELGIUM PROXIMUS | 0.001243083 |
| BOL EQUAL ACCESS | 0.001367758 |
| BOL EQUAL ACCESS | 0.00137 |
| BOLIVIA | 0.00139 |
| BOLIVIA | 0.001393635 |
| BOLIVIA COCHABAMBA | 0.001399784 |
| BOLIVIA COCHABAMBA | 0.0014 |
| BOLIVIA ENTEL MOB MOBILE | 0.002278641 |
| BOLIVIA ENTEL MOB MOBILE | 0.00228 |
| BOLIVIA ENTEL MOVIL | 0.00294 |
| BOLIVIA LA PAZ | 0.00133 |
| BOLIVIA LA PAZ | 0.001334111 |
| BOLIVIA NUEVAT MOBILE | 0.00226989 |
| BOLIVIA NUEVAT MOBILE | 0.00227 |
| BOLIVIA NUEVATEL MOVIL | 0.0029375 |
| BOLIVIA NUEVATEL MOVIL | 0.00294 |
| BOLIVIA NUEVATEL MOVIL | 0.00294 |
| BOLIVIA NUEVATEL MOVIL | 0.00294 |
| BOLIVIA POTOSI | 0.00179 |
| BOLIVIA POTOSI | 0.00179 |
| BOLIVIA POTOSI | 0.00179 |
| BOLIVIA RURAL | 0.002628847 |
| BOLIVIA RURAL | 0.00263 |
| BOLIVIA RURAL | 0.00348 |
| BOLIVIA RURAL | 0.00348 |
| BOLIVIA SANTA CRUZ | 0.00089 |
| BOLIVIA SANTA CRUZ | 0.000893554 |
| BOLIVIA SANTA CRUZ | 0.00179 |
| BOLIVIA SANTA CRUZ | 0.00179 |
| BOLIVIA SUCRE | 0.00179 |
| BOLIVIA TARIJA | 0.00179 |
| BOLIVIA TARIJA | 0.00179 |
| BOLIVIA TARIJA | 0.001791667 |
| BOLIVIA TELECE MOBILE | 0.002266188 |
| BOLIVIA TELECE MOBILE | 0.00227 |
| BOLIVIA TELECEL MOVIL | 0.00294 |

| Destino | Tarifa [USD] |
|---|---|
| BOLIVIA TELECEL MOVIL | 0.00294 |
| BOLIVIA TELECEL MOVIL | 0.00294 |
| BOLIVIA TELECEL MOVIL | 0.00294 |
| BOLIVIA TELECEL MOVIL | 0.00294 |
| BRA GOVDOR VALARES | 0.000069148 |
| BRA GOVDOR VALARES | 0.00007 |
| BRA PORTO ALEGRE | 0.00007 |
| BRA PORTO ALEGRE | 0.000070358 |
| BRASIL | 0.00039 |
| BRASIL - FLORIANOPOLIS | 0.0002 |
| BRASIL - MOVIL | 0.00123 |
| BRASIL - OLO SAO PAULO CAPITAL | 0.000197917 |
| BRASIL - OLO SAO PAULO CAPITAL | 0.0002 |
| BRASIL - OLO SAO PAULO RESTO | 0.00018 |
| BRASIL - OLO SAO PAULO RESTO | 0.00018 |
| BRASIL - RIO DE JANEIRO | 0.000197917 |
| BRASIL - RIO DE JANEIRO | 0.0002 |
| BRASIL - SAO PAULO | 0.00017 |
| BRASIL - SAO PAULO | 0.00017 |
| BRASIL - SAO PAULO | 0.00017 |
| BRASIL - SAO PAULO | 0.00017 |
| BRASIL - SAO PAULO | 0.00017 |
| BRASIL - TIM MOVIL | 0.00123 |
| BRASIL - TIM MOVIL | 0.00123 |
| BRASIL - VIVO FIXED | 0.00015 |
| BRASIL - VIVO FIXED | 0.00015 |
| BRASIL - VIVO MOVIL | 0.0011875 |
| BRASIL - VIVO MOVIL | 0.00119 |
| BRASIL - VIVO MOVIL | 0.00119 |
| BRASIL - VIVO MOVIL | 0.00119 |
| BRASIL - VIVO MOVIL | 0.00119 |
| BRAZIL | 0.00007 |
| BRAZIL | 0.000071716 |
| BRAZIL BEHLO HORIZ | 0.000056274 |
| BRAZIL BEHLO HORIZ | 0.00006 |
| BRAZIL BRASILIA | 0.00006 |
| BRAZIL CAMPINAS | 0.00009 |
| BRAZIL CAMPINAS | 0.000090397 |
| BRAZIL CURITIBIA | 0.00007 |
| BRAZIL CURITIBIA | 0.000070368 |
| BRAZIL FLORIANOPOL | 0.000068943 |
| BRAZIL FLORIANOPOL | 0.00007 |
| BRAZIL FORTALEZA | 0.000067906 |
| BRAZIL FORTALEZA | 0.00007 |
| BRAZIL GOIANIA | 0.000065902 |
| BRAZIL LONDRINA | 0.00008 |
| BRAZIL MOBILE | 0.000746603 |
| BRAZIL MOBILE | 0.00075 |
| BRAZIL NATAL | 0.00007 |
| BRAZIL NATAL | 0.000072342 |
| BRAZIL RECIFE | 0.000068172 |
| BRAZIL RECIFE | 0.00007 |
| BRAZIL RIO DE JANE | 0.000058325 |
| BRAZIL RIO DE JANE | 0.00006 |
| BRAZIL SALVADOR | 0.000065902 |
| BRAZIL SALVADOR | 0.00007 |
| BRAZIL SAO PAULO | 0.00006 |
| BRAZIL SAO PAULO | 0.000060437 |
| BRAZIL VITORIA | 0.00007 |
| BRAZIL VITORIA | 0.000072535 |
| CANADA | 0.000047096 |
| CANADA | 0.00005 |
| CANADA | 0.00013 |

| | |
|---|---|
| CANADA | 0.00013 |
| CHILE | 0.00018 |
| CHILE | 0.000180006 |
| CHILE | 0.00041 |
| CHILE | 0.00041 |
| CHILE - ENTEL PCS MOVIL | 0.0011 |
| CHILE - ENTEL PCS MOVIL | 0.0011 |
| CHILE - ENTEL PCS MOVIL | 0.0011 |
| CHILE - MOVISTAR MOVIL | 0.00083 |
| CHILE - MOVISTAR MOVIL | 0.00083 |
| CHILE - PUNTA ARENAS | 0.00092 |
| CHILE - SANTIAGO DE CHILE | 0.000375 |
| CHILE - SANTIAGO DE CHILE | 0.000375 |
| CHILE - SANTIAGO DE CHILE | 0.000375 |
| CHILE - SANTIAGO DE CHILE | 0.00038 |
| CHILE - SANTIAGO DE CHILE | 0.00038 |
| CHILE - SANTIAGO DE CHILE | 0.00038 |
| CHILE - SANTIAGO DE CHILE | 0.00038 |
| CHILE - SANTIAGO DE CHILE | 0.00038 |
| CHILE - TELSUR CNT | 0.00042 |
| CHILE - TELSUR CNT | 0.00042 |
| CHILE CLARO MOBILE | 0.00062 |
| CHILE CLARO MOBILE | 0.000623702 |
| CHILE OTHER MOBILE | 0.00062 |
| CHILE OTHER MOBILE | 0.000622861 |
| CHILE SANTIAGO | 0.00009649 |
| CHILE SANTIAGO | 0.0001 |
| CHINA | 0.000115991 |
| CHINA MOBILE | 0.000112621 |
| CHINA UNICOM MOBILE | 0.000117674 |
| CHINA UNICOM MOBILE | 0.00012 |
| COLOMBIA | 0.00059 |
| COLOMBIA | 0.000590165 |
| COLOMBIA | 0.00079 |
| COLOMBIA | 0.00079 |
| COLOMBIA AMERICA MOBILE | 0.0001 |
| COLOMBIA AMERICA MOBILE | 0.000102275 |
| COLOMBIA BOGOTA | 0.00079 |
| COLOMBIA BOGOTA | 0.00079 |
| COLOMBIA BOGOTA | 0.00079 |
| COLOMBIA BOGOTA | 0.000791667 |
| COLOMBIA COMCEL MOVIL | 0.000479167 |
| COLOMBIA COMCEL MOVIL | 0.00048 |
| COLOMBIA COMCEL MOVIL | 0.00048 |
| COLOMBIA COMCEL MOVIL | 0.00048 |
| COLOMBIA COMCEL MOVIL | 0.00048 |
| COLOMBIA COMCEL MOVIL | 0.00048 |
| COLOMBIA LOCAL EXTENDIDA | 0.00055 |
| COLOMBIA MEDELLIN | 0.00079 |
| COLOMBIA MOVISTAR MOBILE | 0.000385658 |
| COLOMBIA MOVISTAR MOBILE | 0.00039 |
| COLOMBIA MOVISTAR MOVIL | 0.00058 |
| COLOMBIA MOVISTAR MOVIL | 0.00058 |
| COLOMBIA MOVISTAR MOVIL | 0.00058 |
| COLOMBIA MOVISTAR MOVIL | 0.000583333 |
| COLOMBIA OTHER MOBILE | 0.00033 |
| COLOMBIA OTHER MOBILE | 0.000332515 |
| COLOMBIA TIGO MOBILE | 0.00024 |
| COLOMBIA TIGO MOBILE | 0.000241829 |
| COLOMBIA TIGO MOVIL | 0.00031 |
| COLOMBIA TIGO MOVIL | 0.00058 |
| COLOMBIA TIGO MOVIL | 0.00058 |
| COLOMBIA TIGO MOVIL | 0.00058 |
| COLOMBIA TIGO MOVIL | 0.00058 |
| COSTA RICA | 0.000245685 |
| COSTA RICA | 0.00025 |
| COSTA RICA | 0.00032 |
| COSTA RICA | 0.000322917 |
| COSTA RICA | 0.000322917 |
| COSTA RICA IP OPER | 0.00034 |
| COSTA RICA MOBILE | 0.000649451 |
| COSTA RICA MOBILE | 0.00065 |
| COSTA RICA RICA - ICE MOVIL | 0.0009 |
| COSTA RICA TELEFO MOBILE | 0.00096 |
| CUBA | 0.00967 |
| CUBA | 0.009673766 |
| CUBA | 0.013125 |
| CUBA - MOVIL | 0.013125 |
| CZECH CESKYMOBIL MOBILE | 0.001118774 |
| CZECH REP PRAGUE | 0.000315552 |
| DOMINICAN REPUBLIC | 0.00026 |
| DOMINICAN REPUBLIC | 0.000260105 |
| DOMINICAN REPUBLIC MOBILE | 0.0009 |
| DOMINICAN REPUBLIC MOBILE | 0.000903086 |
| DOMINICANA REP. | 0.00118 |
| DOMINICANA REP. | 0.00118 |
| DOMINICANA REP. - MOVIL | 0.00118 |
| DOMINICANA REP. - MOVIL | 0.00118 |

| | |
|---|---|
| DOMINICANA REP. - MOVIL | 0.00118 |
| DOMINICANA REP. - MOVIL | 0.00118 |
| DOMINICANA REP. - ORANGE MOVIL | 0.00118 |
| DOMINICANA REP. - ORANGE MOVIL | 0.00118 |
| DOMINICANA REP. - ORANGE MOVIL | 0.00118 |
| DOMINICANA REP. - ORANGE MOVIL | 0.00118 |
| ECUADOR | 0.001508456 |
| ECUADOR | 0.00151 |
| ECUADOR ANDINATEL | 0.0019 |
| ECUADOR BELLSOUTH MOBILE | 0.00252 |
| ECUADOR BELLSOUTH MOBILE | 0.002523709 |
| ECUADOR MOVISTAR MOVIL | 0.00346 |
| ECUADOR PACIFITEL | 0.0019 |
| ECUADOR PACIFITEL | 0.0019 |
| ECUADOR PACIFITEL | 0.0019 |
| ECUADOR PORTA MOBILE | 0.00273 |
| ECUADOR PORTA MOBILE | 0.002730464 |
| ECUADOR QUITO | 0.00148924 |
| ECUADOR QUITO | 0.00149 |
| EGIPTO | 0.00151 |
| EGYPT CAIRO | 0.001127201 |
| EGYPT CAIRO | 0.00113 |
| EGYPT MOBINIL MOBILE | 0.001414054 |
| EGYPT VODAFONE MOBILE | 0.00157 |
| EL SALVADOR CTE | 0.00129 |
| EL SALVADOR CTE | 0.001292967 |
| EL SALVADOR TELEFO MOBILE | 0.00225 |
| ESPAÑA | 0.00023 |
| ESPAÑA | 0.00023 |
| ESPAÑA | 0.00023 |
| ESPAÑA | 0.00023 |
| ESPAÑA ORANGE MOVIL | 0.00041 |
| ESPAÑA VODAFONE MOVIL | 0.00041 |
| ESPAÑA VODAFONE MOVIL | 0.00041 |
| ESTADOS UNIDOS | 0.000125 |
| ESTADOS UNIDOS | 0.000125 |
| ESTADOS UNIDOS | 0.000125 |
| ESTADOS UNIDOS | 0.000125 |
| ESTADOS UNIDOS | 0.000125 |
| ESTADOS UNIDOS | 0.00013 |
| ESTADOS UNIDOS | 0.00013 |
| ESTADOS UNIDOS | 0.00013 |
| ESTADOS UNIDOS | 0.00013 |
| ESTADOS UNIDOS | 0.00013 |
| ESTADOS UNIDOS - P800 | 0.00121 |
| ESTADOS UNIDOS - P800 | 0.00121 |
| ESTADOS UNIDOS - P800 | 0.00121 |
| ESTADOS UNIDOS - RURAL | 0.00423 |
| FR GUIANA ORANGE MOBILE | 0.000190098 |
| FRANCE | 0.00008 |
| FRANCE | 0.000082235 |
| FRANCE BOUYGUES MOBILE | 0.00091 |
| FRANCE BOUYGUES MOBILE | 0.000914144 |
| FRANCE CLEC | 0.00008 |
| FRANCE CLEC | 0.000082235 |
| FRANCE FREE MOBILE | 0.00095 |
| FRANCE FREE MOBILE | 0.000952393 |
| FRANCE LYCATEL MOBILE | 0.000891998 |
| FRANCE ORANGE MOBILE | 0.00091 |
| FRANCE ORANGE MOBILE | 0.000914144 |
| FRANCE SFR MEDIA MOBILE | 0.000919881 |
| FRANCE SFR MEDIA MOBILE | 0.00092 |
| FRANCIA - ORANGE MOVIL | 0.00142 |
| FRANCIA - PARIS | 0.00142 |
| GERMANY | 0.000057373 |
| GERMANY | 0.00006 |
| GERMANY E-PLUS MOBILE | 0.00032 |
| GERMANY E-PLUS MOBILE | 0.000323202 |
| GERMANY T-MOBILE MOBILE | 0.00029 |
| GERMANY T-MOBILE MOBILE | 0.000294515 |
| GERMANY TELEFONICA MOBILE | 0.00032 |
| GERMANY TELEFONICA MOBILE | 0.000323202 |
| GERMANY VODAFONE MOBILE | 0.00029 |
| GERMANY VODAFONE MOBILE | 0.000294515 |
| GREECE | 0.00030599 |
| GREECE COSMOTE MOBILE | 0.001128337 |
| GREECE COSMOTE MOBILE | 0.00113 |
| GREECE VODAFONE MOBILE | 0.001128337 |
| GREECE VODAFONE MOBILE | 0.00113 |
| GREECE WIND MOBILE | 0.001128337 |
| GREECE WIND MOBILE | 0.00113 |
| GUADELOUPE | 0.00008 |
| GUATEMALA - COMCEL FIJO | 0.00222 |
| GUATEMALA - COMCEL FIJO | 0.00222 |
| GUATEMALA COMCEL MOBILE | 0.001777763 |
| GUATEMALA COMCEL MOBILE | 0.00178 |
| GUATEMALA MOVISTAR MOBILE | 0.001847188 |
| GUATEMALA MOVISTAR MOBILE | 0.00185 |

| | |
|---|---|
| GUATEMALA SERCOM MOBILE | 0.001536657 |
| GUATEMALA SERCOM MOBILE | 0.00154 |
| GUATEMALA TELGUA | 0.00103 |
| GUATEMALA TELGUA | 0.001030802 |
| HOLANDA - VODAFONE MOVIL | 0.00075 |
| HONDURAS | 0.00175 |
| HONDURAS TIGO MOBILE | 0.002269186 |
| HONDURAS TIGO MOBILE | 0.00227 |
| HONG KONG MOBILE | 0.000250911 |
| INDIA - AIRTEL MOVIL | 0.000479167 |
| INDIA - AIRTEL MOVIL | 0.00048 |
| INDIA - AIRTEL MOVIL | 0.00048 |
| INDIA - AIRTEL MOVIL | 0.00048 |
| INDIA - AIRTEL MOVIL | 0.00048 |
| INDIA - AIRTEL MOVIL | 0.00048 |
| INDIA - BSNL MOVIL | 0.000479167 |
| INDIA - MOVIL | 0.000479167 |
| INDIA - MOVIL | 0.00048 |
| INDIA - MOVIL | 0.00048 |
| INDIA - MOVIL | 0.00048 |
| INDIA - MOVIL | 0.00048 |
| INDIA - VODAFONE MOVIL | 0.00048 |
| INDIA AIRTEL MOBILE | 0.000157552 |
| INDIA AIRTEL MOBILE | 0.00016 |
| INDIA BANGALORE | 0.000251675 |
| INDIA CHENNAI | 0.00025 |
| INDIA MUMBAI | 0.000151503 |
| INDIA OTHER MOBILE | 0.00023 |
| INDIA OTHER MOBILE | 0.00023491 |
| INDIA PUNE | 0.000252518 |
| INDIA VMSL MOBILE | 0.000246107 |
| INDIA VMSL MOBILE | 0.00025 |
| IRELAND DUBLIN | 0.00005 |
| IRLANDA | 0.00073 |
| IRLANDA - VODAFONE MOVIL | 0.00073 |
| ISRAEL | 0.00003 |
| ISRAEL | 0.000034791 |
| ISRAEL | 0.00031 |
| ISRAEL MOBILE | 0.00026 |
| ISRAEL MOBILE | 0.000264857 |
| ITALIA | 0.00033 |
| ITALIA | 0.00033 |
| ITALIA | 0.00033 |
| ITALIA | 0.00033 |
| ITALIA | 0.00033 |
| ITALIA - EUTELIA | 0.00684 |
| ITALIA - EUTELIA | 0.00684 |
| ITALIA - ROMA | 0.00027 |
| ITALIA - ROMA | 0.00027 |
| ITALIA - TIM MOVIL | 0.00444 |
| ITALIA - VODAFONE MOVIL | 0.002666667 |
| ITALY | 0.000057373 |
| ITALY | 0.00006 |
| ITALY H3G MOBILE | 0.003480632 |
| ITALY TI-M MOBILE | 0.00122 |
| ITALY TI-M MOBILE | 0.001223958 |
| ITALY VODAFONE MOBILE | 0.00128 |
| ITALY VODAFONE MOBILE | 0.001281331 |
| ITALY WIND MOBILE | 0.003499756 |
| JAPAN | 0.000195615 |
| JAPAN | 0.0002 |
| JAPAN MOBILE | 0.00062 |
| JAPAN TOKYO | 0.000209752 |
| KOREA SOUTH | 0.00011 |
| LUXEMBOURG | 0.00011 |
| MALTA | 0.00004434 |
| MAURITIUS | 0.002065279 |
| MEXICO | 0.00004 |
| MEXICO | 0.000042261 |
| MEXICO - EA FIJO | 0.0004375 |
| MEXICO - EA FIJO | 0.00044 |
| MEXICO - EA FIJO | 0.00044 |
| MEXICO - EA FIJO | 0.00044 |
| MEXICO - MGM FIJO | 0.00035 |
| MEXICO - MGM FIJO | 0.00035 |
| MEXICO - MGM FIJO | 0.00035 |
| MEXICO - MGM FIJO | 0.00035 |
| MEXICO - MOVISTAR MOVIL | 0.00083 |
| MEXICO - TELCEL MOVIL | 0.00142 |
| MEXICO - TELCEL MOVIL | 0.00142 |
| MEXICO - ZONA 2 | 0.00044 |
| MEXICO - ZONA 2 | 0.00044 |
| MEXICO - ZONA 2 | 0.00044 |
| MEXICO EA MOBILE | 0.00024 |
| MEXICO EA MOBILE | 0.000243193 |
| MEXICO GUADALAJARA | 0.00004 |
| MEXICO GUADALAJARA | 0.00004024 |
| MEXICO MEXICO CITY | 0.00004 |
| MEXICO MEXICO CITY | 0.00004024 |
| MEXICO MGM MOBILE | 0.000185191 |
| MEXICO MGM MOBILE | 0.00019 |
| MEXICO MOBILE | 0.00019 |
| MEXICO MOBILE | 0.00019097 |
| MEXICO MONTERREY | 0.00004 |
| MEXICO MONTERREY | 0.000040913 |
| MEXICO ON-NET A | 0.00003 |
| MEXICO ON-NET A | 0.000032483 |
| MYANMAR | 0.0029 |
| NETHERLANDS | 0.00015 |
| NETHERLANDS | 0.000152797 |
| NETHERLANDS KPN-M MOBILE | 0.000362276 |
| NETHRLDS T-MOBILE MOBILE | 0.000355713 |
| NETHRLDS T-MOBILE MOBILE | 0.00036 |
| NETHRLDS VODAFONE MOBILE | 0.000358964 |
| NETHRLDS VODAFONE MOBILE | 0.00036 |
| NEW ZEALAND | 0.00013 |
| NICARAGUA | 0.00166 |
| NICARAGUA | 0.001664212 |
| NICARAGUA MOBILE | 0.003317136 |
| NICARAGUA TELEFON MOBILE | 0.003246418 |
| NIGERIA MTN MOBILE | 0.000277509 |
| NIGERIA ZAIN MOBILE | 0.000239205 |
| PANAMA | 0.000265216 |
| PANAMA | 0.00027 |
| PANAMA C&W MOBILE | 0.001469266 |
| PANAMA MOVISTAR MOVIL | 0.00225 |
| PARAGUAY | 0.000389727 |
| PARAGUAY | 0.00039 |
| PARAGUAY | 0.00063 |
| PARAGUAY | 0.00063 |
| PARAGUAY ASUNCION | 0.00037 |
| PARAGUAY ASUNCION | 0.000374887 |
| PARAGUAY ASUNCION | 0.00052 |
| PARAGUAY ASUNCION | 0.00052 |
| PARAGUAY ASUNCION | 0.00052 |
| PARAGUAY CLARO MOB MOBILE | 0.000488388 |
| PARAGUAY CLARO MOB MOBILE | 0.00049 |
| PARAGUAY CLARO MOVIL | 0.0011 |
| PARAGUAY CLARO MOVIL | 0.0011 |
| PARAGUAY PERS MOBILE | 0.00082 |
| PARAGUAY PERS MOBILE | 0.00082182 |
| PARAGUAY PERSONAL MOVIL | 0.0011 |
| PARAGUAY TIGO MOBILE | 0.00086 |
| PARAGUAY TIGO MOBILE | 0.000861892 |
| PARAGUAY TIGO MOVIL | 0.00131 |
| PARAGUAY TIGO MOVIL | 0.00131 |
| PARAGUAY TIGO MOVIL | 0.00131 |
| PARAGUAY TIGO MOVIL | 0.00131 |
| PARAGUAY TIGO MOVIL | 0.00131 |
| PARAGUAY VOX MOBILE | 0.000747161 |
| PARAGUAY VOX MOBILE | 0.00075 |
| PERU | 0.00012 |
| PERU | 0.000124173 |
| PERU | 0.00019 |
| PERU - CLARO MOVIL | 0.00052 |
| PERU - CLARO MOVIL | 0.00052 |
| PERU - CLARO MOVIL | 0.00052 |
| PERU - LIMA MOVISTAR | 0.0001 |
| PERU - LIMA OTHERS | 0.00015 |
| PERU - LIMA OTHERS | 0.00015 |
| PERU - LIMA TELEFONICA | 0.0001 |
| PERU - LIMA TELEFONICA | 0.0001 |
| PERU - LIMA TELEFONICA | 0.0001 |
| PERU - LIMA TELEFONICA | 0.0001 |
| PERU - LIMA TELEFONICA | 0.0001 |
| PERU - LIMA TELEFONICA | 0.000104167 |
| PERU - MOVIL | 0.0049 |
| PERU - MOVIL | 0.0049 |
| PERU - MOVISTAR MOVIL | 0.00052 |
| PERU - MOVISTAR MOVIL | 0.00052 |
| PERU - MOVISTAR MOVIL | 0.00052 |
| PERU - MOVISTAR MOVIL | 0.00052 |
| PERU - NEXTEL MOVIL | 0.00085 |
| PERU AMERICA MOVIL MOBILE | 0.00028 |
| PERU AMERICA MOVIL MOBILE | 0.000281296 |
| PERU LIMA | 0.000045795 |
| PERU LIMA | 0.00005 |
| PERU MOBILE | 0.000346373 |
| PERU MOBILE | 0.00035 |
| PERU MOVISTAR MOBILE | 0.0003 |
| PERU MOVISTAR MOBILE | 0.000304597 |
| PERU RURAL | 0.00414 |
| PHILIPPINE GLOBE MOBILE | 0.001616059 |
| PHILIPPINE GLOBE MOBILE | 0.00162 |
| PORTUGAL | 0.00004 |
| PORTUGAL | 0.000042074 |

| | |
|---|---|
| PORTUGAL - MEO MOVIL | 0.00151 |
| PORTUGAL LISBON | 0.00004 |
| PORTUGAL LISBON | 0.000042074 |
| PORTUGAL OLO | 0.00004 |
| PORTUGAL OPTIMUS MOBILE | 0.00136 |
| PORTUGAL TMN MOBILE | 0.00136 |
| PUERTO RICO | 0.00007 |
| PUERTO RICO MOBILE | 0.00007 |
| PUERTO RICO RICO MOVIL | 0.00027 |
| REINO UNIDO | 0.000079167 |
| REINO UNIDO | 0.000079167 |
| REINO UNIDO | 0.000079167 |
| REINO UNIDO | 0.00008 |
| REINO UNIDO | 0.00008 |
| REINO UNIDO - VODAFONE MOVIL | 0.0002 |
| RUSSIA MOBILE | 0.001060541 |
| RUSSIA MOSCOW | 0.000142951 |
| RUSSIA VIMPELCOM MOBILE | 0.001749891 |
| RUSSIA VIMPELCOM MOBILE | 0.00175 |
| SAUDI ARABIA JAWAL MOBILE | 0.001549065 |
| SAUDI ARABIA JAWAL MOBILE | 0.00155 |
| SENEGAL EXPRESSO MOBILE | 0.005051026 |
| SENEGAL ORANGE MOBILE | 0.004417725 |
| SENEGAL ORANGE MOBILE | 0.00442 |
| SENEGAL TIGO MOBILE | 0.005445381 |
| SENEGAL TIGO MOBILE | 0.00545 |
| SERBIA | 0.001951625 |
| SINGAPORE MOBILE | 0.000066159 |
| SLOVAKIA ORANGE MOBILE | 0.00057308 |
| SOUTH AFRICA | 0.00019 |
| SOUTH AFRICA | 0.000193596 |
| SOUTH SUDAN | 0.00318 |
| SPAIN | 0.00008 |
| SPAIN | 0.000084147 |
| SPAIN CANARY IS | 0.000084147 |
| SPAIN ORANGE MOBILE | 0.00023 |
| SPAIN ORANGE MOBILE | 0.000231405 |
| SPAIN OTHER MOBILE | 0.00023 |
| SPAIN OTHER MOBILE | 0.000231405 |
| SPAIN TELEFONICA-M MOBILE | 0.00023 |
| SPAIN TELEFONICA-M MOBILE | 0.000231405 |
| SPAIN VODAFONE MOBILE | 0.00023 |
| SPAIN VODAFONE MOBILE | 0.000231405 |
| SUDAFRICA - VAS | 0.001221567 |
| SUIZA | 0.01641 |
| SUIZA - SWISSCOM MOVIL | 0.00642 |
| SUIZA - SWISSCOM MOVIL | 0.00648 |
| SUIZA - SWISSCOM MOVIL | 0.00648 |
| SUIZA - SWISSCOM MOVIL | 0.00648 |
| SURINAM | 0.00562 |
| SURINAM MOVIL | 0.00384 |
| SURINAME | 0.001597314 |
| SWEDEN | 0.00003 |
| SWEDEN | 0.000034424 |
| SWEDEN COMVIQ MOBILE | 0.00017 |
| SWEDEN TELIA-M MOBILE | 0.00017078 |
| SWITZERLAND | 0.00012 |
| SWITZERLAND | 0.000124308 |
| SWITZRLND SUNRISE MOBILE | 0.00545044 |
| SYRIA | 0.00096 |
| TURKEY CITIES | 0.000309461 |
| TURKEY ISTANBUL | 0.000299877 |
| TURKEY TURKCELL MOBILE | 0.001664597 |
| UK H3G MOBILE | 0.00012 |
| UK LOCAL RATE 84 | 0.00141 |
| UK LOCAL RATE 84 | 0.001413851 |
| UK O2 MOBILE | 0.00012 |
| UK O2 MOBILE | 0.000121921 |
| UK O3 | 0.000129441 |
| UK ORANGE MOBILE | 0.00012 |
| UK ORANGE MOBILE | 0.000121921 |
| UK T-MOBILE MOBILE | 0.00012 |
| UK T-MOBILE MOBILE | 0.000121921 |
| UK TIER1 MOBILE | 0.000200455 |
| UK VODAFONE MOBILE | 0.00012 |
| UK VODAFONE MOBILE | 0.000121921 |
| UKRAINE ASTELIT MOBILE | 0.00305 |
| UKRAINE KHARKIV | 0.00161089 |
| UKRNE KYIVSTAR MOB MOBILE | 0.002997118 |
| UNITED ARAB EMIRATES | 0.00211 |
| UNITED KINGDOM | 0.000038152 |
| UNITED KINGDOM | 0.00004 |
| UNITED KINGDOM OTHER MOBILE | 0.00241 |
| UNITED KINGDOM OTHER MOBILE | 0.002411764 |
| UNITED STATES | 0.000058922 |
| UNITED STATES | 0.00006 |
| URUGUAY | 0.00069 |
| URUGUAY | 0.000694577 |
| URUGUAY | 0.00092 |
| URUGUAY | 0.00092 |
| URUGUAY | 0.00092 |
| URUGUAY | 0.00092 |
| URUGUAY - ANCEL MOVIL | 0.00256 |
| URUGUAY - COLONIA | 0.00092 |
| URUGUAY - COLONIA | 0.00092 |
| URUGUAY - COLONIA | 0.00092 |
| URUGUAY - MALDONADO | 0.00092 |
| URUGUAY - MALDONADO | 0.00092 |
| URUGUAY - MALDONADO | 0.00092 |
| URUGUAY - MALDONADO | 0.00092 |
| URUGUAY - MONTEVIDEO | 0.00065 |
| URUGUAY - MONTEVIDEO | 0.00065 |
| URUGUAY - MONTEVIDEO | 0.00065 |
| URUGUAY - MONTEVIDEO | 0.00065 |
| URUGUAY - MONTEVIDEO | 0.00065 |
| URUGUAY - MOVISTAR | 0.00319 |
| URUGUAY - MOVISTAR | 0.00319 |
| URUGUAY - MOVISTAR | 0.00319 |
| URUGUAY ANCEL MOBILE | 0.00202 |
| URUGUAY ANCEL MOBILE | 0.002023773 |
| URUGUAY CLARO MOBILE | 0.001808291 |
| URUGUAY CLARO MOBILE | 0.00181 |
| URUGUAY MOBILE | 0.00177 |
| URUGUAY MONTEVIDEO | 0.00046 |
| URUGUAY MONTEVIDEO | 0.000462421 |
| URUGUAY MOVISTAR MOBILE | 0.00259 |
| URUGUAY MOVISTAR MOBILE | 0.002593109 |
| USA HAWAII | 0.000179025 |
| USA NORTH A 8XX | 0.00005 |
| USA NORTH A 8XX | 0.000053718 |
| USA PREMIUM | 0.000106121 |
| VENEZUELA | 0.00015 |
| VENEZUELA | 0.000152254 |
| VENEZUELA - CANTV FIJA | 0.001 |
| VENEZUELA - CANTV FIJA | 0.001 |
| VENEZUELA - CARACAS TELCEL | 0.00079 |
| VENEZUELA - DIGITEL MOVIL | 0.00153 |
| VENEZUELA - MOVILNET MOVIL | 0.00152 |
| VENEZUELA - MOVILNET MOVIL | 0.00152 |
| VENEZUELA DIGITEL MOBILE | 0.00106 |
| VENEZUELA DIGITEL MOBILE | 0.001060409 |
| VENEZUELA MOVILNET MOBILE | 0.00098 |
| VENEZUELA MOVILNET MOBILE | 0.00098394 |
| VENEZUELA MOVISTAR MOBILE | 0.001127878 |
| VENEZUELA MOVISTAR MOBILE | 0.00113 |
| VENEZUELA OFF NET | 0.0002 |
| VENEZUELA OFF NET | 0.000204914 |

Fuente: Crossfone Argentina SA (2016)

## ANEXO IV: Destinos de alto riesgo

El siguiente cuadro lista algunos de los destinos asociados comúnmente a escenarios de fraude de terminación.

**Cuadro 13 - Destinos y prefijos asociados a fraudes**

| Destino | Prefijo de telefonía |
|---|---|
| Afganistán | 93 |
| Albania (móviles) | 3556 |
| Bielorrusia | 375 |
| Bosnia | 387 |
| Bulgaria | 359 |
| Burundi | 257 |
| Chile | 56 |
| Corea del Norte | 850 |
| Costa de Marfil | 225 |
| Cuba | 53 |
| Diego García | 246 |
| Yibuti | 253 |
| Eritrea | 291 |
| Eslovenia | 386 |
| Estonia | 372 |
| Etiopía | 251 |
| Gabón | 241 |
| Gambia | 220 |
| Guinea-Bisáu | 245 |
| Guyana | 592 |
| Haití | 509 |
| Honduras | 504 |
| Isla Ascensión | 247 |
| Isla de San Cristóbal | 1869 |
| Isla Santa Elena | 290 |
| Islas Comoras | 269 |
| Islas Cook | 682 |
| Islas Malvinas | 500 |
| Islas Reunión | 262 |
| Islas Salomón | 677 |
| Islas Seychelles | 248 |
| Islas Turcas y Caicos | 1649 |
| Islas Vírgenes Británicas | 1284 |
| Jordania | 962 |
| Kiribati | 686 |
| Letonia | 371 |
| Liberia | 231 |
| Libia | 218 |
| Liechtenstein | 423 |
| Lituania | 370 |
| Madagascar | 261 |
| Maldivas | 960900 |
| Mali | 223 |
| Nicaragua | 505 |
| Nigeria | 227 |
| Palestina | 970 |
| República de Benín | 229 |
| Republica de Guinea | 224 |
| Republica del Congo | 243 y 242 |
| San Marino | 378 |
| Santo Tomé y Príncipe | 239 |
| Senegal | 221 |
| Serbia | 381 |
| Sierra Leona | 232 |
| Siria | 963 |
| Sistemas Satelitales | 882 |
| Somalia | 252 |
| Sudan | 249 |
| Surinam | 597 |
| Timor del este | 670 |
| Togo | 228 |
| Túnez | 216 |

Fuente: Elaboración Propia (2016)

## ANEXO V: Estadísticas de telefonía

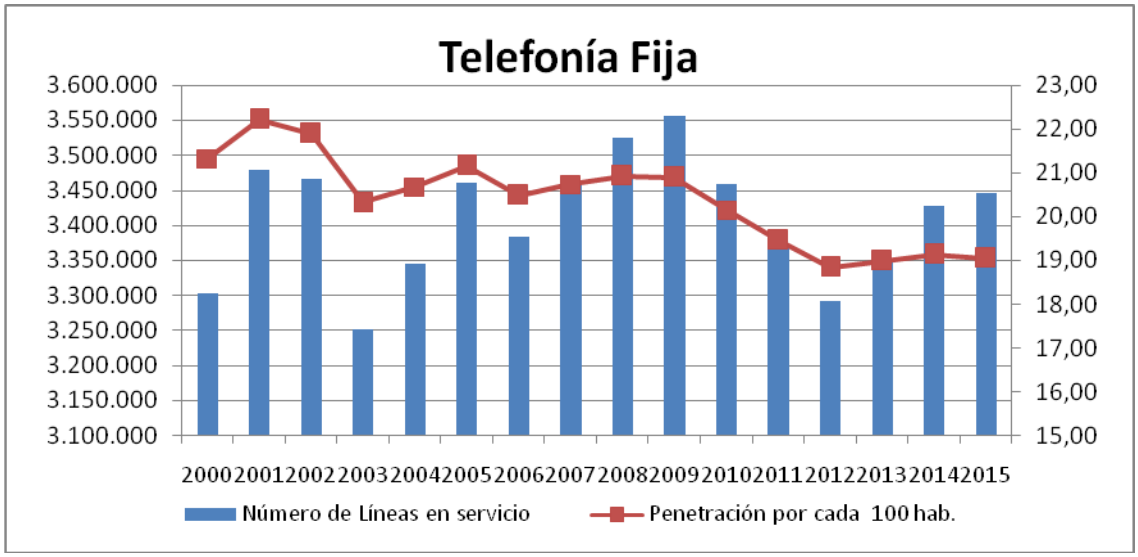
A continuación se reproduce la variación del servicio de telefonía para Chile según estadísticas recuperadas de la Subsecretaría de Telecomunicaciones de Chile.

**Cuadro 14 - Líneas totales en servicio de telefonía fija**

| Año | Mes | Número de líneas en servicio | Crecimiento año anterior | Penetración por cada 100 hab. |
|---|---|---|---|---|
| **2000** | **Dic** | 3,302,498 | | 21.33 |
| **2001** | **Dic** | 3,478,492 | 5.33% | 22.21 |
| **2002** | **Dic** | 3,467,013 | -0.33% | 21.90 |
| **2003** | **Dic** | 3,252,063 | -6.20% | 20.32 |
| **2004** | **Dic** | 3,345,102 | 2.86% | 20.67 |
| **2005** | **Dic** | 3,460,645 | 3.45% | 21.17 |
| **2006** | **Dic** | 3,383,597 | -2.23% | 20.49 |
| **2007** | **Dic** | 3,459,611 | 2.25% | 20.74 |
| **2008** | **Dic** | 3,524,790 | 1.88% | 20.92 |
| **2009** | **Dic** | 3,555,311 | 0.87% | 20.90 |
| **2010** | **Dic** | 3,459,367 | -2.70% | 20.15 |
| **2011** | **Dic** | 3,370,104 | -2.58% | 19.45 |
| **2012** | **Dic** | 3,292,502 | -2.30% | 18.84 |
| **2013** | **Dic** | 3,347,231 | 1.66% | 18.98 |
| **2014** | **Dic** | 3,427,749 | 2.41% | 19.14 |
| **2015** | **Dic** | 3,445,880 | 0.53% | 19.04 |

Fuente: Subsecretaría de Telecomunicaciones de Chile (2016)

**Gráfico 17 - Líneas totales en servicio de telefonía fija**



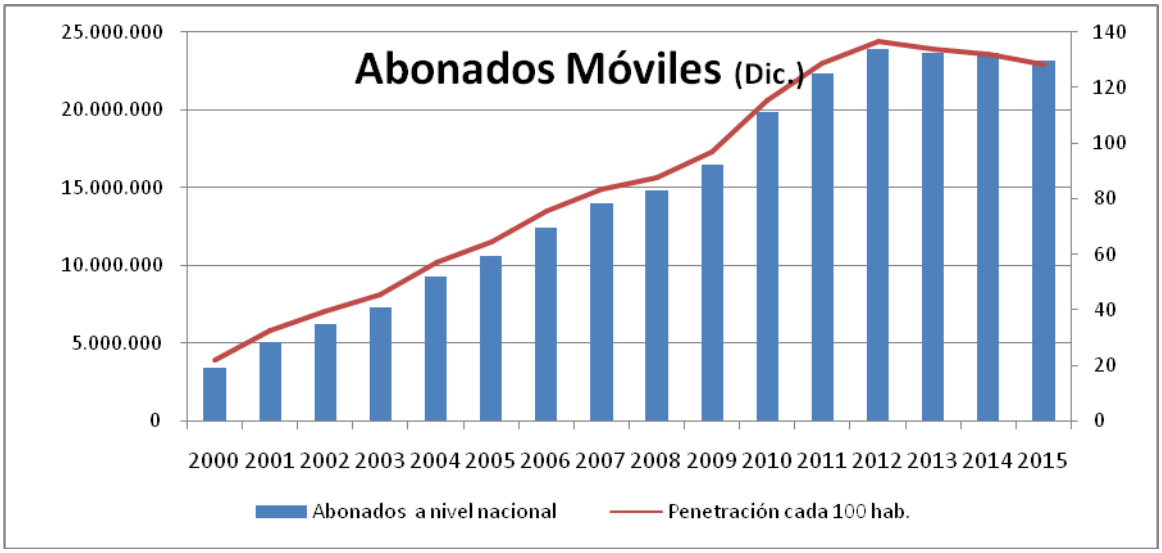

Fuente: Subsecretaría de Telecomunicaciones de Chile (2016)

## Cuadro 15 - Abonados totales en servicio de telefonía móvil

| Año | Mes | Abonados a nivel nacional | Crecimiento anual | Penetración cada 100 hab. |
|---|---|---|---|---|
| **2000** | **Dic** | 3,401,525 | | 21.97 |
| **2001** | **Dic** | 5,100,783 | 49.96% | 32.57 |
| **2002** | **Dic** | 6,244,310 | 22.42% | 39.44 |
| **2003** | **Dic** | 7,268,281 | 16.40% | 45.41 |
| **2004** | **Dic** | 9,261,385 | 27.42% | 57.24 |
| **2005** | **Dic** | 10,569,572 | 14.13% | 64.65 |
| **2006** | **Dic** | 12,450,801 | 17.80% | 75.39 |
| **2007** | **Dic** | 13,955,202 | 12.08% | 83.66 |
| **2008** | **Dic** | 14,796,593 | 6.03% | 87.83 |
| **2009** | **Dic** | 16,450,223 | 11.18% | 96.70 |
| **2010** | **Dic** | 19,852,242 | 20.68% | 115.61 |
| **2011** | **Dic** | 22,315,248 | 12.41% | 128.80 |
| **2012** | **Dic** | 23,940,973 | 7.29% | 136.96 |
| **2013** | **Dic** | 23,661,339 | -1.17% | 134.18 |
| **2014** | **Dic** | 23,680,718 | 0.08% | 132.20 |
| **2015** | **Dic** | 23,206,353 | -2.00% | 128.22 |

Fuente: Subsecretaría de Telecomunicaciones de Chile (2016)

## Gráfico 18 - Abonados totales en servicio de telefonía móvil




Fuente: Subsecretaría de Telecomunicaciones de Chile (2016)

# CURRICULUM VITAE

40 años, Argentina, Soltero.
Charcas 2956 1E (1425)
Palermo, Capital Federal, Argentina
Tel. (011) 48229425 / (011) 1534273414
**garciacarral@gmail.com**

**Experiencia Laboral:**

---

04.2014 – PRESENTE | **Interdotnet Argentina SRL (http://www.ar.inter.net)**

**Gerente de Operaciones**
**Descripción**: Gerente de Operaciones para Interdotnet SRL con funciones de liderazgo sobre las áreas de Diseño y Desarrollo Web, Email Marketing y servicios de hosting, conectividad y datacenter. Desempeñándome actualmente en la empresa que resultó de la fusión de la cartera de clientes de Intermedia Comunicaciones, Desarrollos Digitales e Interdotnet Argentina SRL. Mis funciones incluyen gerenciar los servicios de infraestructura (datacenter, servidores virtuales y hosting), el equipo de diseñadores web, el *software factory* interno (y recursos externos) y el equipo de servicios de email marketing. Adicionalmente sirvo como PM y pre-venta para proyectos de desarrollo de clientes en el exterior (USA) relacionados con medicina, publicidad digital, procesos industriales y otros.

08.2012 – 03.2014 | **Intermedia Comunicaciones (http://www.intermediasp.com)**

**Gerente General**
**Descripción**: Gerente General para IntermediaSP con funciones sobre los departamentos de desarrollo, tecnología y soporte, comercial y administración. IntermediaSP brinda una cadena de valor que incluye diseño y desarrollo web, sumado a soluciones de infraestructura de internet y alojamiento web. Asumí la gerencia general de la empresa a pedido de su socio gerente. La empresa poseía un rojo financiero muy alto y un EBIDTA negativo en el ultimo año. Se realizó la restructuración de personal necesario, redefinición de productos y precios, cambios de infraestructura y refinanciamiento de deudas para llegar al *break even*. Cuando la empresa se encontró en estado operativo sano, su cartera comercial fue vendida a Interdotnet Argentina.

01.2008 - PRESENTE

**Consultor externo**
**Descripción**: Consultor externo para empresas de telecomunicaciones, telefonía o servicios de infraestructura y datos en general.

Algunos de los proyectos en que estuve involucrado:

- Auditoría del servicio de telefonía y propuesta de mejoras de conectividad y telefonía para **Infracom S.A.**
- Asesor externo para **GlobalviewS.A.** sobre problemáticas y mejoras a su red de videovigilancia para el gobierno de la **Ciudad de Buenos Aires**.

- Asesor externo para el *contact center***Next S.A** sobre su red de datos.

- Asesor externo para la empresa de telefonía **Alvis S.A.** sobre redes, infraestructura, productos y nuevos negocios.

- Asesor externo para el **gobierno provincial de La Rioja** en su proyecto de telefonía en el marco de "Internet para Todos".

- Asesor externo y capacitador sobre redes de datos para **Avenida.com**.

02.2012 - 07.2012 | **DINMAX Consulting (http://www.dinmax.com)**

**Project Leader unidad de videojuegos**
**Descripción**: PM de la nueva unidad de videojuegos para plataformas móviles (iOS).

07.2009 - 02.2012 | **CROSSFONE (http://www.crossfone.com.ar/)**

**Director de Operaciones.**
**Descripción**: Diagramación de los procesos internos de la empresa. Management de proyectos. Responsabilidad y dirección sobre las aéreas de Ingeniería, Networking, NOC, IT, Desarrollo y Logística. Plan de negocios y centro de costos. Participación en las estrategias de producto de la empresa. Elaboración de consultorías en campos relacionados a VoIP, *networking*, seguridad informática y servicios de Internet. Virtualización de infraestructura utilizando productos de la suite de Vmware. Desarrollo de planes de *backup* y contingencia. Análisis de nuevas tecnologías. Desarrollo y seguimiento de los planes de carrera de los empleados de las aéreas a cargo. Generación de procesos internos para la empresa.

08.2011 - PRESENTE | **Multilat**

**Consultor externo.**
**Descripción**: Consultor externo para organismos multilaterales (OEI), en especial la confección de pliegos de ofertas publicas o el análisis de ofertas a pliegos de organismos del estado.

12.2005 – 07-2009 | **CROSSFONE (http://www.crossfone.com.ar/)**

**Gerente de Ingeniería y IT.**
**Descripción**: Proyección y administración de la red de voz y datos de Crossfone Argentina (carrier VoIP) que cuenta con servicios diversos de soluciones de voz por IP (Tarjetas prepagas, clientes corporativos, venta de minutos *wholesale*, líneas telefónicas mediante broadband, etc.). Administración de gateways (Cisco AS, Quintum, etc), Softswitchs (Nextone), routers (Cisco), LAN switches (Cisco, Huawei), SBCs que forman la red de la empresa y su interrelación con la filial madre en USA. Diagramación y proyección de las nuevas interconexión de voz (TDM o VoIP) y datos. Liderar las tareas de los otros ingenieros del área. Liderar el área de IT sobre la que recae la administración de servidores, networking y soporte interno. Costeo de recursos del área. Participación en la creación de nuevos proyectos o productos. Participación en la tarifación de las llamadas. Responsabilidad de funcionamiento del backbone de datos y voz de la empresa. Generar documentación y planes de contingencia. Consultaría externa en servicios de acceso a Internet y telefonía en redes de Cable.

11.2001 - 01.2006 | **CABASE (http://www.cabase.org.ar)**

**Coordinador Técnico del NAP CABASE**.
**Descripción**: Dirección y coordinación técnica del nodo de intercambio de tráfico de Internet nacional NAP CABASE. Relación con los responsables técnicos de empresas ISPs y carriers. Creación de normas de interconexión, publicación de redes, cableado, SLAs en relación a la actividad en un NAP (IX)

02.1999 - 12.2005 | **Intermedia Comunicaciones (http://www.intermediasp.com)**

**Gerente de Tecnología.**
**Descripción**: Mis tareas eran planificar, administrar e implementar la plataforma tecnológica de servicios ISP, contenidos y aplicaciones de IntermediaSP, a la vez que dirigí el área de Soporte Técnico a clientes. Esto incluía el mantenimiento de la red, servicios y hardware de la empresa, como así mismo de clientes. También el realizar consultorías de redes, seguridad y servicios de Internet a empresas, y el desarrollar proyectos integrales de redes e Internet, realización de presupuestos de ventas y soporte pre-venta a clientes corporativos.

02.2000 - 12.2000 | **RodríguezRodríguez y Asociados**

**Consultor externo.**
**Descripción**: Consultoría de sistemas informáticos y seguridad a empresas financieras. Diseño de redes. Cableado estructurado a edificios. Armado de centro de datos. Diseño de puestos de trabajo. Instalación de circuitos de CCTV.

**Educación Académica:**

---

03.1995 - 08.2003 | **Universidad de Buenos Aires (UBA)**. Ingeniero Electrónico.

08.2006 - 06.2008 | **Universidad de Buenos Aires (UBA)**. Abogado (abandonado).

08.2008 - 08.2010 | **Universidad de Palermo (UP)**. MBA. (falta entregar tesis).