

Ecarrier – Tecnologías de Información

Tucapel Jiménez #95 oficina C
Santiago Centro – Santiago
Fono-Fax: + 56 (2) 688 3314
servicioalcliente@ecarrier.cl
www.ecarrier.cl



CONTROL DE VERSIÓN

VERSIÓN	FECHA	TIPO REVISIÓN	TIPO DE CAMBIO	REALIZADA POR
00	01/11/2009	Creación		Romina Inzunza

Ecarrier – Tecnologías de Información

Tucapel Jiménez #95 oficina C
Santiago Centro – Santiago
Fono-Fax: + 56 (2) 688 3314
servicioalcliente@ecarrier.cl
www.ecarrier.cl



Anexo Técnico TCero

Sistema de Control de Fraude

Ecarrier – Tecnologías de Información
Noviembre de 2009

Ecarrier – Tecnologías de Información

Tucapel Jiménez #95 oficina C
Santiago Centro – Santiago
Fono-Fax: + 56 (2) 688 3314
servicioalcliente@ecarrier.cl
www.ecarrier.cl



INDICE

CONTROL DE VERSIÓN.....	1
INDICE	3
I. Descripción del Sistema	4
II. Plan de implantación	6
III. Herramientas de desarrollo de software.....	6
IV. Seguridad.....	6
V. Requerimientos.....	6

I. Descripción del Sistema

El sistema de información que se describe a continuación, está orientado a realizar la autorización o rechazo, de las llamadas generadas por intermedio de vuestro portador. El módulo diseñado para este proceso denominado control de fraude, posee los elementos necesarios para interactuar en línea, tanto con los usuarios, informando los eventos más relevantes por medio de correo electrónico, como con el sistema de procesamiento de tráfico telefónico, alimentándolo con la información actualizada de aquellos clientes que han sido pasados a lista negra en forma automática. Además, provee las interfaces gráficas para realizar la mantención de clientes, permitiendo pasar de lista blanca a negra o viceversa, en forma manual.

Finalmente, a esta propuesta se incorpora el desarrollo de un servidor de procesamiento y tasación de CDRs en línea, el cual proveerá la información de cada llamada, pocos segundos más tarde de haberse efectuado; e que incluye los controles batch que amerita cualquier tipo de procesamiento en tiempo real.

Descripción del sistema:

1. Servidor de control de fraude

- Servidor multi-hebra basado en socket de TCP/IP
- Control de direcciones, despacha correo electrónico informando cuando una dirección IP no autorizada está intentando generar solicitudes de aprobación
- Control de inactividad, despacha mail informando que el sistema no ha recibido solicitudes durante un periodo de tiempo configurable
- Autorización o rechazo en línea basado en cantidad de intentos por sensibilidad de destino y en límite de crédito en pesos por número pagador
- Despacho de correo electrónico por cada ANI pasado a lista negra en forma automática, indicando el motivo.

2. Servidor de CDRs en línea

- Servidor multi-hebra basado en socket de TCP/IP
- Control de direcciones, despacha correo electrónico informando cuando una dirección IP no autorizada está intentando cargar información
- Control de inactividad, despacha mail informando que el sistema no ha recibido solicitudes durante un periodo de tiempo configurable
- Realiza medición y tasación en forma simultánea por cada CDR
- Despacho de correo electrónico informando errores de proceso, como falta de información, numeraciones no ingresadas a la base de datos, ANIs no válidos, etc.

3. Prototipo de pruebas de cliente

- Cliente basado en socket de TCP/IP
- Se conecta a servidores de control de fraude y de CDRs en línea
- Permite chequear el funcionamiento de cada servidor
- Permite revisar las respuestas que entrega el servidor

4. Proceso batch de control de CDRs Softswitch

- Proceso diario que chequea que todos los CDRs hayan sido cargados en línea
- Realiza la carga y tasación de todos los CDRs que fueron pasados por alto, informando los horarios de cada falla

5. Otros procesos

- Proceso automático de recálculo de consumos en pesos
- Proceso de medición de CDRs generados por CTC Mundo
- Modificar procesos de mediciones de cada compañía local, para excluir aquellos CDRs
- cargados desde el Softswitch o desde CTC Mundo

6. Parámetros

- Módulo Web, incluye seguridad de acceso
- Permite configurar los servidores en términos de definición de IP válidas, sensibilidad por destino, límites de crédito, cuentas de despacho de correo electrónico, etc.

7. Modificaciones al módulo de Servicio al Cliente

- Consulta y Mantenimiento de estados de ANIs por número llamador y pagador
- Modificación de límites de crédito caso a caso.

II. Plan de implantación

Desarrollo: 3 semanas

Definición de parámetros, pruebas y sintonía fina con servidor de radius: 1 semanas

Puesta en marcha: 1 semana

III. Herramientas de desarrollo de software

Microsoft Visual Basic 6.0 - SQL Server 7.0: Para los servidores, prototipos de pruebas y procesos

IIS - PHP: Para los módulos web.

IV. Seguridad

Conexión a la base de datos:

Corresponde al primer nivel de acceso y otorga permisos a los usuarios con relación al perfil definido para cada uno de ellos. Este nivel opera con los servicios de seguridad de Microsoft SQL 7.0 y su principal función es proteger la información ante eventuales intentos de acceso externos al sistema.

Conexión al sistema:

Corresponde al segundo nivel de acceso, opera en conjunto con el nivel de conexión a la base de datos y otorga los permisos necesarios para la operación del sistema.

V. Requerimientos

Servidor de datos:

- Servidor Dual, 2 procesadores Intel Pentium III o superior.
- 1 Gb Mb. RAM
- Discos Duros SCSI en modalidad RAID (Tamaño a definir considerando volúmenes esperados)
- Tarjeta de red 100BaseT
- Microsoft Windows 2000 Server
- Microsoft Internet Information Server 4.0
- Microsoft SQL Server 7.0 o superior

Otros:

- La programación del servidor RADIATOR la debe proveer el Cliente y consiste en conectar por medio de radius al Softswitch y por medio de TCP/IP al servidor de control de fraude.
- Para realizar la tasación en línea, es requisito que la transacción de solicitud entregue al menos la siguiente información: ANI, DNIS, fecha de la llamada, hora de la llamada y duración en segundos.