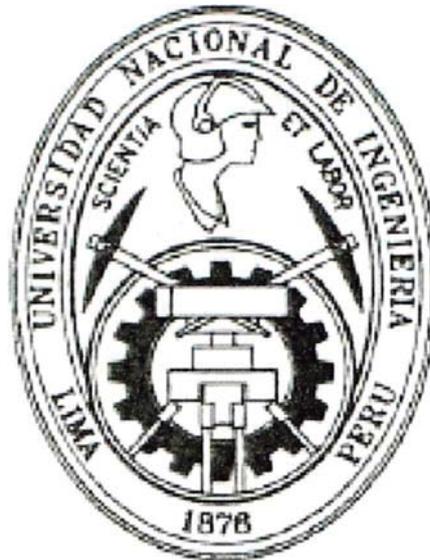


UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas



**MEJORA EN LA GESTION DEL FRAUDE EN
TELECOMUNICACIONES**

INFORME DE SUFICIENCIA

Para optar el título profesional de

INGENIERO INDUSTRIAL

CARLOS ENRIQUE CASTILLO HIGINIO

**LIMA – PERU
2005**

El presente Informe de Suficiencia esta dedicado a mi nuevo gran amor

Sofia Valentina

Agradecimientos especiales a mis padres por el apoyo brindado a lo largo de todos estos años, así como a toda la comunidad de mi Alma Mater por haberme formado y soportado todos mis años de estudios.

INDICE

DESCRIPTORES TEMATICOS	1
RESUMEN EJECUTIVO	2
INTRODUCCION	4
1. CAPITULO I : ANTECEDENTES	5
1.1 MISION	
1.2 VISION	
1.3 DIAGNOSTICO ESTRATEGICO	6
1.3.1 ANTECEDENTES DE LA EMPRESA	6
1.3.2 FORTALEZAS Y DEBILIDADES	7
1.3.3 OPORTUNIDADES Y RIESGOS	9
1.4 DIAGNOSTICO FUNCIONAL	10
1.4.1 SERVICIOS	10
1.4.2 CLIENTES Y PROVEEDORES	11
1.4.3 PROCESOS	11
1.4.4 ORGANIZACIÓN	13
2. CAPITULO II : MARCO TEORICO	16
2.1 FRAUDE EN TELECOMUNICACIONES	16
2.2 IMPACTOS DEL FRAUDE EN LAS EMPRESAS	16
2.2.1 MOTIVOS DEL FRAUDE EN TELECOMUNICACIONES	17
2.2.2 COSTOS DIRECTOS	17
2.2.3 COSTOS INDIRECTOS	17
2.3 PRINCIPALES TIPOS DE FRAUDE	18
2.3.1 FRAUDE EN LA RED FIJA	18
2.3.2 FRAUDE EN LA RED CELULAR	21
2.4 GESTION DE FRAUDE	23
2.5 FASES DE LA GESTION DEL FRAUDE	26
2.6 REDISEÑO DE PROCESOS	27
2.6.1 EJES DE ACTUACION	28
2.6.2 PREGUNTAS FRECUENTES	28
2.6.3 HERRAMIENTAS UTILIZADAS	29
2.6.4 EQUIPOS DE TRABAJO	33
3. CAPITULO III: PROCESO DE TOMA DE DECISIONES	34
3.1 PLANTEAMIENTO DEL PROBLEMA	34
3.2 ALTERNATIVAS DE SOLUCION	36
3.3 METODOLOGIA DE SOLUCION	40

3.3.1	ANÁLISIS DE DATOS	41
3.3.1.1	DATOS HISTÓRICOS	41
3.3.1.2	INDICADORES DE GESTIÓN	41
3.3.1.3	INTERACCIÓN ENTRE LAS ÁREAS	44
3.3.2	LEVANTAMIENTO DE PROCESOS	50
3.3.3	DOCUMENTOS Y SISTEMAS DE APOYO	57
3.3.4	LEVANTAMIENTO DEL PERFIL DE CONOCIMIENTOS	59
3.3.5	ELABORACIÓN DEL DIAGNÓSTICO	60
3.4	ESTRATEGIAS ADOPTADAS	61
3.5	TOMA DE DECISIONES	62
4.	CAPITULO IV :EVALUACION DE RESULTADOS	81
5.	CAPITULO V :CONCLUSIONES Y RECOMENDACIONES	86
6.	BIBLIOGRAFIA	89
7.	ANEXOS	90

DESCRIPTORES TEMATICOS

Telecomunicaciones

Fraude Evitado

Fraude Detectado

Umbral

CDR

Antifraude

Rediseño de Procesos

Indicadores de gestión

E-business

Incobrables

RESUMEN EJECUTIVO

En la actualidad el fraude en telecomunicaciones es uno de los problemas más graves que vienen afectando a las empresas de telecomunicaciones en todo el mundo, generando grandes pérdidas económicas y de imagen a la misma. El fraude en la Industria de las telecomunicaciones ha causado perjuicios de muchos billones de dólares a las operadoras en todo el mundo. Consecuentemente, las pérdidas de ingresos son enormes, con relación al no pago de llamadas, servicios y productos. En el medio peruano existen diversas modalidades de fraude que afectan la red de telecomunicaciones.

Somos una empresa de servicios que pertenece a un grupo empresarial en el rubro de las telecomunicaciones. Nuestros clientes actualmente son todas las Unidades de negocios del grupo, Los servicios que brindamos son especializados que permiten que las Unidades de Negocios concentren esfuerzos en las actividades que le generan mayor valor (razón del negocio). Actualmente el problema que presenta la Gerencia

de Control de Fraude es en el proceso de la gestión del fraude por su elevado tiempo de ciclo.

La solución que se propone es el rediseño del proceso de gestión de fraude con las iniciativas de reducción de sub. Procesos de control, estandarización de los procesos, creación de una cultura de prevención del fraude y el secreto de las telecomunicaciones y todo soportado por un sistema de gestión (aplicativo e-business) que centralice la información, esta solución nos va permitir reducir considerablemente los tiempos de atención, y mejorar el servicio en calidad, seguridad y oportunidad. Con la actual coyuntura que vive las empresas la nueva solución nos permitirá también administrar nuestros recursos y aumentar el margen de ganancia a la Gerencia.

INTRODUCCION

El objetivo del presente informe es poner a disposición de la Empresa y nuestros clientes una alternativa de solución a la problemática de nuestro servicio de Control de Fraude

El cambio en los procesos permitirá una disminución de los tiempos de ciclo y esto a su vez generará menos pérdidas económicas y de imagen al grupo telefónica. Se mejorara las calidad del servicio, tiempos de atención, se podrán determinar las responsabilidades a lo largo de todo el proceso identificado por las fases de la gestión de fraude.

Otro de los beneficios que se espera es el ahorro generado en los proceso de facturación y cobranza así como en la atención de reclamos.

Cabe mencionar que mucha información no se presenta en el informe por motivos de confidencialidad de la información. Se presenta en forma genérica.

CAPITULO I

ANTECEDENTES

1.1 MISION

Proporcionar servicios profesionales de Control de Fraude y Protección de la Información Empresarial con eficiencia calidad y oportunidad, para apoyar el normal desarrollo de las actividades de nuestro cliente, Minimizando las pérdidas económicas y de imagen en todos los clientes, concentrándonos en la prevención, detección, disuasión del fraude y la creación de nuevos servicios, ampliando progresivamente nuestra cobertura de control.

1.2 VISION

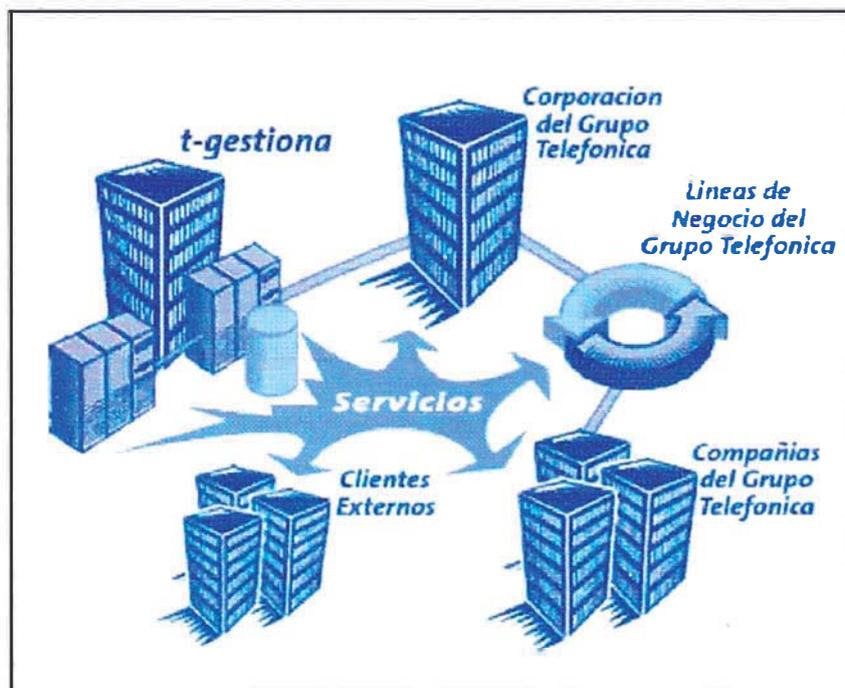
Ser el proveedor líder del mercado en servicios De Control de Fraude y Protección de la Información Empresarial del Grupo Telefónica y empresas Externas, en términos de calidad, precio y oportunidad.

1.3 DIAGNOSTICO ESTRATEGICO

1.3.1 ANTECEDENTES DE LA EMPRESA

Somos una empresa del Grupo Telefónica especializada en la prestación de servicios de gestión de negocios bajo el modelo de Centro de Servicios Compartidos. Nuestro objetivo es no sólo realizar esas tareas sino gestionarlas eficientemente en nombre de nuestros clientes, quienes mantienen, no obstante, control sobre las mismas.

Somos una compañía capaz de prestar servicios administrativos a uno de los grupos empresariales más importante del mercado peruano: el Grupo Telefónica, capaz de unir a más de 12 millones de clientes, dando acceso a todos sus clientes a un nuevo mundo de posibilidades avanzadas en comunicación.



El CSC en el Grupo

La presencia y liderazgo del Grupo Telefónica en Latinoamérica y Europa posibilitan a ofrecer servicios de máxima calidad al disponer de los mejores profesionales, de procesos orientados a las mejores prácticas, y de sistemas de “**e-Business**” última generación para mejorar la relación con nuestros clientes, así como los clientes y proveedores de estos.

En las siguientes líneas vamos enfocarnos en la Sub. Gerencia de Control de Fraude de Telefónica Gestión de Servicios Compartidos Perú. S.A.C. y el servicio de Control de Fraude en Telecomunicaciones.

1.3.2 FORTALEZAS Y DEBILIDADES

1.3.2.1 FORTALEZAS

1.3.2.1.1 Respaldo del grupo empresarial “Grupo Telefónica” líder en Latinoamérica y en Europa capaz de unir a más de 80 millones de clientes, en más de 40 países

1.3.2.1.2 know how en el servicio de Control de Fraude en Telecomunicaciones en el país, con una experiencia comprobada de 7 años brindando el servicio.

1.3.2.1.3 Capacidad de cobertura a nivel nacional, nuestros sistemas comerciales, administrativos y de control

se encuentran distribuidos en toda la red telefónica a nivel nacional.

1.3.2.1.4 Confidencialidad en el manejo de la información, administramos la jefatura de Protección de la Información Empresarial que brinda servicios a todo el Grupo Telefónica. En los 7 años de actividad no se han presentado casos de fuga de información clasificada que atente con las leyes de protección de las telecomunicaciones.

1.3.2.1.5 Conocimiento de las necesidades de nuestros clientes, Conocemos todos los productos y servicios que brindan los negocios del grupo y formamos parte del comité de nuevos productos.

1.3.2.1.6 No existe competidor en el mercado, hasta la fecha no existe ninguna empresa en el mercado peruano que ofrezca dicho servicio. No existen consultoras y organizaciones que brinden capacitación especial en el tema de Control de Fraude en Telecomunicaciones.

1.3.2.2 DEBILIDADES

1.3.2.2.1 Falta de integración de los procesos, los procesos son independientes no existe un proceso definido para la gestión del fraude o un proceso que

integre a las áreas comprometidas en los casos de fraude.

1.3.2.2.2 Procesos de atención burocráticos, existen procesos en los cuales se requiere de muchos tramites innecesarios para la ejecución de tratamientos de fraude.

1.3.2.2.3 Falta de cultura de atención al cliente, antes del 2001 pertenecíamos a Telefónica del Perú. S.A. (Operadora de Telefonía Fija), éramos parte del proceso, ahora brindamos el servicio.

1.3.2.2.4 Falta de conocimiento del Fraude en telecomunicaciones, existen áreas en el proceso de gestión de fraude que no tienen claros los conceptos del fraude en telecomunicaciones y sus consecuencias.

1.3.3 OPORTUNIDADES Y RIESGOS

1.3.3.1 OPORTUNIDADES

1.3.3.1.1 Imagen de marca en el mercado, con la marca existente de TELEFONICA podemos salir a ofrecer nuestros servicios de control de fraude a diferentes operadoras que existe en el mercado

1.3.3.1.2 Proyectos e-business, política corporativa aplicada en toda la región.

1.3.3.1.3 Oportunidad de brindar los servicios a países de la región. Regionalización de los servicios, mejores prácticas.

1.3.3.2 RIESGOS

1.3.3.2.1 Dependencia de procesos, muchos de nuestros procesos pertenecen a los negocios del grupo

1.3.3.2.2 No existen leyes que regulen el fraude en telecomunicaciones.

1.4 DIAGNOSTICO FUNCIONAL

Tres servicios que brinda las Sub. Gerencia de Control de Fraude:

1.4.1 SERVICIOS

1.4.1.1 SERVICIO DE CONTROL DE FRAUDE EN TELECOMUNICACIONES

Servicio de protección de ingresos de EL CLIENTE, ante la eventualidad de Fraude en Telecomunicaciones perpetrado por personal interno, malos clientes, entidades y/o personas fraudulentas en los diferentes servicios que la Empresa ofrece, minimizando el impacto en los aspectos Económico-Financieros de la Empresa, mediante la prevención, detección, análisis, solución y disuasión para enfrentar las diferentes tipologías de Fraude en Telecomunicaciones

1.4.1.2 SERVICIO DE PROTECCION DE LA INFORMACION EMPRESARIAL:

Brindar a los Clientes los conceptos y herramientas básicas de Protección de la Información Empresarial y asesorarlos en la implementación de la Política y Normativas que la sustentan, aportando a la disminución de los riesgos de pérdida o fuga de la información clasificada (Reservada, Restringida y de Uso Interno) de la Empresa.

1.4.1.3 SERVICIO DE INFORMACIONES DE SEGURIDAD:

Servicio que comprende la realización de investigaciones a solicitud de EL CLIENTE, ante hechos irregulares que afecten los intereses e imagen del mismo.

1.4.2 CLIENTES Y PROVEEDORES

Por el nivel de ingresos nuestros clientes están dividido como:

1.4.2.1 CLIENTES VIP

- Operadora de Telefonía Fija (OTF)
- Telefónica Corporativo
- Telefónica Móviles

1.4.2.2 GRANDES CLIENTES

- Telefónica Multimedia
- Telefónica Empresas (ex – Telefónica Data)
- Telefónica Publicidad e Imagen

1.4.2.3 CLIENTES GENERALES

- Transporte urgente de mensajes SAC (TUMSAC)
- Terra
- Teleatento Perú

1.4.3 PROCESOS

Los procesos más importantes que se presentan en la gestión del fraude son los siguientes:

1.4.3.1 PROCESO DE GESTION DE FRAUDE RED FIJA

Proceso que se ejecuta para la Red Fija, en este proceso se detectan los casos de fraude que afectan dicha red. En el proceso están involucrados diversas gerencias de los negocios (Clientes), como son Facturación y Cobranzas, Servicios Comerciales, OMRS, atención al cliente, más adelante describiremos el proceso en forma detallada.

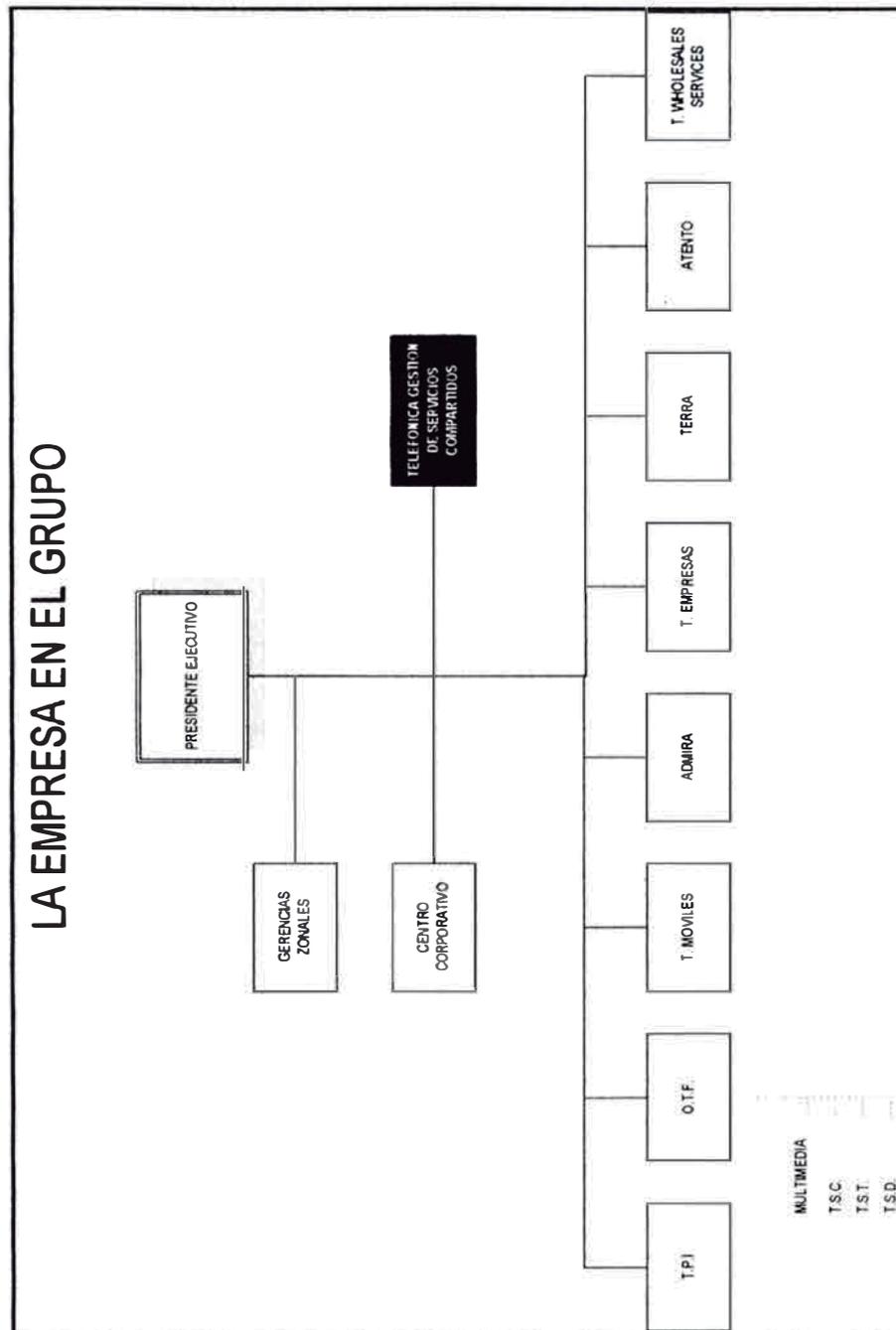
1.4.3.2 PROCESO DE GESTION RED MOVIL

Proceso que se ejecuta para la Red Móvil, en este proceso se detectan los casos de fraude que afectan dicha red. En el proceso están involucrados diversas gerencias del negocio de Telefónica Móviles, como son Facturación y Cobranzas, Servicios Comerciales, OMRS, atención al cliente, más adelante describiremos el proceso en forma detallada.

1.4.4 ORGANIZACIÓN

1.4.4.1 LA EMPRESA EN EL GRUPO

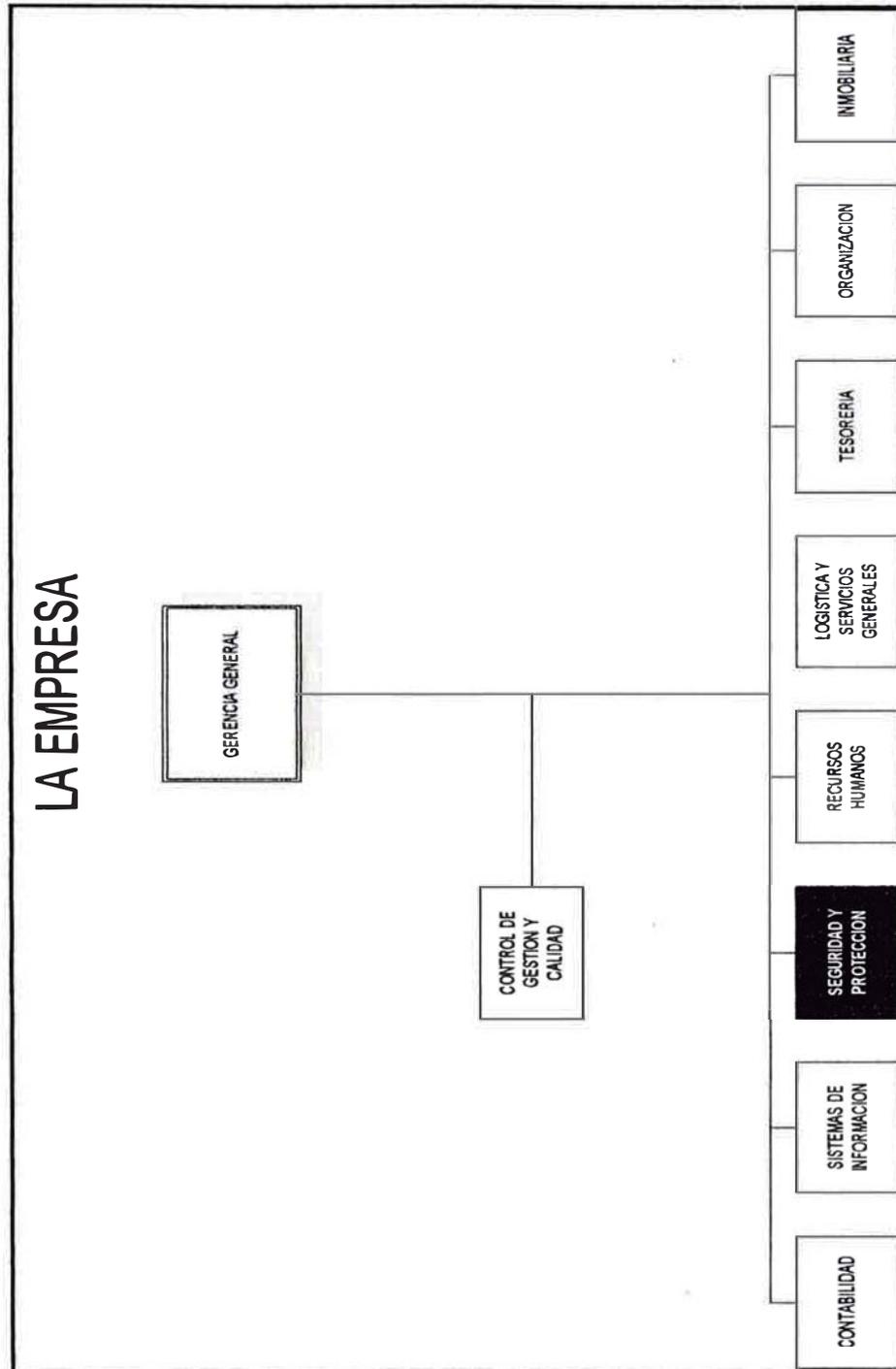
La ubicación de **Telefónica Gestión de Servicios Compartidos Perú SAC.**



Organigrama Grupo Telefónica

1.4.4.2 LA EMPRESA

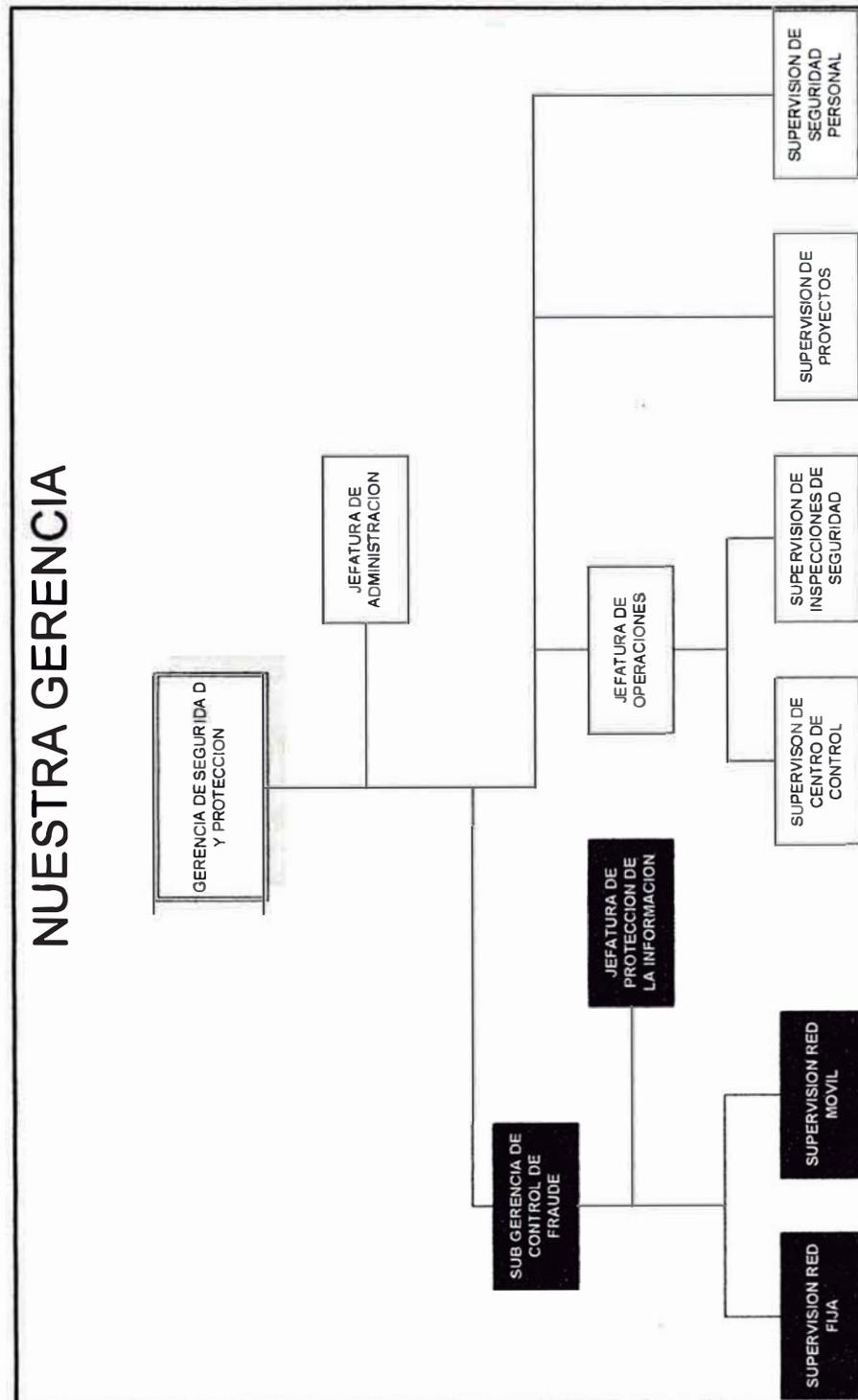
El organigrama de **Telefónica Gestión de Servicios Compartidos Perú SAC.**



Organigrama Telefónica Gestión Servicios Compartidos

1.4.4.3 NUESTRA GERENCIA

Organigrama Gerencia de Seguridad y Protección



Ubicación de la Sub. Gerencia de Control de Fraude

CAPITULO II

MARCO TEORICO

2.1 FRAUDE EN TELECOMUNICACIONES

Consiste en la utilización del producto o servicio de telecomunicaciones con la intención del no pago.

El fraude en la Industria de las telecomunicaciones ha causado perjuicios de muchos billones de dólares a las operadoras en todo el mundo. Consecuentemente, las pérdidas de ingresos son enormes, con relación al no pago de llamadas, servicios y productos. Los costos de esas acciones generan serios problemas a ser cuantificados

2.2 IMPACTOS DEL FRAUDE EN LAS EMPRESAS

Diariamente varios casos de fraude son reportados por las empresas operadoras de telecomunicaciones

Los costos reales de fraude pueden ser muy superiores que el ingreso perdido. El Impacto real es raramente cuantificado reduciendo la visibilidad y la eficiencia de las medidas y acciones de combate antifraude.

2.2.1 MOTIVOS DEL FRAUDE EN TELECOMUNICACIONES

- Causar perdida o daño : Vándalos
- Ahorrar dinero :Defraudador Casual Oportunista
- Por fama: Hacker
- Para hacer Dinero: Defraudador profesional
- Aumento del anonimato :Delincuente

2.2.2 COSTOS DIRECTOS

- Pago por interconexiones.
- Costos administrativos.
- Ventas, Recaudaciones, facturaciones, Cobranza.
- Reclamos relacionados al fraude.
- Gestión de Fraude.

2.2.3 COSTOS INDIRECTOS

- Planificación del mercado basado en niveles elevados de fraude.
- Impactos negativos en los clientes y en la imagen de la empresa.
- Inversiones de redes basadas en datos erróneos.

2.3 PRINCIPALES TIPOS DE FRAUDE

Los fraudes son las mayores fuentes de perjuicio en la industria de las telecomunicaciones y en nuestro mercado puede ser dividida en las siguientes principales categorías:

2.3.1 FRAUDE EN LA RED FIJA

2.3.1.1 FRAUDE POR SUSCRIPCION

En ese tipo de fraude el fraudador adquiere la línea telefónica con la intención de no pagar la cuenta telefónica, luego el uso anormal ocurre dentro del periodo activo de la línea telefónica. Generalmente la línea telefónica es usada para vender llamadas o para el uso usufructo propio del fraudador.

En nuestro medio el Fraude por suscripción consiste en la obtención de líneas telefónicas con la utilización de documentación falsa o mediante la suplantación de personas con documentación verdadera sin conocimiento del titular

2.3.1.2 FRAUDE POR HURTO DE LÍNEA

Consiste en el uso ilegal del servicio por terceras personas logrado a través de una derivación del hilo telefónico desde puntos vulnerables de la planta externa.

Este fraude es el que actualmente está generando la mayor cantidad de pérdidas a la empresa. Pese a las medidas técnicas de prevención, control, detección y operativas realizadas no se ha obtenido resultados satisfactorios.

De ha detectado que esta modalidad de fraude es complementada con el uso de interfaces electrónicas conectadas a dos líneas cuya finalidad es emular el servicio suplementario de conferencia tripartita y el fraudulento tenga mayor facilidad en la reventa de llamadas. En el GRAFICO se puede apreciar en forma ilustrativa



2.3.1.3 FRAUDE POR LLAMADAS LIBRE FACTURACION

Este fraude se genera por la manipulación del teléfono público con la finalidad de provocar un corto circuito en el aparato provocando errores en sus componentes electrónicos internos y por ende el descontrol del equipo en la administración de llamadas.

Frente a este problema el negocio a tomado medidas de carácter técnico y mecánico para la protección del equipo, esto también ha sido complementado con operativos y capturas de inescrupulosos que finalmente son liberados.

2.3.1.4 FRAUDE POR TARJETAS RECICLADAS

Esta modalidad de fraude consiste en adulterar las tarjetas prepago inteligentes a través de la reprogramación o cambio del chip con ayuda de herramientas electrónicas.

Se tiene conocimiento por las capturas de realizadas a los comercializadores de estas tarjetas que se fabrican en la actualidad fuera del Perú.

2.3.1.5 FRAUDE POR CALL BACK

Este tipo de fraude aprovecha la diferencia de tarifas telefónicas de los países, las empresas dedicadas al Call Back instalan su centro de operaciones por lo general en los países que tienen la menor tarifa (EE.UU. Reino Unido, etc.)

ofreciendo a los clientes de todo el mundo un tono de marcado local, o permitiéndoles llamar a cualquier destino a tarifas reducidas que varían entre un 20 y un 80 por ciento de la tarifa original.

Las llamadas de Call Back son ampliamente distribuidas por revendedores e incluso por transportadores internacionales, para usuarios de red fija y celular.

En la actualidad no todos los países considera a la mayoría de las técnicas de Call Back como actividad fraudulenta, sino como al uso de facilidades de tráfico internacional, en particular, si no afectan la calidad de servicio de la red.

2.3.2 FRAUDE EN LA RED CELULAR

Existe una mayor variedad de formas de realizar algún delito en éste negocio, debido a no sólo la cantidad de servicios que se dan, sino también a la alta cotización de los equipos celulares y su independencia a la línea que en él se puede programar.

A continuación se detallan los fraudes más relevantes que se han podido detectar hasta el momento en éste servicio:

2.3.2.1 FRAUDE POR SUSCRIPCIÓN

En ese tipo de fraude el fraudador adquiere la línea telefónica con la intención de no pagar la cuenta telefónica, luego el uso anormal ocurre dentro del periodo activo de la línea telefónica.

Generalmente la línea telefónica es usada para vender llamadas o para el uso usufructo propio del fraudador.

En nuestro medio el Fraude por suscripción consiste en la obtención de líneas telefónicas con la utilización de documentación falsa o mediante la suplantación de personas con documentación verdadera sin conocimiento del titular

En ésta modalidad las pérdidas NO solo resultan del tráfico telefónico cursado y que hemos llegado a controlar, sino al costo del equipo que en más del 70%, la Empresa subvenciona.

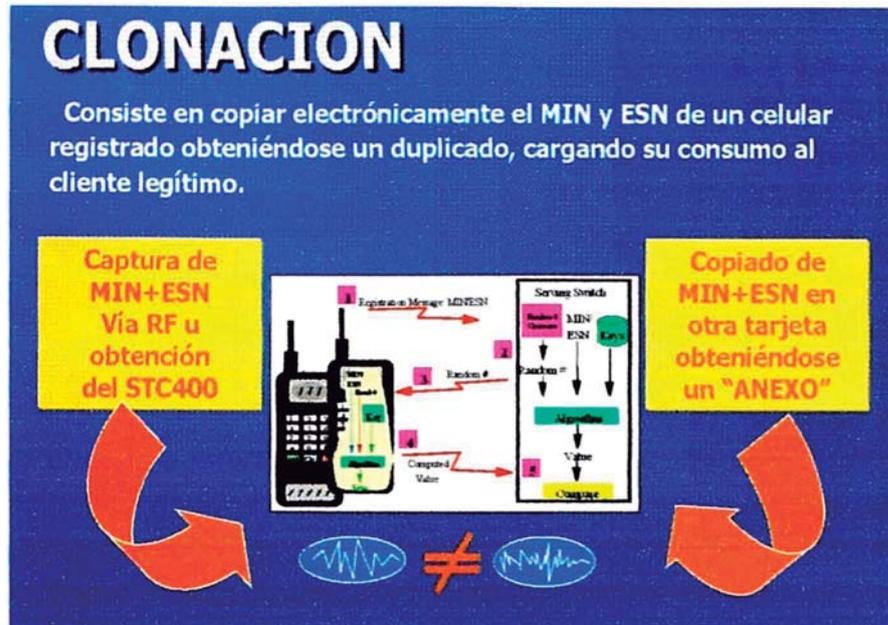
Hay que resaltar que la tecnología que soporta nuestra moderna red digital hace que nuestros equipos se cotizan hasta por un valor que supera al doble que el de nuestra competencia

2.3.2.2 FRAUDE TIPO CLONING

Esta modalidad, que consiste en abastecerse de los códigos electrónicos del equipo que posee determinada línea celular, ha desplegado toda una evolución de ingeniería que consiste en copiarlos en otro aparato y desde allí cursar tráfico que posteriormente será facturada al cliente legítimo de la línea (titular).

Los Servicio de Roaming y de Larga Distancia Internacional son los productos más codiciados para ésta modalidad de

fraude, y a la vez los que mayor efecto negativo causan a las empresas de telefonía celular.



Esquema de la Clonación

2.4 GESTION DE FRAUDE

Es el proceso de analizar, tomar decisiones, planificar, ejecutar, coordinar y controlar las actividades de la empresa para minimizar las perdidas económicas y de imagen a la empresa

Debe incluir a toda la organización, así como a proveedores y distribuidores

El fraude afecta a toda operadora de tele comunicaciones y proveedor de servicios; ya sean aquellas que ya están establecidas o aquellas que recién están entrando al mercado. El fraude reduce el lucro, afecta a los buenos clientes y dificulta la eficiencia operacional. Los costos reales de fraude pueden ser muy superiores a los ingresos

perdidos; como por ejemplo: el desvío de recursos, inversiones desnecesarias en la red, pérdidas de clientes. El impacto real raramente es cuantificado, lo que reduce la visibilidad de la eficiencia de medidas y acciones.

Para que se tenga el control del fraude es necesario un plan. Las mejores estrategias comienzan con la comprensión de los riesgos; cómo el fraude puede ser perpetrado y el impacto subsiguiente. Como cada operación difiere de los demás, todas poseen sus riesgos individuales. Para que se tenga un cuadro completo de los riesgos de fraude es necesaria que las amenazas y vulnerabilidades de la empresa sean especificadas. Pero todavía no es lo suficiente. Necesitamos también cuantificar el potencial de impactos en términos financieros directos e indirectos. De esta forma podemos construir una estrategia gerencial eficiente.

La gestión de fraude engloba los siguientes puntos

2.4.1 EVALUACION DE RIESGO Y ANALISIS (comprensión del problema)

La comprensión es el pilar fundamental de una administración exitosa. Desde una evaluación de riesgos más amplia hasta revisiones y análisis más minuciosos ayudaran en el direccionamiento del desarrollo de estrategias.

2.4.2 DEFINICION DE ESTRATEGIAS

La definición de estrategias es un factor primordial para la implantación exitosa de controles administrativos, construyendo a partir del análisis de riesgos para que se pueda determinar cómo, dónde y cuándo los controles deben ser aplicados.

2.4.3 DESENVOLVIMIENTO ORGANIZACIONAL

La responsabilidad y el dominio de la administración de fraude deben ser definidos: revisión organizacional, planificación de la estructura del equipo y programas de concientización. Las habilidades para administrar fraudes y la concientización deben también ser propagadas por toda la empresa.

2.4.4 ESPECIFICACION Y PLANEAMIENTO DE CONTRA MEDIDAS

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

2.4.5 IMPLEMENTACION DE CONTROLES

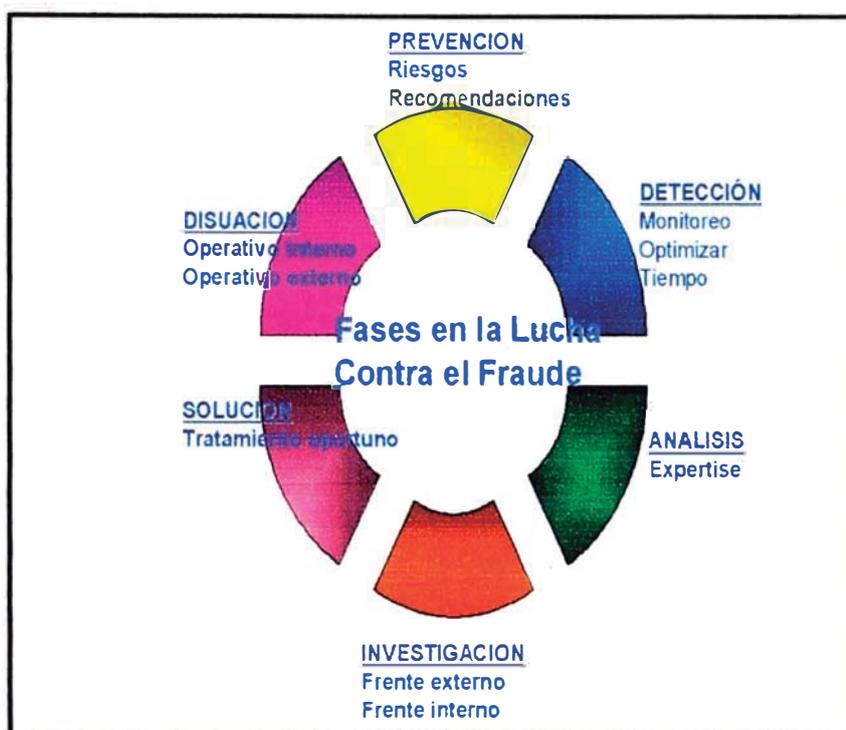
Hasta los controles mas apropiados pueden tornarse ineficientes debido a una implementación débil. El desarrollo de procedimientos de apoyo la garantía de una integración apropiada

con toda la empresa son elementos fundamentales para la implementación de cada control.

2.4.6 DEFINICION DE MECANISMOS DE MEDICION E INFORMES

La visibilidad continua será guiada por mecanismos eficaces de clasificación, medición e informes, ayudando en el entendimiento y facilitando la administración.

2.5 FASES DE LA GESTION DEL FRAUDE



Fases de la Gestión del Fraude

2.5.1 PREVENCIÓN

Fase de preparación y disposición de medidas y recomendaciones para evitar un riesgo de fraude en

telecomunicaciones, es la primera y última etapa del ciclo de la gestión del fraude.

2.5.2 DETECCION

Es la fase donde se localizan las alertas mediante los sistemas antifraude y comerciales es la etapa de la monitoreo de alertas. Es la etapa técnica de todo el ciclo de gestión del fraude.

2.5.3 ANALISIS E INVESTIGACION

Es la fase donde se realiza el estudio minucioso de la data proveniente de la etapa de detección es la etapa conocida como Caja Negra (Expertise), así como el estudio profundo de los frentes externos e internos.

2.5.4 SOLUCION Y DISUACION

Es la fase donde se realiza el tratamiento oportuno a los casos de fraude, es la etapa donde se realiza las coordinaciones y tratamientos de gestión con todas las áreas involucradas (afectadas) en el proceso. Así como operativos para inducir a desistir las acciones fraudulentas.

2.6 REDISEÑO DE PROCESOS

La experiencia indica que es posible mejorar la rentabilidad de las empresas si la gerencia logra una comprensión clara y profunda de los procesos de su propio negocio y del comportamiento de los costos.

Los procesos están compuestos por personas, todo rediseño de procesos conlleva un rediseño de hábitos, actitudes y valores culturales. Posicionar visualmente los colectivos de personas segmentados “Ad-Hoc” de una organización para conocer su situación respecto a un tema preciso.

2.6.1 EJES DE ACTUACION

Los ejes o pilares del rediseño de procesos son:

- Reducción de Costes
- Reducción de tiempos de tramitación
- Mejora en la calidad del servicio
- Creación de ventajas competitivas

2.6.2 PREGUNTAS FRECUENTES

- ¿Dónde añadimos valor?
- ¿Por qué hacemos las cosas que hacemos (y de ese modo)?
- ¿Satisfacemos realmente a nuestros clientes?
- ¿Obtenemos lo mejor de nuestra gente?
- ¿Cómo trabajan nuestros competidores?
- ¿Cómo está cambiando el mercado?
- ¿En qué tiempo tenemos que (y el riesgo de no hacerlo) responder?

- Si tenemos que cambiar, ¿por dónde empezamos? ¿cuan lejos?
- ¿cuan rápido?

2.6.3 HERRAMIENTAS UTILIZADAS

El equipo de mejora de procesos se enfoca en el refinamiento del proceso actual. Después de tener el modelo del proceso actual de aplican las siguientes herramientas bajo el principio de Eliminación de la Burocracia que toma la Organización.

2.6.3.1 ANALISIS DEL VALOR AGREGADO

El análisis de valor agregado tiene por objeto evaluar los componentes (o etapas) de un proceso, para encontrar formas más económicas y/o de una mayor calidad para desarrollarlo.

El objetivo del análisis de valor agregado es hacer una revisión de un proceso en función de la búsqueda de una mayor efectividad y generar a nuestro producto o servicio un plus de diferenciación.

Eliminar todas las actividades que no generan valor al proceso productivo o de servicios.

2.6.3.2 ELIMINACION DE LA DUPLICACION

Eliminar actividades que se duplican en diferentes etapas del proceso. Muchas de estas actividades son actividades de redundancia.

La redundancia es la repetición de operaciones con fines de control o seguridad. Existe en los procesos la natural tendencia a producir redundancias en la medida que los riesgos implícitos en los procesos son altos o haya disputa por la "propiedad" del éxito en los mismos.

La dificultad para determinar la redundancia reside en que la misma muchas veces no es evidente, ya que se hace adoptando diferentes nombres o características.

2.6.3.3 SIMPLIFICACION DE LOS METODOS

Simplificar los métodos de trabajo, En ella se busca la combinación de varios trabajos o tareas en una sola, nos permite una reducción de tiempos. Se busca la reducción de los controles y las verificaciones al mínimo indispensable y que éstos sean ejecutados, en la medida de lo posible, por el propio trabajador.

2.6.3.4 REDUCCION DE LOS TIEMPOS DE CICLO DEL PROCESO

Eliminar los famosos cuellos de botella eliminación de retrasos y retrasos sistemáticos. Reducción de los tiempos del ciclo y en los plazos de respuesta. De tal forma se logran menores tiempos para el desarrollo del servicio. De igual forma son más rápidas las respuestas a los requerimientos de los clientes, disponiendo de mayores niveles de flexibilidad. Se deben

diseñar los procesos de manera para reducir estos retrasos lo mas posible, considerando la cultura organizacional y los perfiles del personal para que el cambio organizacional no sea tan drástico.

2.6.3.5 ELIMINACION DE ERRORES

Mejorar la calidad del producto final implica eliminar los errores en todo el ciclo productivo. La "calidad", según definición, es el conjunto de propiedades y características de un producto o servicio que le confieren su aptitud para satisfacer las necesidades y expectativas de los clientes. Le eliminación de los errores se logra al normalizar los procesos (ver anexo) y estar bajo control y al examinar todas las causas de no conformidad y las reclamaciones de los clientes.

Uno de los resultados más significativos de ser eficiente en los procesos y reducir la espera, es la subsecuente reducción de errores

2.6.3.6 RE- ESTRUCTURACION ORGANIZACIONAL

La Implementación de un programa de reestructuración organizacional que permita mayor eficiencia y facilite la prestación de servicios a los usuarios. La reestructuración nos va permitir emplear de manera eficiente los recursos de la organización para atender las necesidades de nuestro cliente.

2.6.3.7 ESTANDARIZACIÓN

Ello implica la búsqueda de la mejor forma de realizar una tarea o proceso y su correspondiente documentación a los efectos de darle continuidad y permitir su medición y su mejora continua.

2.6.3.8 LOGRAR ASOCIACION DE PROVEEDORES

Una organización y sus proveedores son interdependientes y una relación mutuamente beneficiosa aumenta la capacidad de ambos

Para crear valor útil para los clientes de la Organización. Se deben buscar alianzas con los proveedores.

2.6.3.9 AUTOMATIZAR Y USO DE TECNOLOGIA DE INFORMACION

En este mundo globalizado y de constantes cambios, las empresas obligadamente requieren ser cada vez más ágiles y se deben adaptar con mayor facilidad a estos cambios. Actualmente, las compañías dependen en su totalidad de tener la información exacta en el momento preciso, las empresas que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnología que permitan tener la información requerida y lista para ser utilizada.

2.6.4 EQUIPOS DE TRABAJO

El equipo de trabajo esta dividido en tres grandes grupos:

2.6.4.1 CONSEJO SUPERIOR (Comité de Dirección, Comisión ejecutiva)

- Delimita el marco de trabajo y las orientaciones estratégicas
- Controla y orienta el proyecto
- Valida los resultados de cada etapa y toma decisiones sobre la base de recomendaciones
- Sigue el avance de la implantación y realiza arbitrajes si es necesario.

2.6.4.2 UNIDADES INVOLUCRADAS

Recursos involucrados en el proceso de análisis.

- Proveen elementos para los análisis
- Participan en los análisis y los validan
- Se apropian de las propuestas y se comprometen en la implantación.

2.6.4.3 EQUIPO DE PROYECTO

- Elabora el plan de trabajo
- Pilota y/o participa en los análisis
- Elabora las propuestas y el plan de implantación
- Formaliza cada etapa, comunica y valida los avances.

CAPITULO III

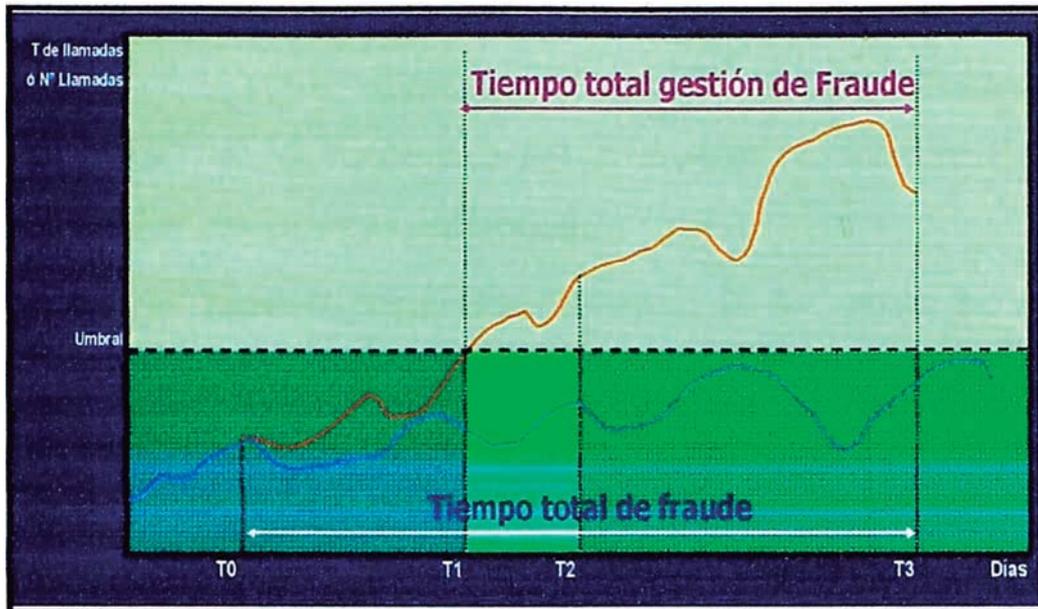
PROCESO DE TOMA DE DECISIONES

3.1 PLANTEAMIENTO DEL PROBLEMA

El propósito del trabajo de investigación es implementar medidas de solución para reducir las pérdidas económicas al Grupo Telefónica por el concepto de fraude en telecomunicaciones. Dichas pérdidas se ven incrementadas en forma directamente proporcional con el tiempo de vida del fraude.

Podemos plantear como problema el **“TIEMPO TOTAL DE FRAUDE”** lo que se tiene que buscar es reducir dicho tiempo con diferentes medidas o alternativas de solución. En la gráfica adjunta se puede apreciar en forma clara la definición del problema.

La gráfica nos muestra dos evoluciones de llamadas, la línea de color azul es el tráfico generado por un cliente normal, la línea de color rojo es el tráfico fraudulento.



Grafica: Tiempo X Umbral (CDR's)

- **Umbral:** Es el límite establecido de tráfico por grupo de clientes (perfiles de consumo). Los tráficos que sobrepasan el umbral son posibles alertas de casos de alta probabilidad de fraude que tienen que ser analizados (Etapas de análisis)
- **T0:** Tiempo de Inicio de la primera llamada fraudulenta
- **T1:** Tiempo donde las llamadas fraudulentas sobrepasan el umbral establecido para los casos de fraude
- **T2:** Tiempo que se detecta el caso de alta probabilidad de fraude
- **T3:** Tiempo de termino de las llamadas fraudulentas

Podemos dividir todo el Tiempo total de fraude en tres grandes zonas:

- **Zona de fraude bajo sombra:** (tiempo que se definió en el proceso de análisis y ejecución del Proyecto) Es el tiempo donde el tráfico fraudulento no sobrepasa el umbral establecido. (Rango T1:T0)
- **Zona de Detección:** (tiempo que se definió en el proceso de análisis y ejecución del Proyecto) Es el tiempo donde el analista de fraude detecta el caso de fraude. (Rango T2:T1)
- **Zona de Reacción:** (tiempo que se definió en el proceso de análisis ejecución del Proyecto) Es el tiempo de demora después de ser detectado hasta el último tráfico fraudulento. (Rango T2:T3)

3.2 ALTERNATIVAS DE SOLUCION

Con el fin de reducir el tiempo total de fraude y por consecuencia reducir las pérdidas económicas al grupo Telefónica, las posibles alternativas de solución las podemos clasificar en tres grupos.

- Rediseño de Procesos
- Redefinición de Umbrales
- Up-grade del sistema antifraude

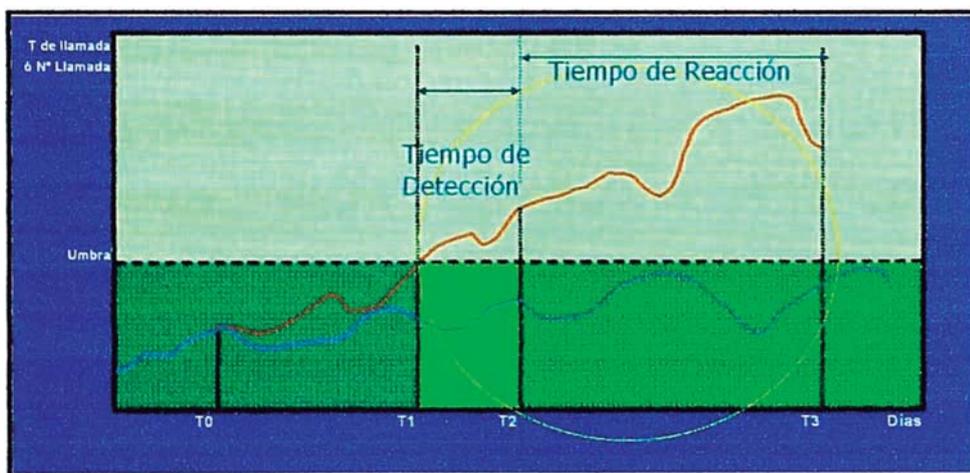
Considerando las tres alternativas se ha decidido enfocar la solución en la primera alternativa, esta nos va a permitir reducir el tiempo de ciclo de gestión del fraude específicamente

en dos de la grandes zonas encontradas en la definición de nuestro problema (Zonas de reacción y detección).

Las tres alternativas como se puede ver más adelante son independientes, se pueden aplicar las tres alternativas indistintamente pero la actual coyuntura de la empresa nos limita por el momento a aplicar la primera alternativa. A continuación se detallan en forma mas especifica las tres alternativas.

3.2.1 REDISEÑO DE LOS PROCESOS

Esta alternativa nos va permitir reducir los tiempos de la zona de reacción y zona de detección. La solución plantea un rediseño del proceso de gestión del fraude que involucra a los diferentes negocios del grupo y su interacción con sus diversas áreas.



Gráfica: Tiempo X Umbral (CDR's)

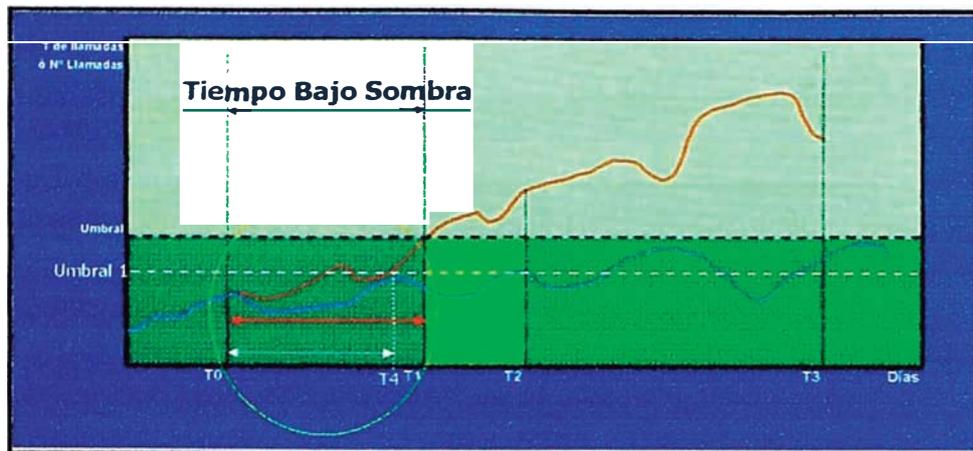
Como podemos apreciar en la figura la zona de reacción es la zona donde se produce la mayor concentración de tiempo. En esta zona se eliminará la burocracia, se eliminará la duplicación de los trabajos, vamos a reducir los tiempos mediante la fusión y

un reordenamiento de las actividades, se creará una cultura orientada a las consecuencias que genera el fraude en toda la cadena productiva de la empresa y con la ayuda de la tecnología de la información, centralizar toda la información en un aplicativo e- business que lo llamaremos **Sistema Centralizado de Casos de Fraude (SICECAF)**, que nos va reducir considerablemente los tiempos.

En la zona de detección los que se va buscar es simplificar los métodos de detección con la creación de estándares para las diferentes topologías de fraude así eliminar nuestros defectos y con la ayuda del **SICECAF** mejora la calidad de la información que se entrega y reducir los tiempos de detección.

3.2.2 REDEFINICION DE UMBRALES

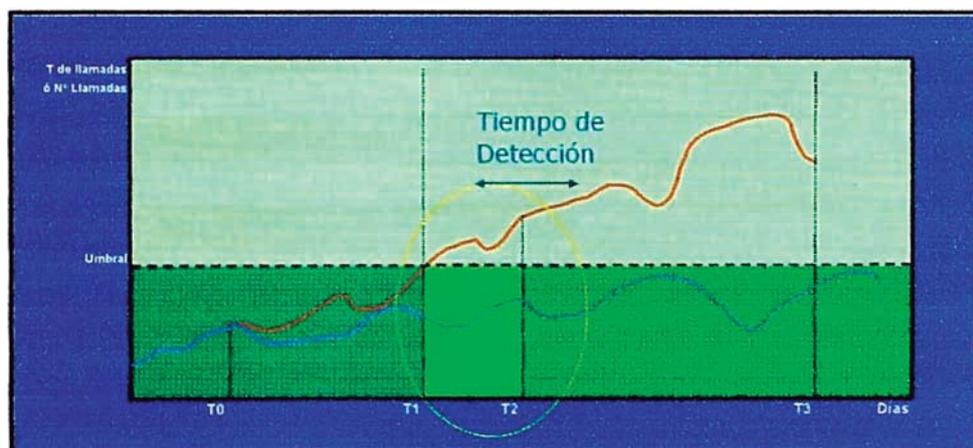
Esta alternativa de solución se concentra en la zona de Fraude Bajo Sombra, sugiere una reducción en los umbrales establecidos, va generar un aumento de CDR's para su análisis, lo que involucra un aumento de personal (estudio realizado). Por la coyuntura actual de la empresa esta alternativa no era aceptada, pero como podemos ver en la grafica), el tiempo de reducción no es muy significativo.



Gráfica: Tiempo X Umbral (CDR's)

3.2.3 UPGRADE DEL SISTEMA ANTIFRAUDE

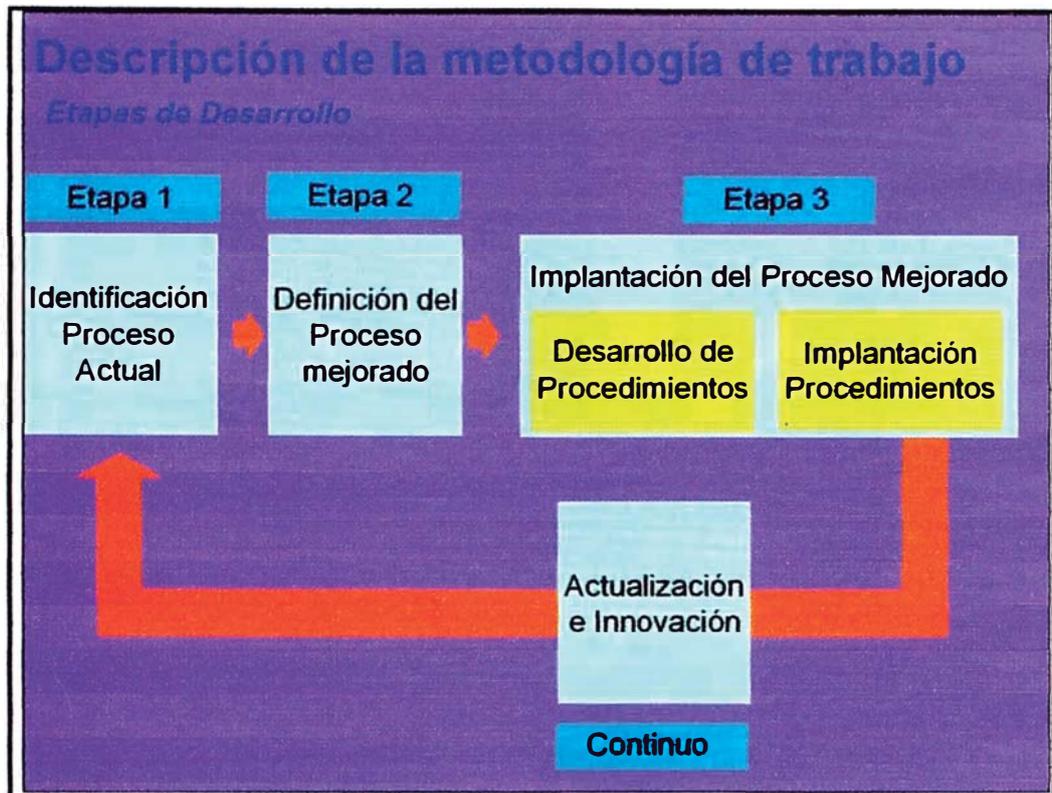
Esta alternativa de solución se concentra en la zona de detección de Fraude, se sugiere una mejora del sistema actual antifraude, con un perfilador de casos lo que nos va generar un aumento de CDR's para su análisis, lo que involucra un aumento de personal (estudio realizado). Por la coyuntura actual de la empresa esta alternativa no era aceptada por el momento.



Gráfica: Tiempo X Umbral (CDR's)

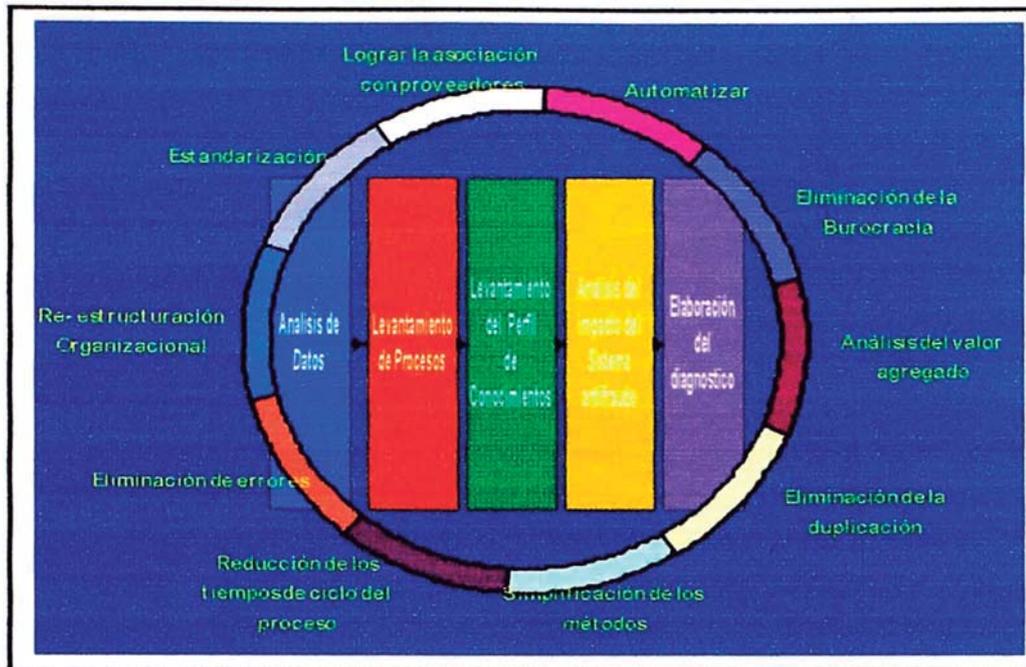
3.3 METODOLOGIA DE SOLUCION

El presente trabajo se llevo a cabo bajo el siguiente esquema:



En la etapa 1 se utilizará la Metodología de Diagnostico de Procesos,

- Análisis de Datos
- Levantamiento de Procesos
- Levantamiento del Perfil de Conocimientos
- Análisis del sistema antifraude
- Elaboración del diagnostico



En la etapa 2 se utilizarán las herramientas del rediseño de procesos para la toma de decisiones, la implementación y la evaluación de resultados que se encuentran en los puntos 3.4, 3.5, y 4 respectivamente.

3.3.1 ANALISIS DE DATOS

Es la primera etapa de la metodología de solución es esta etapa se recoge toda la información que se muestra a continuación.

3.3.1.1 DATOS HISTORICOS

Los datos presentados en esta etapa es la información escrita que se cuenta para nuestro análisis en esta etapa se analizaron los siguientes datos, toda la data histórica corresponde a los años 1997 e inicios del 2002.

- **Casos Reportados 1997-2002:** Para los presentes años los tipos de fraude que se reportaban eran los casos de suscripción en la Red Fija y la Red Móvil, casos de Hurtos de Línea, e los casos de clonación. Como se puede apreciar en lo cuadros adjuntos:

BASICA	Tipo de Fraude	Nº Casos	Monto Detectado (\$)
Año 1997	Suscripción	91	1109700
	Hurto de Línea	62	1071360
Año 1998	Suscripción	114	1470800
	Hurto de Línea	224	1458240
Año 1999	Suscripción	86	989526
	Hurto de Línea	216	927520

MOVILES	Tipo de Fraude	Nº Casos	Monto Detectado (\$)
Año 1997	Suscripción	421	370179
	Cloning	20	143000
Año 1998	Suscripción	320	320458
	Cloning	234	713700
Año 1999	Suscripción	92	93131,675
	Cloning	580	594500

Situación del fraude

También se encontraron casos de fraude interno y casos de inconsistencias técnicas que no se mencionan en el siguiente trabajo.

- **Procedimiento de Cortes por deuda:** Es de mucha importancia conocer como era el proceso de gestión de corte para los casos de deuda en la parte de tiempos así nos damos una idea de cuanto tiempo el fraudulento

podía vivir en una línea convencional como se puede apreciar a continuación.

Red Básica:



Gráfico: corte por deuda Básica

Red Móvil



Gráfico: corte por deuda Movil

- CDR's para el análisis de datos
- **Casos de altos consumos – facturación:** Eran casos de altos consumos que nos reportaban mensualmente. La mayoría de los casos terminaban en casos de suscripción.
- **Zonas de riesgo:** Las zonas de riesgo eran las zonas de la ciudad de Lima donde se encontraban la mayor cantidad de casos de fraude.

- **Destinos de Riesgo:** Números internacionales de mayor tráfico reportados por cada caso de fraude.
- **Números de riesgo:** Tabla donde se encontraban números llamados de cabecera, estos números se presentaban frecuentemente en los casos de fraude.

3.3.1.2 INDICADORES DE GESTION

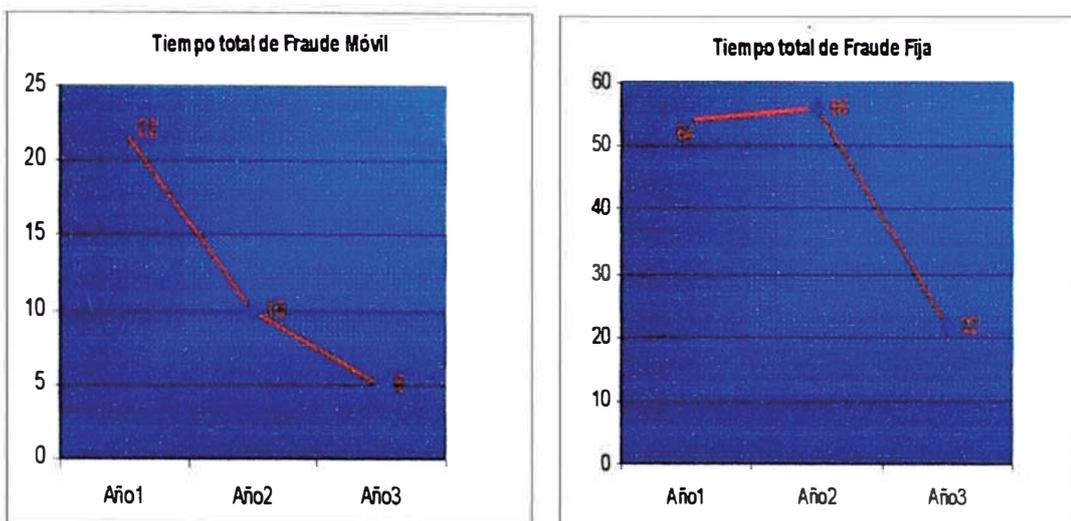
Los indicadores de gestión son claves para el pilotaje de los procesos que se manejaban para el control y análisis de la gestión, los únicos indicadores que manejábamos eran el tiempo total de fraude y el Monto total de pérdida generada por el caso de fraude:

- **Tiempo Total de Fraude:** Es el tiempo total desde la primera llamada fraudulenta hasta la última llamada. Esta información se obtenía de los casos cerrados por fraude.
- **Monto Detectado:** Es el monto total en dólares desde la primera llamada hasta la última llamada fraudulenta.

Como podemos ver en el cuadro siguiente las gestiones de fraude se encontraban con altos tiempos, el control se llevaba por el total de casos reportados. Hay que indicar que para la detección no existía una estandarización de información para los diferentes tipos de fraude, los casos reportados eran a criterio del analista.

Basica	Nº Casos	Monto Detectado (S/)	Tiempo Total de Fraude
Año 1997	153	2 181 060	54
Año 1998	338	2 929 040	56
Año 1999	302	1 917 046	22

Móvil	Nº Casos	Monto Detectado (\$)	Tiempo Total de Fraude
Año 1997	441	513 179	22
Año 1998	554	1 034 158	10
Año 1999	672	687 632	5



Grafica: Evolución Tiempos de fraude

3.3.1.3 INTERACCION ENTRE LAS DIVERSAS AREAS

En todo el proceso de gestión de fraude se interactúa con diversas áreas de los negocios, para el caso de fraude en Telefonía Móvil se interactúa con el negocio de Telefónica Móviles, par el caso de los casos de fraude en la red fija se interactúa con la Operadora de Telefonía Fija (OTF).

A continuación describiremos en forma breve las interacciones que se dan con cada negocio así como la forma de comunicación que existe.

3.3.1.3.1 CONTROL DE FRAUDE EN LA RED MOVIL

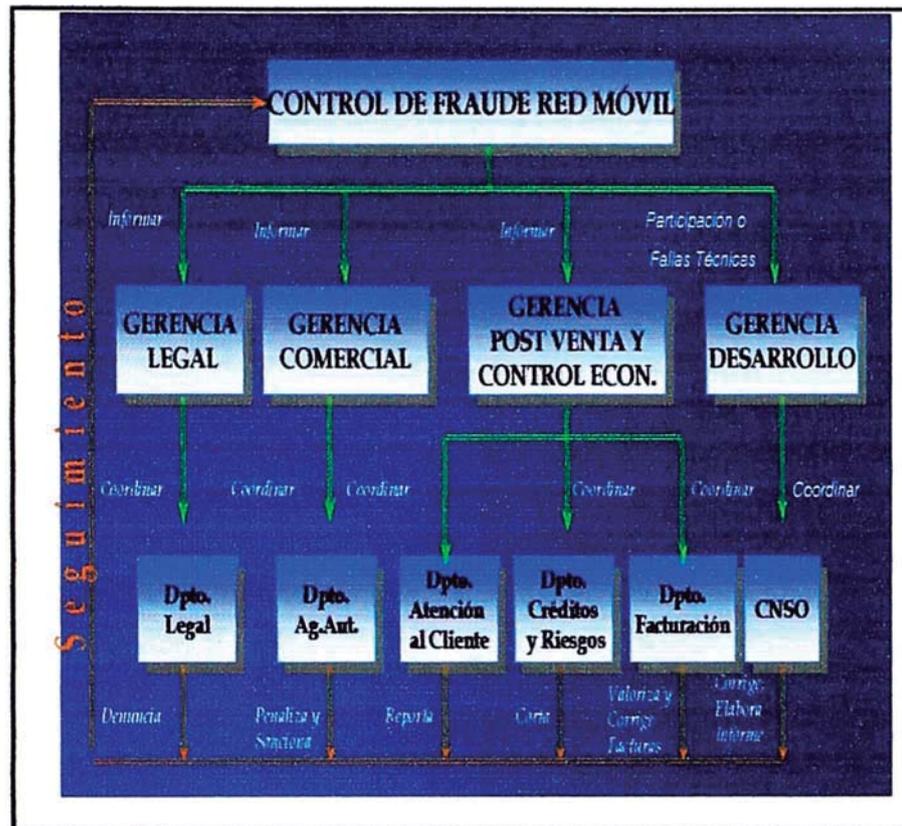


Gráfico: Interacción red Fija

- **Gerencia Legal:** Se informan los casos para su seguimiento respectivo, la información se realiza vía mail. Se realiza la información por Documento Gerencial cuando existe un grupo de casos con el mismo perfil o

en los casos donde se van a realizar operativos con ayuda de personal externo.

- **Gerencia Post Venta y Control Económicos:** se informa vía mail para el tratamiento con el cliente, depuración y/o ajuste de facturas, en el mail se indica los periodos afectados. Existe una retroalimentación con la dicha Gerencia con los casos de reclamos. Los casos de reclamos por consumo elevado en algunos casos son derivados a la Sub. Gerencia de Control de Fraude vía mail o Documento Gerencial dependiendo del monto reportado por reclamo.
- **Gerencia Comercial:** Se informa los casos Detectados para su tratamiento así como para la coordinación de envío de documentación para sustentar la venta de equipos involucrados en fraude. La vía de coordinación es por Documento Gerencial.
- **Gerencia de Desarrollo:** se informa en forma general para solicitar información almacenada de tráfico para el análisis, así como la coordinación por fallas técnicas detectadas en la fase de análisis de los casos de fraude.

3.3.1.3.2 CONTROL DE FRAUDE EN LA RED FIJA



Gráfico: Interacción red Fija

- **Sub. Gerencia Legal:** Se informan los casos para su seguimiento respectivo, la información se realiza vía e-mail. Se realiza la información por Documento Gerencial cuando existe un grupo de casos con el mismo perfil o en los casos donde se van a realizar operativos con ayuda de personal externo.
- **Gerencia Tups:** Se informan los casos de fraude que afectan los teléfonos públicos, estos pueden ser Públicos Internos y Públicos externos. La información se realiza vía e-mail. Se realiza la información por Documento Gerencial cuando existe un grupo de casos

con el mismo perfil o en los casos donde se van a realizar operativos con ayuda de personal externo.

- **Gerencia Local:** Se informan los casos de fraude que afectan los teléfonos residenciales en sus diversos segmentos como medio, VIP, Bajo, alto, no segmentado en el caso de rurales y Tops, La información se realiza vía e-mail. Se realiza la información por Documento Gerencial cuando existe un grupo de casos con el mismo perfil o en los casos donde se van a realizar operativos con ayuda de personal externo.
- **Gerencia de Comunicaciones de Empresa:** Se informan los casos de fraude que afectan los teléfonos de Compañías en sus diversos segmentos como Grandes Clientes, Clientes Medianos, Clientes pequeños, Pymes y Tops. La información se realiza vía e-mail. Se realiza la información por Documento Gerencial cuando existe un grupo de casos con el mismo perfil o en los casos donde se van a realizar operativos con ayuda de personal externo.
- **Gerencia de Larga Distancia:** Se informan los casos de fraude que afectan el trafico Internacional, para el pago de interconexión internacional. La información se realiza vía e-mail. Se realiza la información por Documento

Gerencial cuando existe un grupo de casos con el mismo perfil o en los casos donde se van a realizar operativos con ayuda de personal externo.

3.3.2 LEVANTAMIENTO DE PROCESOS

El levantamiento de procesos o identificación del proceso actual fue la etapa más importante para nuestro rediseño de proceso de gestión del fraude, a continuación describiremos el proceso macro.

3.3.2.1 Detectar: Sub. Proceso que coincide con una de las fases de la gestión de fraude. La función principal de este sub. proceso es determinar los posibles casos de fraude a analizar.

- **Entrada:** CDR's
- **Salida:** Alertas de Posible Fraude
- **Variables:** Umbrales de detección- No existe un estándar para los diferentes tipos de fraude
- **Unidades Involucradas:** Control de fraude y Sistemas de Información
- **Documentos:** Archivos de texto

3.3.2.2 Analizar: Sub. proceso que coincide con una de las fases de la gestión del fraude. Este sub. proceso lo denominamos caja negra es donde se analizan las alertas de posible fraude cuyo resultado nos presenta los casos con alta probabilidad de fraude y fraude

- **Entrada:** Alertas de Posible Fraude
- **Salida:** Casos de Fraude y Casos de alta probabilidad de Fraude
- **Variables:** Por motivos de confidencialidad de la Información de la empresa no podemos mencionar las variables que se presentan en el sub. Proceso.
- **Unidades Involucradas:** Control de fraude
- **Documentos:** Archivos de texto, Archivos xls, correos electrónicos.

3.3.2.3 Condición de alta probabilidad de fraude:

Donde se toma la decisión si el caso es de alta probabilidad de fraude o no es fraude. Si el caso es de NO fraude se desecha el caso. En el caso que se detecta alta probabilidad de fraude pasa al proceso de control de supervisión.

3.3.2.4 Control de supervisión: Sub. proceso de almacenamiento de casos para el control y distribución para la continuidad de la gestión dependiendo del tipo de fraude.

- **Entrada:** Alertas de alta probabilidad de fraude
- **Salida:** Casos de Fraude

- **VARIABLES:** Tipos de fraude, segmento de negocios afectados, tipos de líneas afectadas, umbrales establecidos, variables utilizadas en el sub. Proceso de investigación.
- **UNIDADES INVOLUCRADAS:** Control de fraude, Negocios afectados por el fraude y Facturación.
- **DOCUMENTOS:** Archivos de texto, Archivos xls, correos electrónicos, Documentos de Gerencia, contratos de servicios y otros.

3.3.2.5 Condición de fraude: Donde se toma la decisión

si el caso es de Fraude o de alta probabilidad de fraude. Si el caso es fraude se envía el caso a los negocios afectados por su control respectivo, se realiza vía e-mail o documento de Gerencia dependiendo la trascendencia del caso, también se informa a la Gerencia de facturación para realizar el ajuste o depuración al caso detectado. En el caso que se detecta alta probabilidad de fraude pasa al sub. proceso enviar caso.

3.3.2.6 Enviar caso: Los casos de alta probabilidad de

fraude se agrupan por su grado de criticidad por su distribución al área de servicios comerciales para su tratamiento comercial o al área de OMRS para su tratamiento técnico.

- **Entrada:** Casos de alta probabilidad de fraude
- **Salida:** Casos de Fraude Críticos
- **Variables: Tipos de fraude,** segmento de negocios afectados, tipos de líneas afectadas, umbrales establecidos, variables utilizadas en el sub. Proceso de investigación.
- **Unidades Involucradas:** Control de fraude, Gerencia de Servicios Comerciales, OMRS y Negocios afectados por el fraude.
- **Documentos:** Archivos de texto, Archivos xls, correos electrónicos, Documentos de Gerencia.

3.3.2.7 Condición Crítica de fraude: Donde se toma la decisión cual va ser el proceso para el caso de fraude. Si el caso de alta probabilidad de fraude tiene una condición crítica alta se envía el caso a la revisión Técnica, se realiza vía e-mail o documento de Gerencia dependiendo la trascendencia del caso. Si el caso de alta probabilidad de fraude tiene una condición crítica baja se envía a la gerencia de Servicios Comerciales para su tratamiento.

3.3.2.8 Revisión y Seguimiento: es un sub. proceso que pertenece a los negocios afectados, es de conocimiento para el seguimiento del negocio a la Gerencia de Servicios

Comerciales. Esto se debe a que ellos son dueños del servicio afectado.

3.3.2.9 Tratamiento Comercial: Es un sub. proceso que pertenece a la a la Gerencia de Servicios Comerciales. Es donde se realiza las gestiones directamente con el cliente. Ven los reclamos en línea, etc. Si el cliente no acepta sus consumos estos casos son enviados a tratamiento Técnico respectivo. Dicho sub. proceso no pertenece a la Sub. Gerencia de Control de Fraude pero genera en nuestro proceso de gestión de fraude gran cantidad de tiempo. No lo describimos detalladamente por falta de permisos pero en el punto de toma de decisiones y estrategias adoptadas indicamos las medidas adoptadas.

3.3.2.10 Revisión Técnica: Es un sub. proceso que pertenece a la a la Gerencia de Soporte Técnico- planta externa. Es donde se realiza los seguimientos de líneas y/o tratamientos técnicos de detecciones de fallas o vulnerabilidades en su planta. Dicho sub. proceso no pertenece a la Sub. Gerencia de Control de Fraude pero genera en nuestro proceso de gestión de fraude gran cantidad de tiempo. No lo describimos detalladamente por falta de permisos pero en el punto de toma de decisiones y estrategias adoptadas indicamos las medidas adoptadas.

3.3.2.11 Revisión de resultado: Es un sub. proceso que pertenece a la a la Gerencia de Soporte Comercial. Analizan los resultados de las inspecciones técnicas y lo remiten al área de control de Fraude y a los negocios respectivos. Dicho sub. proceso no pertenece a la Sub. Gerencia de Control de Fraude pero genera en nuestro proceso de gestión de fraude gran cantidad de tiempo. No lo describimos detalladamente por falta de permisos pero en el punto de toma de decisiones y estrategias adoptadas indicamos las medidas adoptadas.

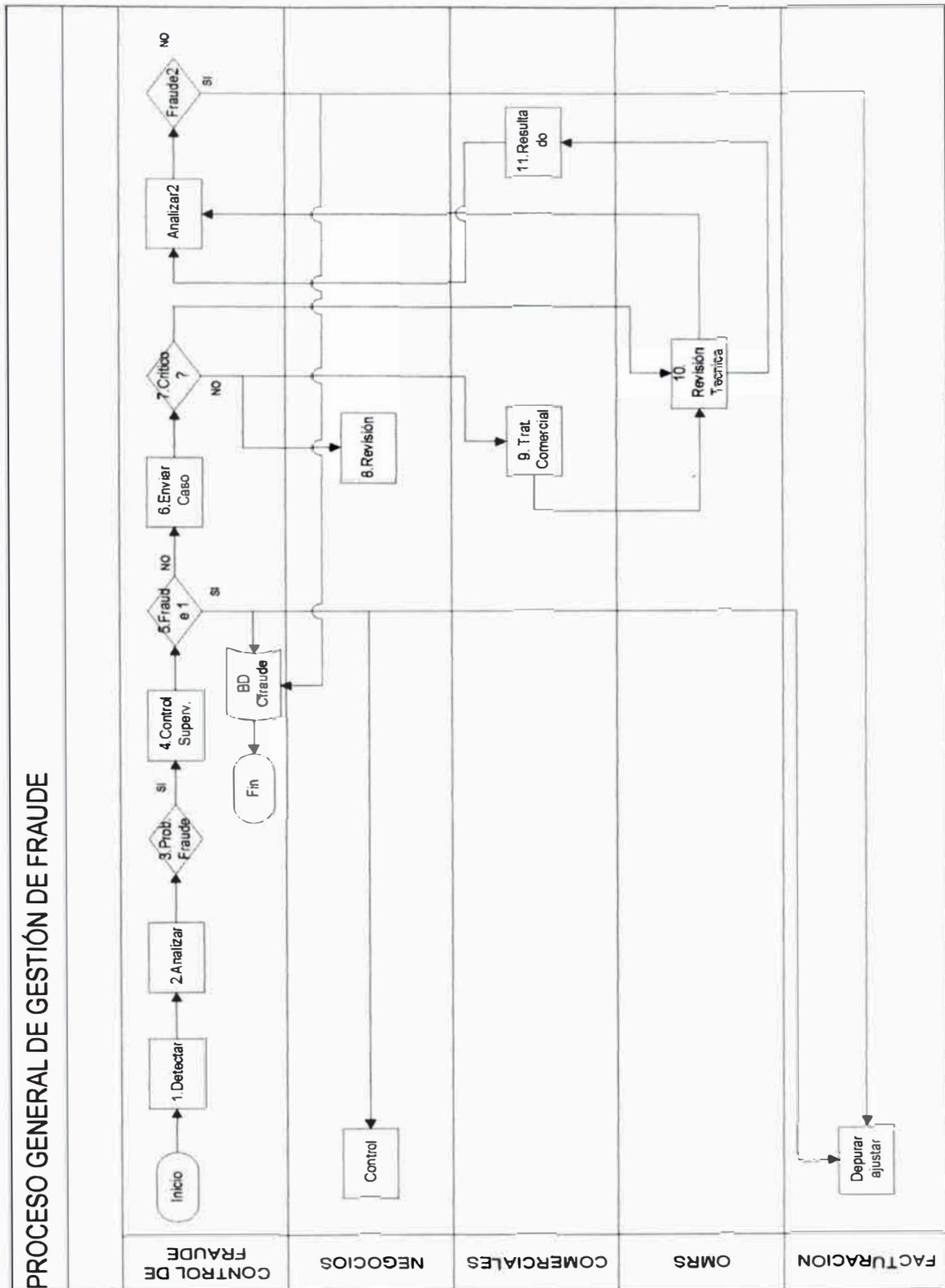
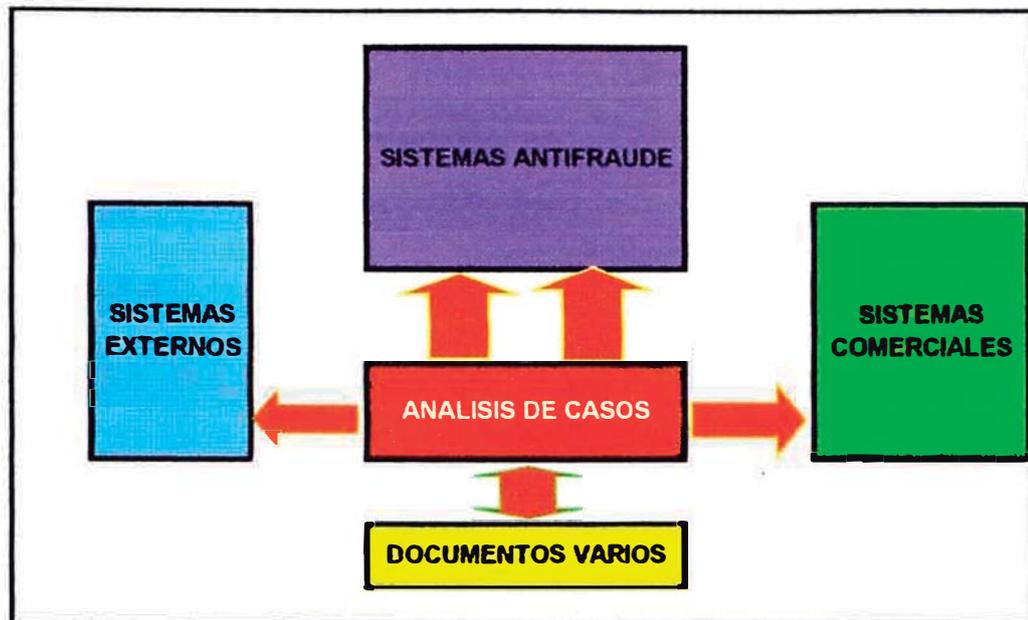


Grafico: Proceso General de control de fraude

3.3.3 DOCUMENTOS Y SISTEMAS DE APOYO



Relación de sistemas y Documentos de apoyo

No existe un sistema que soporte toda la gestión de fraude. La TI que se manejan son independiente para cada fase de la gestión del fraude como lo podemos mencionar:

Fase de Detección:

3.3.3.1 SISTEMA DE PROCESAMIENTO DE CDR'S :

Sistema que se encarga de procesar los CDR's hasta el valor de los detalles. Su primera función es almacenar los CDR's que sobrepasan los umbrales establecidos. La segunda función es originar los detallados de datos para su análisis.

Fase de Análisis:

3.3.3.2 SISTEMAS COMERCIALES

Son los sistemas de apoyo que permiten realizar el análisis de los casos. Estos sistemas son: OMEGA, LDIST, TASDET, BADECON, STC400 y el GESTEL.

3.3.3.3 SISTEMAS ANTIFRAUDE

Sistemas que nos permiten perfilar los casos de fraude e interactuar con bases de datos de anteriores casos de fraude. Contamos con dos sistemas antifraude el ATACS y el FRAUD VIEW.

3.3.3.4 SISTEMAS EXTERNOS DE APOYO:

Sistemas externos que nos permiten apoyar las decisiones de fraude. Podemos mencionar los siguientes: RENIEC, INFOCORP, REGISTROS PUBLICOS Y LA SUNAT.

3.3.3.5 DOCUMENTOS GENERALES

Existe una gran cantidad de documentación que se utilizaba en el proceso de gestión de fraude como casos de fraude, contratos para análisis de casos, documentos diversos de entrega del servicio, resultados de las áreas técnicas, resultado de las áreas comerciales, Documentos de ajustar y depurar trafico fraudulento, etc. muchos de los cuales se realizaban por correo electrónico. Es importante mencionar que casi la totalidad de acciones que se realizaban eran

gestionadas por este medio este procedimiento se ejecutaban para cada uno de los casos reportados, calculamos que para cada caso reportado existían un promedio de 20 correos para su ejecución.

3.3.4 LEVANTAMIENTO DEL PERFIL DE CONOCIMIENTOS



Gráfica: Levantamiento Perfil de conocimientos

Se desarrollo un levantamiento de información a cuatro grandes grupos involucrados en el proceso de gestión de fraude bajo las premisas de actividades desarrolladas para el proceso, Conocimiento para realizar las actividades y finalmente sobre el conocimiento que se tiene del fraude en telecomunicaciones.

Los cuatro grandes grupos fueron:

Personal de Control de fraude

Personal de las áreas técnicas

Personal de las áreas comerciales

Personal de las unidades de negocio.

3.3.5 ELABORACIÓN DEL DIAGNOSTICO

3.3.5.1 Eliminación de burocracia

- Existen procesos de control que no agregan valor al producto final.
- Mucha documentación para reportar un caso
- No hay Sinergia entre las áreas de Control de Fraude
- Mucha interacción de Control de fraude con las diversas áreas de los negocios
- Personal con poco o casi ningún conocimiento del tema de fraude en telecomunicaciones involucrados en el proceso de gestión del fraude

3.3.5.2 Reducción de los tiempos de ciclo

- Tiempos de ciclos muy largos
- No hay control de tiempos en las fases de gestión del fraude. No podemos asignar responsabilidades
- Mucha documentación que generan altos tiempos de ciclo.
- No existe responsable en las diferentes áreas de los negocios que vean los temas de fraude

3.3.5.3 Eliminación de errores

- Muchos casos de falsos positivos en la fase de detección y análisis
- No existe una estándar para los casos de fraude en sus distintas tipologías
- Existe encubrimiento de los casos de fraude por miedo a tomar la responsabilidad de los casos

3.3.5.4 Estandarización

- El servicio no esta estandarizado
- No existen indicadores de gestión adecuados

3.4 ESTRATEGIAS ADOPTADAS

La estrategia principal adoptada para solucionar el problema es el rediseñar el proceso de gestión de fraude y que sea soportado por un sistema de gestión.

Las iniciativas a la estrategia son:

3.4.1 Estandarizar los entregables por caso de fraude, esto se va ver reflejado en la etapa de detección y análisis. La estandarización del entregable se va dar en todas la topologías de fraude, vamos a reducir los errores.

3.4.2 Eliminar la Burocracia y actividades duplicadas y que no generen valor al proceso. Bajo la premisa de fusión y reordenamiento de sub. procesos actividades.

- 3.4.3 Crear indicadores de gestión y de productividad para las diferentes fases del proceso.
- 3.4.4 Crear una cultura orientada al conocimiento del fraude en telecomunicaciones y la protección del secreto de las telecomunicaciones.
- 3.4.5 Crear un aplicativo informático que soporte toda la gestión del fraude, para reducir los tiempos de reacción , mejora la calidad de la información a manejar y disminuir considerablemente la documentación existente

3.5 TOMA DE DECISIONES

3.5.1 ESTANDARIZACIÓN DE ENTREGABLES

Se procede a realizar la estandarización bajo las variables que se manejan para las diferentes tipologías de fraude, es importante conocer los diferentes requerimientos de los clientes, conocer que datos es importante para cada unidad de negocio que va interactuar en el proceso. La estandarización se ejecuto en las siguientes etapas.

Estandarización de Umbrales: Se realiza para cada tipología de fraude, es la primera estandarización que se realiza, permite manejar al área de control de fraude responsabilidades por las tipologías de fraude. Eliminamos errores de concepto entre los analistas de fraude, todos

manejan los mismo umbrales, mayor control de casos no reportados.

Estandarización de datos de Análisis: Se realiza para cada tipología de fraude, se desarrolla un listado de variables comunes y características que se deben manejar para los casos de fraude. Eliminamos errores y responsabilidades en los casos de fraude no detectados. Mejora la calidad de trabajo de los analistas de fraude.

Estandarización de Entregables: En el primer paso fue la elaboración de plantillas para entrega de los casos de fraude en todas las tipologías, divididas para cada negocio. El segundo paso fue llevar dicha plantilla al sistema integrado de gestión.

3.5.2 ELIMINAR BUROCRACIA

Las actividades duplicadas y que no generen valor a los procesos se van a eliminar y/o fusionar con otras actividades. Con los procesos ya estandarizados podemos eliminar algunos sub procesos como son el proceso de Control y supervisión (4) y Control de los negocios.

Al analizar los procesos nos podemos percatar que la demora se da en la documentación excesiva que se tiene que generar para atender un caso de fraude.

En el caso del sub. proceso de Control y supervisión se elimina ya que la estandarización de los casos de fraude en sus distintas tipologías nos permite una reducción en los errores.

3.5.3 CREAR CULTURA DE CONOCIMIENTO DE FRAUDE EN TELECOMUNICACIONES

Se desarrolla un plan comunicación con respecto a los temas de fraude y el secreto de telecomunicaciones. En su primera etapa para las personas involucradas en el proceso de gestión de fraude, en su segunda etapa para el personal crítico y la última etapa a todo el personal.

El plan de comunicación se desarrollo en tres etapas:

3.5.3.1 Diseño y validación

En esta etapa desarrollamos:

- Concepto y diseño del plan
- Validación con los interlocutores de cada negocio
- Cronograma de Charlas

3.5.3.2 Gestión

En esta etapa se desarrollo propiamente el plan de comunicación bajo el siguiente esquema:

Gestión Interpersonal: Diseño y envío de mensajes personalizados al personal encargado del proceso en cada uno de los negocios. Diseño de cartillas con la información de fraude en telecomunicaciones.

Gestión Grupal: Diseño y Ejecución de Charlas, reconocimiento a los trabajadores con mejor desempeño en la charlas, previa evolución de resultados.

Gestión Masiva: Elaboración de notas informativas, comunicación en los medios de comunicación interna, así como la campaña semanal de pantallas con temas de fraude.

3.5.3.3 Evaluación

Proceso de análisis mensual del resultado por las diferentes fases del fraude y el personal involucrado en ellas.

3.5.4 CREAR INDICADORES DE GESTIÓN Y PRODUCTIVIDAD

Una vez determinado la estandarización ya podemos empezar a medir nuestra gestión, para poder realizar dichas medidas se crearon indicadores en las diferentes fases de la gestión del fraude.

3.5.4.1 INDICADORES DE DETECCIÓN

3.5.4.1.1 FRAUDE DETECTADO BAJO UMBRAL:

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador evalúa el monto promedio por caso de fraude que no es detectado. Es decir los montos bajo el umbral establecido para cada tipología de fraude.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

$$\frac{\text{Monto Bajo Umbral}}{N^{\circ} \text{ Casos}}$$

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicaran cambio de los valores de los umbrales.

- **Periodicidad**

Mensual

3.5.4.1.2 TIEMPO PROMEDIO DE FRAUDE BAJO UMBRAL

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona información para toma de decisiones en la fase de detección.

- **Definición:**

El presente indicador evalúa el tiempo de permanencia del fraude bajo umbral. Fraude no detectado para cada tipología de fraude.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

$$\frac{\text{Promedio Tiempo A}}{\text{T1-T0}}$$

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicaran cambio de los valores de los umbrales.

- **Periodicidad**

Mensual

3.5.4.2 INDICADORES DE ANALISIS

3.5.4.2.1 FRAUDE DETECTADO HASTA INGRESO DE ALERTA.

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador evalúa el monto promedio por caso de fraude al momento de su detección. Es decir los montos de detección establecido para cada tipología de fraude.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

<i>Monto por Ingreso de Alerta</i>
<i>Nº Casos</i>

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicarán el grado de reacción en la etapa de análisis.

- **Periodicidad**

Semanal

3.5.4.2.2 TIEMPO PROMEDIO DE ANALISIS.

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona información para toma de decisiones en la fase de Análisis.

- **Definición:**

El presente indicador evalúa el tiempo reacción y análisis con relación a la primera alerta que sobrepasa el umbral establecido.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

$$\left[\text{Promedio Tiempo } B \right]$$

T_2-T_0

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicaran cambio en el procedimiento de análisis y/o prioridad de las tipologías de fraude.

- **Periodicidad**

Semanal

3.5.4.3 INDICADORES DE REACCION

3.5.4.3.1 FRAUDE DETECTADO DESPUES INGRESO DE ALERTA.

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador evalúa el monto promedio por caso de fraude al momento de su finalización. Es decir los montos de la fase de reacción establecido para cada tipología de fraude.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

<i>Monto despues Ingreso de Alerta</i>
<i>Nº Casos</i>

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicarán el grado de importancia al tratamiento en la etapa de Reacción. Los valores pueden variar para arriba o abajo.

- **Periodicidad**

Mensual

3.5.4.3.2 TIEMPO PROMEDIO DE REACCION.

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona información para toma de decisiones en la fase de Reacción.

- **Definición:**

El presente indicador evalúa el tiempo reacción con relación a los casos reportados por fraude.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

$$\text{Promedio Tiempo C}$$

$$T_3 - T_2$$

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicaran cambio en el procedimiento de reacción y/o prioridad de las tipologías de fraude. Los valores pueden variar para arriba o abajo.

- **Periodicidad**

Mensual.

3.5.4.4 INDICADORES GENERALES

3.5.4.4.1 FRAUDE DETECTADO POR CASO DE FRAUDE

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador evalúa el monto promedio total por caso de fraude al momento de su finalización.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

<input type="checkbox"/> Fraude Detectado	Pérdida económica ocasionada por el fraudulento
--	---

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicarán el grado de importancia al tratamiento general de la gestión del fraude.

- **Periodicidad**

Mensual

3.5.4.4.2 FRAUDE EVITADO POR CASO DE FRAUDE

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador evalúa el monto promedio total por caso de fraude que se evita al no detectar oportunamente un caso de fraude

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

□ Fraude Evitado = Pérdida económica que se evitó por la acción oportuna de LCF
--

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados alejados del valor óptimo indicarán el grado de importancia al tratamiento general de la gestión del fraude.

- **Periodicidad**

Mensual

3.5.4.4.3 PORCENTAJE DE FACTURACIÓN

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador mide el nivel de fraude detectado con respecto a la facturación del negocio.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

<input type="checkbox"/> % Fraude Detectado Total Facturado	Muestra el porcentaje que representa el fraude frente a lo que se factura
--	---

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados mayores al 0.5% indican tomar medidas más disuasivas para disminuir las incidencias de fraude

- **Periodicidad**

Mensual

3.5.4.4.4 PORCENTAJE DE INCOBRABLES

- **Justificación:**

Su uso se debe al tratamiento de cada tipología de fraude bajo determinadas condiciones. Nos proporciona los límites de responsabilidad.

- **Definición:**

El presente indicador mide el nivel de fraude detectado con respecto a la bolsa de casos de incobrables.

- **Recolección de Datos:**

Facturación Sistemas: Tráfico Facturado

Base de datos casos de fraude

Bolsa de reclamos y Incobrables

- **Metodología de cálculo:**

<input type="checkbox"/> % Fraude Detectado Total Incobrables	Muestra el porcentaje que representa el fraude frente a lo que se deja de percibir
--	--

- **Valor de rango:**

El valor de rango es variable de acuerdo a las condiciones del entorno y las tipologías de fraude.

- **Interpretación:**

Resultados mayores al 5% indican tomar medidas más disuasivas para disminuir las incidencias de fraude

- **Periodicidad**

Trimestral

3.5.5 CREAR APLICATIVO INFORMATICO

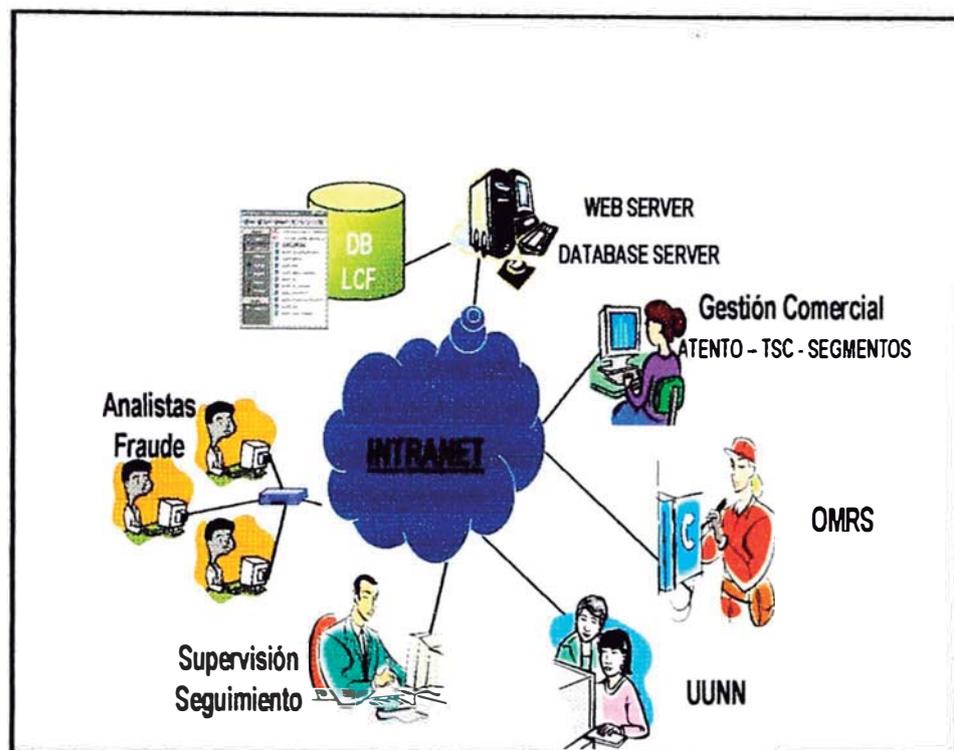
Sistema Centralizado de Casos de Fraude (SICECAF)

La solución que se presenta es un aplicativo e-business, que nos va permitir centralizar la información y nos va dar soporte a toda la gestión de fraude.

3.5.5.1 OBJETIVOS:

- Reducir la abundante documentación que se requiere para la gestión de cada caso de fraude.
- Agilizar el actual procedimiento inter gerencial de los casos de fraude entre el TGSC y sus clientes.
- Generar ahorros en la empresa, al usar la tecnología para la automatización, administración, análisis de casos de perfiles de clientes con probabilidad de fraude, así mismo como el reporte a las Unidades de Negocio.
- Reducir las pérdidas económicas por fraude en los negocios, al procesar más eficientemente la información de los casos detectados, de tal forma de tener una acción de oportuna.
- Establecer vínculos más estrechos e interactivos entre el TGSC y sus clientes (Unidades de Negocio).
- Incrementar la satisfacción de los clientes del TGSC.

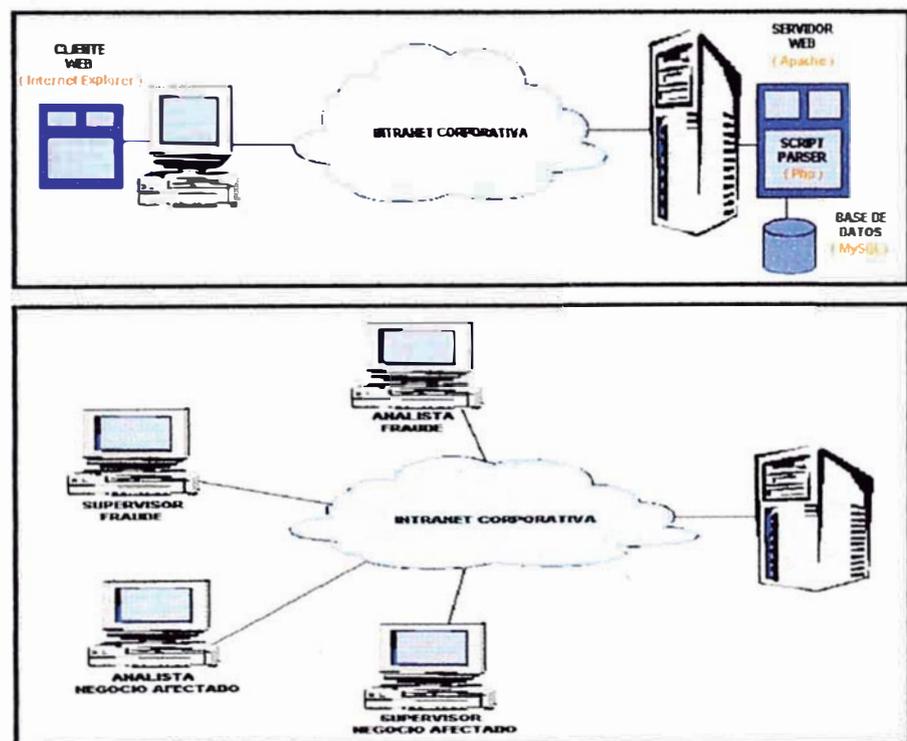
- Esta interfase nos va a permitir hacer un seguimiento en línea de todos los casos, y a nuestros CLIENTES (Negocios-Segmentos) ir añadiendo comentarios e información adicional acerca del tratamiento con el cliente
- Mejor control de las fases de la gestión del fraude



3.5.5.2 CARACTERÍSTICAS FUNCIONALES

- Servidor Web, Servidor Base de Datos (RDBMS), generación de páginas web dinámicas
- Acceso: a través de una interfase web
- Control Total sobre los datos a llenar y los datos que se muestran

- Seguridad: política de seguridad con perfiles de usuario
- No existe error en el llenado de los registros-plantillas determinadas
- Segmentación: Cada CLIENTE tendrá la información relevante y exclusiva para su negocio
- Esta interfase nos va a permitir hacer un seguimiento en línea de todos los casos, y a nuestros CLIENTES (Negocios-Segmentos) ir añadiendo comentarios e información adicional acerca del tratamiento con el cliente
- Gran capacidad de organización, búsqueda y almacenamiento



Esquema Solución e- business 2

3.5.5.3 COSTO DEL APLICATIVO

Primera fase:

Costo directo: \$ 15,480.00

Costo Indirecto: \$ 2,742.85

Costo Total: \$18,222.85

Desarrollo del aplicativo		18223
Costo Directo		
Desarrollo: Visual Interdev 6.0 y visual Basic 6.0	9640	
Servidor Web	3340	
Repositorio de datos: SQL Server 7.0	2500	
Total	<u>15480</u>	
Costo Indirecto		
Capacitación	940	
Help Desk	963	
Mantenimiento	840	
Total	<u>2743</u>	

CAPITULO IV

EVALUCION DE RESULTADOS

4.1 COSTO TOTAL DEL PROYECTO

Podemos apreciar en el cuadro adjunto el costo de todo el proyecto, para el proyecto solo estamos considerando al grupo operativo encargado, no se esta considerando el personal de mando involucrado en el proyecto.

Costo del Proyecto	52166
H-H proyecto	33943
Desarrollo del aplicativo	18223
Costo Directo	
Desarrollo: Visual Interdev 6.0 y visual Basic 6.0	9640
Servidor Web	3340
Repositorio de datos: SQL Server 7.0	2500
Total	15480
Costo Indirecto	
Capacitación	940
Help Desk	963
Mantenimiento	840
Total	2743

4.2 PERDIDA POR CASO DETECTADO

En el siguiente cuadro podemos ver la relación que existe con los ahorros (perdida Reducida) por las diferente redes.

	Basica	Nº Casos	Monto Detectado (S/)	Monto Detectado X Caso
Antes de proyecto	Año 1997	153	2 181 060	14 255
	Año 1998	338	2 929 040	8 666
	Año 1999	302	1 917 046	6 348
	Año 2000	797	4 484 000	5 626
	Año 2001	1189	4 885 000	4 108
	Año 2002	2205	8 866 000	4 021
	Promedio	831	4 210 358	5 069
Despues de proyecto	Año 2003	2278	2 752 394	1 208
	Año 2004	981	1 094 796	1 116
	Promedio	1630	1 923 595	1 162

Ahorro

Promedio de casos / Año *	1891
Ahorro por caso detectado	3 907
Ahorro Anual(S./)	7 385 934
Ahorro Anual(\$)	2 110 267

	Móvil	Nº Casos	Monto Detectado (\$)	Monto Detectado X Caso
Antes de proyecto	Año 1997	441	513 179	1 164
	Año 1998	554	1 034 158	1 867
	Año 1999	672	687 632	1 023
	Año 2000	1747	838 560	480
	Año 2001	14232	1 195 488	84
	Año 2002	21160	931 040	44
	Promedio	12380	988 363	80
Despues de proyecto	Año 2003	32160	385 920	12
	Año 2004	5600	67 200	12
	Promedio	18880	226 560	12

Ahorro

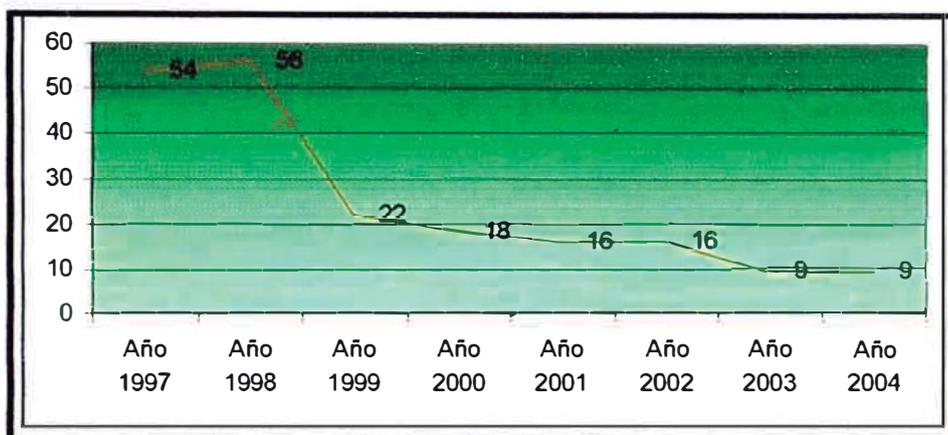
Promedio de casos / Año *	22517
Ahorro por caso detectado	68
Ahorro Anual(\$)	1 527 521

4.3 EVOLUCION DEL TIEMPO DE FRAUDE

Es el principal indicador que se maneja, podemos observar la evolución.

4.3.1 RED BASICA

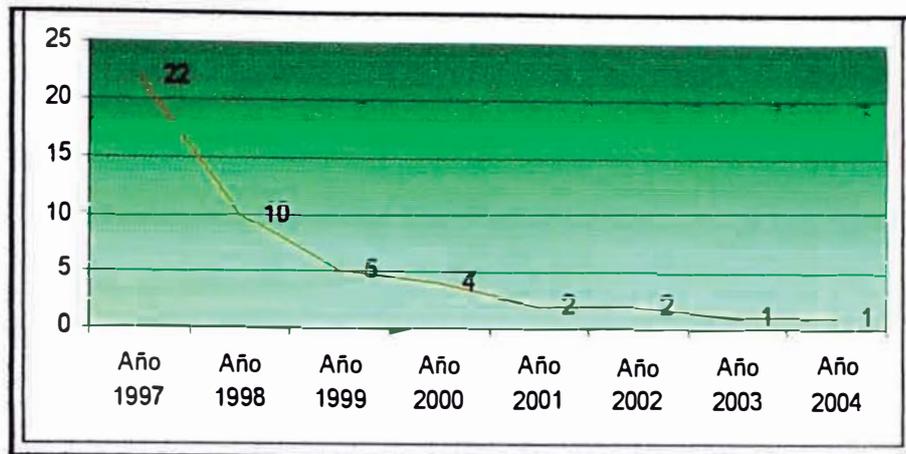
	Basica	Tiempo Total de Fraude
Antes de proyecto	Año 1997	54
	Año 1998	56
	Año 1999	22
	Año 2000	18
	Año 2001	16
	Año 2002	16
Despues de proyecto	Año 2003	9
	Año 2004	9



Gráfica Evolución tiempo promedio Fraude

4.3.2 RED MOVIL

	Móvil	Tiempo Total de Fraude
Antes de proyecto	Año 1997	22
	Año 1998	10
	Año 1999	5
	Año 2000	4
	Año 2001	2
	Año 2002	2
Despues de proyecto	Año 2003	1
	Año 2004	1



Gráfica Evolución tiempo promedio Fraude

4.4 FRAUDE EVITADO

El fraude evitado monto que deja de ser fraude por su detección a tiempo. El cálculo se realiza en base a los periodos de facturación de los clientes.

Basica	Nº Casos	Fraude Evitado (S./)	Fraude Evitado por caso
Año 2002	2205	37 680 500	17 089
Año 2003	2278	22 936 613	10 069
Año 2004	981	9 123 300	9 300

Móvil	Nº Casos	Fraude Evitado (\$)	Fraude Evitado por caso
Año 2002	21160	1 258 436	59
Año 2003	32160	936 080	29
Año 2004	5600	128 800	23

4.5 AHORRO PARA LOS NEGOCIOS

4.5.1 Red Fija

Básica		
Directo		<u>4.729.995</u>
Fraude Evitado **	3.463.835	
Fraude Detectado **	1.266.160	
Indirecto		
		<u>110.739</u>
Proceso de reclamo	64.823	
Proceso de facturación	45.916	
Ahorro Total		<u><u>4.840.734</u></u>
Factor 0,40		

4.5.2 Red Móvil

Móvil		
Directo		<u>787.434</u>
Fraude Evitado **	329.177	
Fraude Detectado **	458.256	
Indirecto		
		<u>128.670</u>
Proceso de reclamo	77.202	
Proceso de facturación	51.468	
Ahorro Total		<u><u>916.104</u></u>
Factor 0,30		

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se produjo una reducción en los tiempos de ciclo de gestión del fraude de un 46% en la red fija (9 días promedio mensual) y un 50% en la red móvil (1 día promedio mensual, en la actualidad estamos en menos de 1 día)
- Con respecto a los montos detectados en la red fija se generó un ahorro anual promedio de 2 millones de dólares y en la red móvil un ahorro anual de 1.5 millones de dólares.
- Se reglamentó el uso del fraude evitado para los cálculos de niveles de inversión en up-grade de sistemas antifraude.
- Para la red fija se generaron ahorros en los procesos de reclamo y los procesos de facturación de 64,800 dólares y 46,000 dólares respectivamente.

- Para la red móvil se generaron ahorros en los procesos de reclamo y los procesos de facturación de 77,000 dólares y 51,000 dólares respectivamente.
- Se mejoró considerablemente la calidad de entrega de los reportes por fraude. En línea.
- Se lleva un mejor control de las responsabilidades en las diferentes fases de la gestión del fraude.
- Actualmente el proceso de gestión de fraude es un procedimiento que tiene prioridad alta en varias unidades de negocios
- Se creó una unidad especializada para supervisar los seguimientos de línea.
- Los indicadores de gestión nos permiten realizar un control de objetivos y una mejora continua de los procesos.
- El sistema de gestión de fraude **SICECAF** permite la integración de todas las unidades de los negocios. Se crea la sinergia entre las áreas de control de fraude
- Se recomienda en una segunda etapa una interacción del sistema de gestión de fraude e-business con los sistemas comerciales y de apoyo.

5.2 RECOMENDACIONES

- Se recomienda en una segunda etapa del sistema de gestión de fraude **SICECAF**, nuevas funcionalidades e interacción con los sistemas comerciales y de apoyo.
- Se recomienda la mejora continua del Proceso de Gestión de Fraude
- Capacitación constante en nuevas modalidades de fraude y tecnologías en Telecomunicaciones
- Creación de área de inspecciones en línea dependiente de la Subgerencia de Control de Fraude para trato directo y oportuno de los casos.
- Integrar un Comité Multigerencial de lanzamiento de nuevos productos y servicios.

BIBLIOGRAFIA

- **Curso de Detección, Control y Gestión del Fraude en Telecomunicaciones.**
FML- Seguring Business – Brasil
- **Introducción al Fraude en Telecomunicaciones**
Grupo Especial AHCJET de Control de Fraude –Republica Dominicana
- **Interact The world's leading business conference on really hard stuff**
FairIsaac – San Diego California
- **Revenue Assurance & Fraud Management en telecom**
FML- Seguring Business – Brasil
- **Fraud and Revenue Assurance - Seguring Business**
FML- Seguring Business – Brasil
- **Análisis de Riegos – Telefónica Ingeniería de Seguridad**
Rafael Martín Enriquez – Argentina

ANEXOS

1. NORMAS REGULATORIAS

A partir del mes de agosto de 2000, mediante la nueva Ley de Organismos Reguladores, el OSIPTEL ha recibido mayores facultades y atribuciones legales, regulatorias y sancionatorias, entre otras definiciones relacionadas con el riesgo de fraude, dicha norma legal precisa que se atenta contra el derecho de las telecomunicaciones:

- ✓ Cuando una persona que no es quién cursa la comunicación, ni es el destinatario, intenta conocer, alterar, publicar, o utilizar el contenido de la misma o facilita que otra persona conozca de su existencia.
- ✓ Cuando se sustrae, intercepta, interfiere o desvía el curso de la comunicación.

El Osiptel ha incrementado las facultades de supervisión, puede iniciarla de oficio o a instancia de parte la supervisión, existiendo o no indicios de infracción, con o sin citación previa las entidades supervisadas deberán permitir el acceso de los funcionarios autorizados.

Las sanciones que puede aplicar el Osiptel van desde 100 UIT hasta más de 1000 UIT, siempre que no supere el 10 % de las ventas o ingresos brutos de la empresa infractora.

2. NORMAS VIGENTES:

2.1. Constitución Política del Perú:

Artículo 2.- Toda persona tiene derecho (...)

Inciso 10: Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen (...)

2.2. Código Penal

Intervención Telefónica

"Artículo 162°: El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.
(...)."

2.3. Decretos supremos

Decreto Supremo 013-93-TCC: Texto Único Ordenado de la Ley de Telecomunicaciones:

Artículo 4.- Toda persona tiene derecho a la inviolabilidad y al secreto de las telecomunicaciones. El Ministerio de Transportes, Comunicaciones, Vivienda y Construcción se encarga de proteger este derecho.

Artículo 87.- Constituyen infracciones muy graves: (...)

4) La interceptación o interferencia no autorizadas de los servicios de telecomunicaciones no destinados al uso libre del público en general.

5) La divulgación de la existencia o del contenido, o la publicación o cualquier otro uso de toda clase de información obtenida mediante la interceptación o interferencia de los servicios de telecomunicaciones no destinados al uso público general (...)"

Decreto Supremo 013-93-TCC: Reglamento General de la Ley de la Telecomunicaciones:

Artículo 10°.- Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones, cuando deliberadamente una persona que no es quien cursa la comunicación ni es el destinatario, sustrae, intercepta, interfiera, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo

u otra persona, conozca la existencia o el contenido de cualquier comunicación.

Las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación cursada a través de los servicios públicos de telecomunicaciones, están obligadas a preservar la inviolabilidad y el secreto de la misma.

Los concesionarios de servicios públicos de telecomunicaciones, están obligados a adoptar las medidas más idóneas para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios."

3. CONTRATO DE CONCESION

Mencionaremos partes del contrato de concesión celebrado con el gobierno peruano.

Sección 8.10: Secreto de las Telecomunicaciones y Protección de Datos.

Obligación de Salvaguardar el Secreto de las Telecomunicaciones y Protección de Datos.

La **EMPRESA CONCESIONARIA** establecerá medidas y procedimientos razonables para salvaguardar el secreto de las telecomunicaciones y mantener la confidencialidad de la información

personal relativa a los **USUARIOS** que atienda en el curso de sus negocios.

La EMPRESA CONCESIONARIA designará a nivel de la administración de la empresa, el personal que estará a cargo de la implementación, cumplimiento y supervisión de tales medidas

La EMPRESA CONCESIONARIA enviará al **MINISTERIO** y a **OSIPTEL** un informe anual sobre las medidas y procedimientos que se hayan establecido en su funcionamiento y sobre los cambios y las mejoras necesarias, debiendo presentar tales informes el 15 de febrero de cada año, comenzando el año siguiente al de la **FECHA EFECTIVA**.

Ámbito de la Obligación de Secreto y Protección de Datos.

La EMPRESA CONCESIONARIA salvaguardará el secreto de las telecomunicaciones y mantendrá la confidencialidad de la información personal relativa a sus **USUARIOS**, que atienda en el curso de sus negocios, salvo (i) el consentimiento previo, expreso y por escrito del **USUARIO** y demás partes involucradas o (ii) una orden judicial específica.

4. NORMALIZACION:

La normalización es la actividad de formular, publicar y aplicar, en relación a problemas reales o potenciales, documentos normativos dirigidos a la obtención de un grado óptimo de orden en un contexto dado.

La normalización ofrece importantes ventajas, principalmente para mejorar la adaptación de los productos, procesos y servicios a los propósitos para los cuales fueron diseñados, prevenir obstáculos técnicos al comercio y facilitar la cooperación tecnológica.

Más específicamente, la elaboración y aplicación de normas ofrece una serie de ventajas tanto para el fabricante de un producto o prestador de un servicio, como para los consumidores o usuarios; entre tales ventajas se destacan las siguientes:

- ✓ racionalizar las actividades productivas;
- ✓ maximizar la capacidad de producción;
- ✓ reducir inventarios;
- ✓ simplificar el trabajo;
- ✓ unificar criterios mínimos de calidad;
- ✓ facilitar la intercambiabilidad de piezas;
- ✓ usar maquinarias y herramientas más adecuadas;
- ✓ facilitar la capacitación del personal;

- ✓ disminuir los costos de producción;
- ✓ incrementar la productividad y competitividad de la empresa.

TECNICA EMPLEADA

Elaboración de Anteproyectos de Norma : Tomando como base normas internacionales, regionales o extranjeras, antecedentes técnicos nacionales y mejores practicas; este anteproyecto de norma se estudia en una Comité Técnico constituido por todas las areas involucradas en el proceso de gestión y otros sectores interesados en el tema, quienes hacen las observaciones del caso y generan un proyecto de norma.

Consulta Pública: El proyecto de norma es enviado a consulta pública a todas las partes interesadas, durante un periodo de 20 días, para que lo estudien y elaboren las observaciones que consideren pertinentes.

Comité Técnico: El Secretario Técnico del respectivo Comité elabora un resumen de las observaciones recibidas durante la consulta pública y se lo envía a todas las entidades que respondieron a la consulta; estas entidades constituyen el Comité Técnico y se reúnen para analizar las observaciones y el texto de la norma, hasta que se logre un consenso del texto final de la norma.

Aprobación de Norma: La norma es presentada al Directorio, junto con un informe del procedimiento de estudio, para su aprobación como norma.

Oficialización de la Norma: la Norma se oficializa y publica por todos los medios de comunicación existentes.