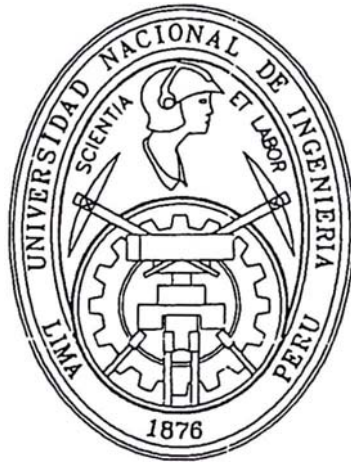


# Universidad Nacional de Ingeniería

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS



**“LA TECNOLOGIA RED PRIVADA VIRTUAL - VPN  
EN UNA EMPRESA FINANCIERA EN MICROFINANZAS”**

## **INFORME DE INGENIERIA**

Para optar el Título Profesional de :

**INGENIERO DE SISTEMAS**

**Jesús Alberto Zea Salas**

Lima - Perú

2003

## **DEDICATORIA**

A mis padres Jesús Zea Cano y Ernestina Salas Ormazabal  
por todo el esfuerzo realizado y por los consejos recibidos  
durante mi desarrollo personal

## **AGRADECIMIENTO**

A mis profesores, catedráticos, compañeros de trabajo  
y en especial a mi esposa Fanny por el apoyo recibido  
durante estos años en mi desarrollo profesional

## **INDICE**

CAPITULO I.	GENERALIDADES	10
1.	Antecedentes	10
2.	Objetivos	12
3.	Metas	12
CAPITULO II.	METODOLOGÍA	13
1.	Análisis de la Tecnología en la Solución de Conexiones	13
2.	Evaluación de los Recursos Informáticos	14
2.1	Estandarización de la Plataforma Informática en todas las Agencias	14
2.2.	Fortalecer la interconectividad de Agencias Locales en la Ciudad del Cusco	16
3.	Red Privada Virtual – VPN	16
3.1	Conectando Networks sobre Internet	16
3.2	Requerimiento básico	17
3.3	Fundamento al desarrollar un Túnel	18
3.4	Protocolo PPTP	20
CAPITULO III.	INTERCONEXIÓN DE VOZ Y DATOS PARA CMAC CUSCO	22
1.	Justificaciones Técnicas	22
2.	Recursos Necesarios	25
3.	Configuración de Hardware	26
4.	Diseño y Planeamiento del Directorio Activo	28

5. Reestructuración de servicios basados en Redes Públicas	32
6. Instalación del primer Controlador de Dominio y Catalogo Global	33
7. Instalación de los VPNS	35
8. Migración de Servidores Locales	36
9. Supervisión configuración implantada	37
CAPITULO IV. COSTOS Y BENEFICIOS	47
1. Costos	47
2. Beneficios	48
CAPITULO V. CONCLUSIONES Y RECOMEDACIONES	50
BIBLIOGRAFÍA	52
ANEXOS	53

## **DESCRIPTORES TEMATICOS**

- Red Privada Virtual
- Interconexión Infointernet
- VPN
- Voz IP
- Tecnología Tunneling
- Cableado Estructurado
- Redes Públicas y Privadas
- Topología Tipo Estrella

## **RESUMEN**

El presente Informe de Ingeniería describe las etapas y procedimientos mínimos que deben realizarse para la instalación de una interconexión de Voz y Data entre las agencias de una Empresa Financiera en Microfinanzas.

Se describe la configuración de una Red Privada Virtual - VPN y los enlaces de Voz basados en redes públicas y de la configuración de la Estructura del directorio Activo para la administración centralizada de toda la red de sistemas.

Adicionalmente, se especifican las actividades técnicas desarrolladas en cada una de las etapas del proyecto de interconexión, los recursos necesarios que deben utilizarse, las fases llevadas a cabo, los requerimientos de hardware que se presentaron, los tiempos planteados y los tiempos reales empleados, los costos efectuados y los beneficios obtenidos en toda la institución.

Por último, detallamos las conclusiones y recomendaciones que deberán tomarse en cuenta como resultado final de la instalación y operatividad del presente proyecto.

## INTRODUCCION

El Proyecto de Interconexión de Voz y Datos para las Agencias de Provincia de la CMAC Cusco S.A. consta en la configuración de un TUNEL SEGURO (VPN) y enlaces de voz basados en redes publicas y configuración de la estructura del Directorio Activo para la administración centralizada de toda la red de sistemas.

Este proyecto se formuló y se convirtió en una necesidad prioritaria de ejecución para la institución, debido al crecimiento operativo continuo que viene experimentando y a la necesidad de brindar mayores y mejores servicios y productos a todos los clientes a nivel de la Ciudad del Cusco y sobre todo a los clientes de las agencias de provincias donde opera la institución.

Asimismo, es importante mencionar que era necesario contar con una arquitectura y plataforma informática segura y eficiente en nuestros sistemas de computación como en nuestras redes de comunicaciones de datos que garanticen los resultados esperados.

La elección de esta plataforma de trabajo es una tarea muy importante debido a que nos permite alcanzar otras metas estratégicas en beneficio de la institución como son:

- La reducción de costos por transacción
- La mayor seguridad y confidencialidad de nuestros datos



- La facilidad en la administración
- Lograr un sistema tolerante a fallos
- El menor tiempo posible en la solución de problemas
- Capacidad para crecer en configuraciones aún más complejas

# **CAPITULO I**

## **GENERALIDADES**

### **1. Antecedentes**

A inicios del año 2000, la Caja Municipal de Ahorro y Crédito Cusco S.A. experimentó un cambio en sus procedimientos y sobre todo en su plataforma informática, con la adquisición de un nuevo Sistema Informático proveniente de la CMAC Arequipa.

Una vez concluidos los trabajos de migración y puesta en marcha del nuevo sistema, la CMAC Cusco S.A. entró en una etapa de familiarización y adecuación al nuevo sistema. Este período duró aproximadamente seis meses en los cuales tanto los usuarios del sistema como el personal informático que brinda soporte doblaron esfuerzos para sacar adelante la institución. Esta etapa fue muy rica puesto que todos asimilamos los nuevos procesos operativos instalados y sobre todo el personal de informática comenzó a dominar cada uno de estos procesos que forman parte del nuevo sistema.

En cuanto a las estrategias y planeamiento de sistemas, en primera instancia hicimos un análisis y una evaluación de la infraestructura informática con que contaba el departamento y sobre las proyecciones a corto y mediano plazo que

deberíamos seguir en función de las expectativas de la Gerencia y del desarrollo institucional.

Una de estas expectativas principales e importantes, era realizar la “Interconexión de todas las Agencias de la CMAC Cusco S.A.” y el trabajo debería orientarse sobre este objetivo pero sin descuidar por supuesto nuestra razón de ser, la de dar el “soporte adecuado, oportuno, seguro y de la mejor manera posible” a los usuarios de toda la institución.

Es por todo esto, que a partir de Febrero del 2000 el departamento trabajó en función de lograr estos objetivos, proponiéndose solicitar el Apoyo a la Gerencia para llevar a cabo la ejecución de los primeros proyectos que impulsarían y garantizarían los objetivos finales. Estos proyectos fueron:

- Evaluación de los recursos informáticos instalados y Proceder a Estandarizar toda la plataforma informática en todas las agencias
- Fortalecer la interconectividad de las agencias locales en la ciudad del Cusco

Estos trabajos serían la base fundamental para emprender el “Proyecto de Interconexión de todas las agencias”

Es importante mencionar que siempre se mantuvo la línea de mantener en lo posible la infraestructura de Hardware instalada puesto que la institución había realizado ya un fuerte desembolso en ello desde hace dos años atrás y sobre todo por la adquisición del nuevo software financiero y administrativo.

## **2. Objetivos**

Realizar los trabajos que fuesen necesarios para lograr la interconexión de todas las actuales agencias de la CMAC Cusco S.A. y establecer una metodología de trabajo para la interconexión de futuras agencias.

## **3. Metas**

- Evaluación de los recursos informáticos instalados y Proceder a Estandarizar toda la plataforma informática en todas las agencias
- Fortalecer la interconectividad de las agencias locales en la ciudad del Cusco
- Análisis de la Tecnología VPN utilizando la solución Tunneling para las conexiones
- Proyecto de Interconexión de la Agencias de provincia en la CMAC Cusco S.A.

## **CAPITULO II**

### **METODOLOGIA**

#### **1. Análisis de la tecnología en la Solución de Conexiones**

Esto surge a consecuencia de las diferentes de alternativas disponibles para lograr la interconexión entre toda la institución.

Factores principales tomados en cuenta:

- Proveedores de este tipo de servicios
- Tipo de enlaces
- Costo de los enlaces
- Factibilidad de contar con los servicios en los lugares donde contamos con agencias
- Tiempos de instalación y Puesta en Marcha
- Seguridad

Ver cuadro N° 01 de Alternativas de enlaces en los Anexos.

Por los costos y por la capacidad de inversión de la institución la alternativa de Telefónica Data era la más conveniente pero teníamos un detalle, era una Red

Pública. Aquí nace la idea de la TECNOLOGÍA VPN UTILIZANDO LA SOLUCIÓN TUNNELING PARA LAS CONEXIONES.

## **2. Evaluación de los Recursos Informáticos**

### **2.1. Estandarizar la Plataforma Informática en todas las agencias**

Lo primero que hicimos es realizar un trabajo de campo sobre el parque informático de la institución tanto en Hardware y software.

La oficina principal contaba con tres servidores: Uno para correo electrónico e internet, otro para las operaciones financieras y administrativas y otro para la información estadística de la institución.

La institución contaba con servicio de correo electrónico e internet con un ancho de banda de 64 Kbps

En cada una de las 05 agencias adicionales, existía un servidor que soportaba el sistema financiero y atendía las operaciones locales de la agencia. Para dar soporte técnico a estas instalamos en cada una un modem y una cuenta de correo exclusiva.

Como resultado de este estudio, determinamos:

- Estandarizar el software base de los servidores en una misma plataforma

Encontramos dos tipos de sistemas operativos instalados en los servidores:

- a) Netware 4.11 y
- b) Windows NT 4.0

Al evaluar precios de licencias (US\$ 15,000 en Netware y US\$ 5,500 en Windows en esos instantes) y sobre todo los temas de seguridad, monitoreo, soporte y facilidades técnicas para efectuar el proyecto principal de interconexión, nos decidimos a optar por la plataforma Microsoft con su Sistema Operativo Windows 2000 Server, Exchange 2000 Server, ISA Server y en el ámbito de PC Windows 2000 Professional.

- Re-estructurar los Servidores de Centro de Computo de la Oficina Principal y de todas las agencias

Se logró reinstalar de una manera más adecuada toda la infraestructura informática del Centro de Computo de la Oficina Principal y de todas las agencias. De esta manera se estaba poniendo las bases para la futura interconexión.

En esta etapa, se realizaron las siguientes actividades:

Se adquirieron 05 discos de 9 GB para la Oficina Principal

- a) Se adquirieron memorias para llevar el Servidor de Comunicaciones de la Oficina Principal a 512 Kb de RAM y cada servidor adicional a 128 Kb de RAM
- b) Se instaló el sistema operativo Windows 2000 Server en cada uno de los servidores en todas las agencias de la institución

- c) En la Oficina Principal en cuanto a la seguridad, se instaló el ISA Server y el antivirus McAfee, el Exchange Server 2000 reestructurando los correos electrónicos y accesos de Internet y reinstalando correctamente el arreglo de disco Raid 5 en el servidor principal eliminándolo del estadístico como se le encontró inicialmente.

## **2.2. Fortalecer la interconectividad de agencias locales en la Ciudad del Cusco**

En cuanto a las agencias de la ciudad del Cusco, estas se encontraban conectadas con: a) La Agencias de Afligidos con Fibra Optica y b) La Agencia de Wanchaq con servicio DIGIRED de Telefónica del Perú a 64 Kbps.

El problema se tenía con la interconexión de la Agencia de Wanchaq, por tener dos tipos de routers (3Com y Cisco) y la lentitud en los accesos al sistema y que algunas veces no enlazaban, se optó por determinar por una mejor alternativa y que más efectiva puesto que la interconexión que se tenía simplemente no funcionaba y estaba causando un gasto mensual de US\$560.00 a la institución sin tener los beneficios esperados.

La primera solución fue de instalar el servicio de Radio Enlace con radios Orinoco a 11 Mbps mostrando buenos resultados de interconectividad.

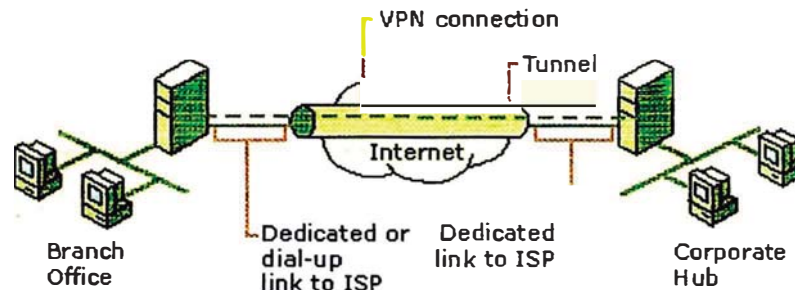
## **3. Red Privada Virtual - VPN**

### **3.1. Conectando Networks sobre Internet**

Existen dos métodos para usar VPNs para conectar LAN (local area networks) en sitios remotos



- Usando líneas dedicadas para conectar Oficinas remota a la LAN corporativa.
- Usando línea dial-up para conectar Oficinas remota a la LAN corporativa.



### 3.2. Requerimiento básico

Generalmente cuando desarrollamos de una solución de networking remota en una institución mediana o grande se necesita controlar los accesos corporativos, recursos e información. La solución debe permitir mover o reubicar clientes dentro la red (caso de analistas de créditos o R/P en ventanillas) o tener clientes remotos (fuera de la red) conectados a los recursos de la LAN, además la solución debe permitir a cada una de las oficinas remotas estar conectadas entre ellas y compartir recursos e información (conexión router-a-router).

En resumen la solución debe asegurar la privacidad e integridad de la data a través del Internet. Lo mismo concierne en aplicaciones con datos delicados al transmitirse en una internetwork coporativa.

Por lo tanto, una solución VPN debe proporcionar por lo menos lo

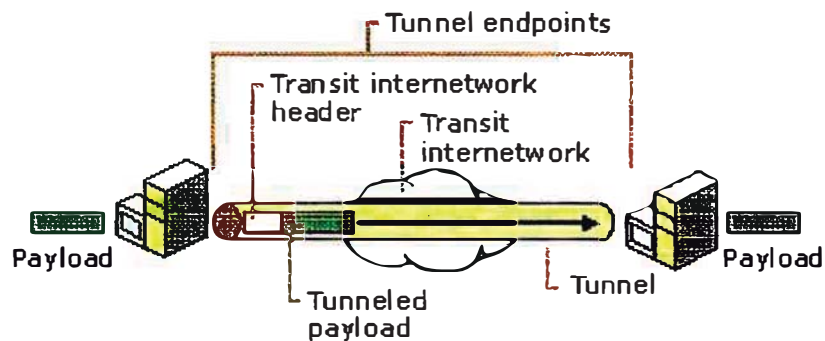
siguiente:

- Autenticación del usuario. La solución debe verificar a los clientes de VPN y restringir a los accesos VPN solamente a los clientes autorizados. Así como, la información de auditoría y estadística correspondiente sobre los accesos efectuados donde y cuando.
- Administración de direcciones. La solución debe asignar una dirección a los clientes VPN en la intranet y asegurar que las direcciones privadas se mantienen privadas.
- Data Encriptada. Los datos que estén en la red pública se deben hacer ilegibles a los clientes desautorizados en la red.
- Administración de claves. La solución debe crear y actualizar claves encriptadas para los clientes y el servidor.
- Soporte Multiprotocolo. La solución debe manejar los protocolos comunes usados en la red pública. Éstos incluyen IP, intercambio del paquete de la red interna (IPX), etcétera.

### **3.3. Fundamento al desarrollar un Túnel**

Tunneling es un método que permite utilizar en una infraestructura internetwork la transferencia de data desde una network hacia otra network. La data es transferida como paquetes desde un protocolo a otro y tal como el paquete se ha producido en el nodo origen, el protocolo tunneling encapsula la trama en un header adicional. El header adicional provee la información del ruteo para que la trama encapsulada pueda atravesar la red interna.

Los paquetes encapsulados son ruteados entre endpoints del tunnel en la red interna. La ruta lógica a través de la cual los paquetes encapsulados viajan a través de la internetwork es llamada tunel. Una vez que la trama encapsulada llega a su destino la trama es descapsulada y reenviada a su destino final. Tunneling posee todos estos procesos (encapsulación, transmission y descapsulación de paquetes).



Nuevas tecnologías tunneling han sido introducidas en los recientes años. Una de estas tecnologías novedosas es la siguiente:

- Point-to-Point Tunneling Protocol (PPTP). PPTP permite al tráfico IP, IPX, or NetBEUI estar encriptados y luego encapsularlos en una header IP para luego ser enviados a través de la IP internetwork corporativa o IP internetwork pública tal como lo es el Internet.

IPSec tunnel mode. El modo de tunel IPSec permite que los paquetes IP puedan ser encriptados y luego encapsularlos en una header IP para enviarlos a través de IP internetwork corporativas o a IP internetwork públicas tal como lo es el Internet.

### 3.4 Protocolo PPTP

PPTP es una capa de 2 protocolos que encapsula tramas PPP en un datagrama IP para la transmisión sobre una IP internetwork, tal como es el Internet. PPTP puede ser usado por accesos remotos y de conecciones VPN router-a-router.

El protocolo Tunneling Point-to-Point (PPTP) usa una conexión TCP para mantenimiento del tunnel y una versión modificada de la Generic Routing Encapsulation (GRE) para encapsular tramas PPP para data tunneled. Las cargas útiles (payloads) de las tramas PPP encapsuladas pueden ser encriptadas y/o comprimidas. La siguiente Figura muestra la estructura de un paquete PPTP conteniendo data de usuario.

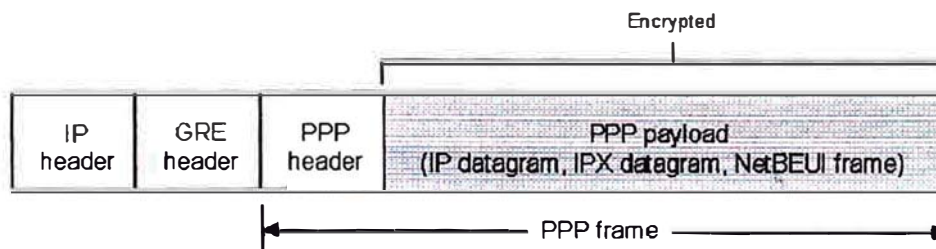


Figura. Estructura de un paquete PPTP conteniendo datos de usuario

El VPN permite a las corporaciones y usuarios conectarse a servidores remotos, oficinas sucursales, o a otras compañías sobre una red interna pública, mientras mantiene las comunicaciones seguras. En todos estos casos, la conexión segura le parece al usuario como una comunicación network privada, a pesar de que esta comunicación ocurre sobre una red interna pública. La tecnología VPN está diseñada para que las ediciones de las direcciones que rodean el

negocio actual tienden hacia la teleconmutación creciente y operaciones globales extensamente distribuidas, donde los trabajadores pueden ser capaces de conectarse a recursos centrales y comunicarse con todos los demás.

## **CAPITULO III**

### **INTERCONEXIÓN DE VOZ Y DATOS PARA CMAC CUSCO**

#### **1. Justificaciones Técnicas**

Existen dos actividades importantes y son:

##### **i. Túneles Seguros sobre Redes Públicas y Privadas**

Con la aparición del fenómeno INTERNET, y la difusión de este medio de comunicación han aparecido nuevas tecnologías que nos permiten ahora interconectarnos de una manera nunca antes prevista. Por otro lado los costos de conexión han sido reducidos al mínimo.

Sin embargo es necesario dejar bien en claro que INTERNET es una gran red a la que cualquier persona tiene acceso, de allí su nombre de RED PÚBLICA. Para fines de tratamiento de información y especialmente a la información que es utilizada por una entidad financiera se presenta el reto de garantizar la confidencialidad y seguridad de la información.

Al ser INTERNET una red pública, cualquier individuo puede acceder de muchas maneras a la información que transita por allí. Para solucionar

estos problemas se ha creado una tecnología llamada TUNELLING, la cual consiste en utilizar el transporte de la red pública para enviar información encriptada es decir información codificada que no puede ser vista por ninguna otra persona sino por quien la envió y la recibió.

Para describir un poco este proceso que resulta ser el más importante, mencionaremos una analogía. Asumamos que INTERNET es un puente que une 2 puntos separados por un océano. Debido a que cualquier persona puede transportarse por el puente, la institución que también requiere utilizar dicho puente contrata camiones blindados. Posteriormente se inicia el paso del puente y allí ocurre lo siguiente; los demás transeúntes que en ese momento utilizan el puente pueden ver los camiones blindados transitando, pero no pueden ver el contenido que llevan. De la misma manera en un TÚNEL SEGURO, la información viaja protegida de cualquier posibilidad de análisis de terceros.

Otro análisis que podemos hacer de la analogía antes expuesta es ¿Por qué usar el puente y no usar un puente privado?. Digamos que porque no tiene otro costo para nosotros mayor que el peaje. Por ello decimos que Internet es una red pública de bajo costo. De otra manera habría que construir un puente a un costo más elevado para conseguir los mismos resultados.

## **Conclusión**

Por lo anteriormente expuesto se concluye que es imprescindible debido a la naturaleza de la institución de configurar los llamados TÚNELES SEGUROS.

## **ii. Instalación y Configuración del Directorio Activo**

Debido al crecimiento y a la integración de nuestras sucursales así como de los servicios y facilidades que brindamos a nuestros usuarios, la administración de la red cada vez se torna mas complicada. Esto no sería problema si dentro de nuestras estructuras de costo contemplamos un creciente incremento de recursos humanos que nos permitan satisfacer la demanda de requerimientos de los múltiples usuarios, Por otro lado al incrementarse el número de usuarios, la posibilidad de una falla es más visible. Esto significa que en entornos de redes normales y operando en condiciones totalmente estables siempre existe la posibilidad de problemas. Si suponemos que la posibilidad de aparición de problemas es de .5% al día, entenderemos también que para una red con 200 computadoras, se esperaría que un equipo por lo menos presente fallas diariamente. Son conocidos los problemas que se generan por la inoperatividad de un equipo. Ya que cada equipo es asignado a un integrante de la institución y a que este realiza una labor productiva dentro de la misma, se entiende que se produce una perdida de calidad de servicio global que en muchos casos no es bien percibida. Cuando estas fallas tienen que ver con servidores el problema se torna mas complicado ya que esto significa muchas veces la falta de atención de toda una agencia.

Como la institución esta sometida a exigencias por organismos supervisores, no es posible ni aceptable tener paros en los sistemas y falta de atención por prolongados periodos



## **Conclusión**

Es importante pues contar con sistemas y plataformas que nos permitan una facilidad en la administración y la posibilidad de solucionar problemas con la mayor celeridad. Es por ello que se propone la instalación de Directorio Activo como una herramienta de última generación que nos permita lograr las siguientes metas:

- La reducción de costos por transacción
- La facilidad en la administración
- Lograr un sistema tolerante a fallos
- El menor tiempo posible en la solución de problemas
- Capacidad para crecer en configuraciones aun más complejas.

## **Objetivo General**

Establecer una base sólida tecnológica y estable para el desarrollo de las operaciones financieras en ambientes de redes públicas y privadas

## **2. Recursos Necesarios**

### **i. Hardware**

Los recursos de hardware están dados por todos los equipos que la institución posee a los cuales se les realizará un upgrade (mejoras, véase hoja de requerimientos de hardware) y así serán utilizados en el proceso de instalación y configuración de los sistemas antes descritos.

## **ii. Software**

Para hacer posible la implementación de las tecnologías descritas es necesario instalar en todos los servidores que la empresa tenga:

Microsoft Windows 2000 Server

Para los equipos adicionales los cuales son las estaciones de trabajo se instalará:

Microsoft Windows 2000 Professional

## **iii. Recursos Humanos**

Debido a la magnitud del proyecto se requiere la participación de un experto en certificación MS para las comunicaciones y la participación activa de la jefatura de sistemas en la etapa de planeamiento de las configuraciones.

Para la ejecución de la instalación y a fin de lograr un menor tiempo en el logro de resultados, será necesaria la participación del personal de soporte que la empresa tenga en la actualidad.

## **3. Configuración de Hardware**

En este punto se realizarán las siguientes actividades

### **i. Configuración del Firmware de todos los Servidores con Upgrade de BIOS según especificaciones de fabricante**

A fin de poder iniciar este proyecto debemos garantizar un 100% de compatibilidad de todo el hardware que se tiene en lo referente a Servidores.

Debido a que Windows 2000 es un sistema operativo relativamente nuevo el fabricante recomienda una actualización de todos el Firmware de cada uno de los componentes que se han instalado en los servidores con las ultimas versiones disponibles en el sitio web.

## **ii. Configuración de los Routers**

Los routers a adquirirse deberán ser configurados a fin de funcionar con los enlaces suministrados por Telefónica.

Asimismo es necesario la configuración de dichos dispositivos a fin de soportar el transporte de voz.

## **iii. Configuración de otro Hardware**

Asimismo se dispone de hardware que permitirá el incremento de la tolerancia a fallos. Nos estamos refiriendo al arreglo de discos. Este dispositivo también deberá ser configurado para poder utilizar la plataforma Windows 2000 Server

## **iv. Factores críticos de éxito de la etapa**

- Nuevo esquema de trabajo
- Ancho de Banda Limitado
- Estabilidad del servicio

- Disponibilidad del 100% de Hardware
- Optimización y adecuación de la infraestructura actual para la nueva estructura planificada.

#### **v. Objetivos a cumplirse**

- 100% funcionalidad
- Prestaciones superiores a las obtenidas en instantes previos a la aplicación de cambios
- Administración y Prestaciones de acuerdo a premisas definidas en el planeamiento global del proyecto.

### **4. Diseño y Planeamiento del Directorio Activo**

El presente informe tiene por objeto explicar la metodología y pasos a seguir para poder configurar apropiadamente la red de servidores con el objetivo de lograr un entorno para la seguridad y administración centralizada.

#### **i. Planeamiento Estructural para un entorno compuesto por Oficinas Sucursales**

##### **Disponibilidad Actual**

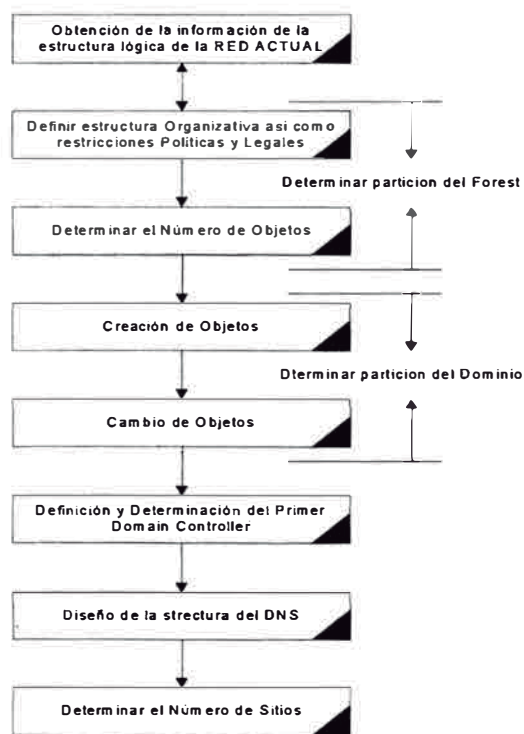
- Se cuentan con enlaces dedicados los cuales permiten una configuración centralizada de Microsoft Active Directory.
- La mayoría de servidores, poseen el sistema operativo Windows 2000 Server.

- Se han configurado dominios en cada sucursal los cuales están 100% funcionales.

## ii. Metodología

**a. Planeamiento Estructural.** En este punto se determina la necesidad de determinar una partición del FOREST. Ello debido a las políticas de administración y consideraciones legales.

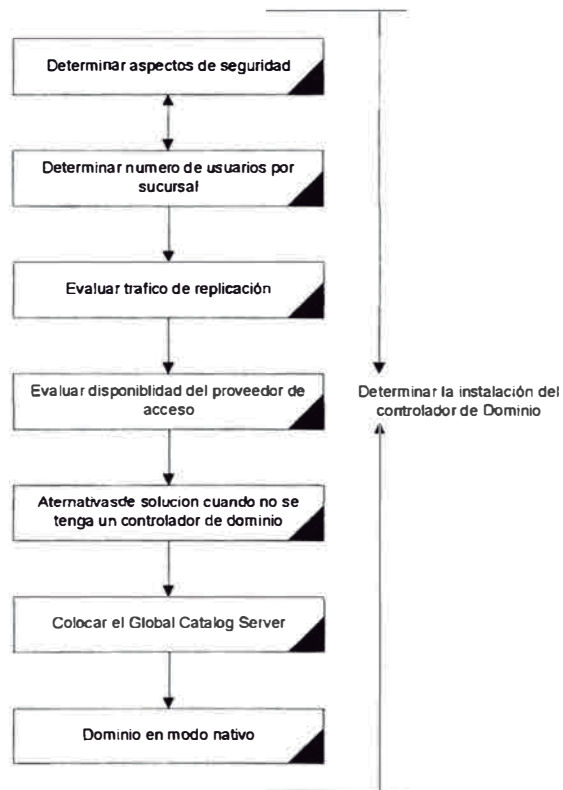
### Diagrama de Procedimientos



### b. Determinación de Catalogo Global y el Controlador de Dominio.

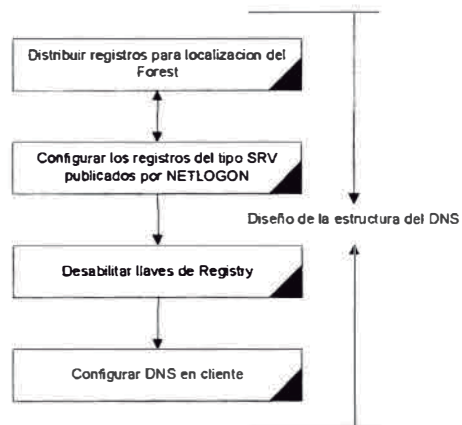
En las oficinas sucursales y en otros entorno distribuidos la mayor decisión es decidir donde localizar los controladores de dominio y los catálogos globales.

## Diagrama de Procedimientos



**c. Diseño del DNS.** Para poder considerar autenticaciones con el menor trafico posible en los escenarios WAN, es necesario planificar la configuración de estos servicios.

## Diagrama de Procedimientos

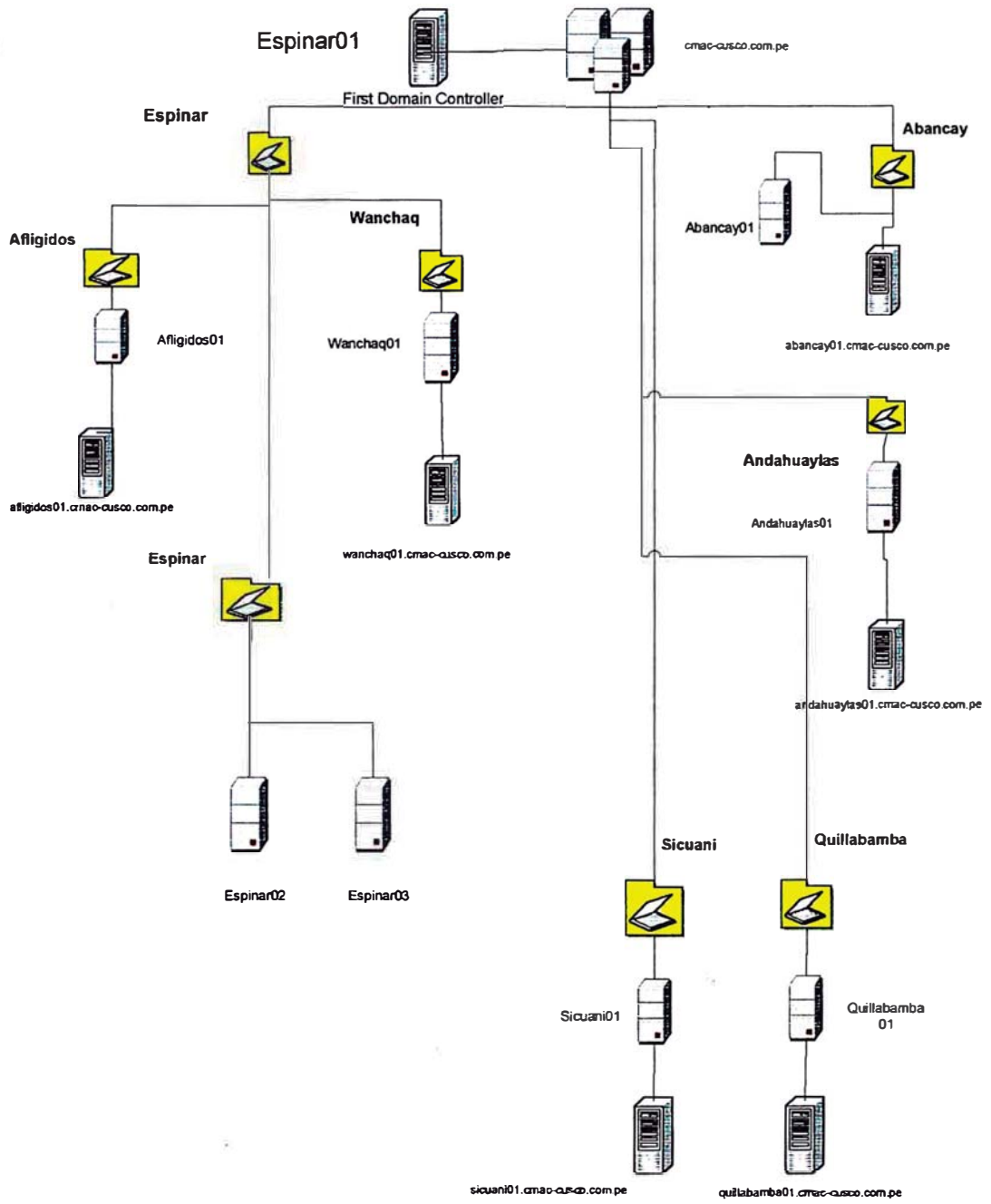


**d. Determinación del número de Sites.** Esta definición se realizará de acuerdo a los siguientes factores:

- Numero de localizaciones independientes
- Conectividad y disponibilidad entre servidores
- Numero de lugares sin controladores de dominio.

Ver Esquema Preliminar adjunto

# ESQUEMA PRELIMINAR





## **5. Reestructuración de servicios basados en Redes Públicas**

En este punto se realizarán las siguientes actividades

### **i. Planeamiento de las políticas de seguridad que se utilizarán en la institución**

En este punto se evaluarán y planearán las directivas de seguridad para la fácil administración de la red. En este caso debe considerarse un estándar para cada servidor conectado a una red pública así como las políticas de acceso al servidor.

Las restricciones de seguridad, administración, planeamiento y/o reposición de estaciones de trabajo en los sistemas de redes remotos conectadas a circuitos públicos, deberán ser analizadas en esta etapa.

### **ii. Definición del FIRE WALL físico y lógico, así como sus componentes. Configuración de la puerta de Enlace a Internet**

La instalación y configuración de las barreras de protección que prevengan accesos no autorizados así como ataques que afecten nuestro tráfico. Configurar los servicios de tal manera que podamos ejercer un 100% de control sobre estos elementos.

### **iii. Configuración de la ubicación del Sistema de Correo Electrónico, así como de sus componentes actuales**

Debido a que la institución posee un sistema de correo electrónico basado en dominio propio, deben reestructurarse ambos servicios con

el objeto de poder facilitar y centralizar su administración. Por otro lado debido a que este servicio consume un ancho de banda importante, es de necesidad estratégica el planeamiento de sus políticas y utilización

#### **iv. Factores críticos de éxito de la etapa**

- Nuevo esquema de trabajo
- Ancho de Banda Limitado
- Estabilidad del servicio
- Optimización y adecuación de la infraestructura actual para la nueva estructura planificada.

#### **v. Objetivos a cumplirse**

- 100% funcionalidad
- Prestaciones superiores a las obtenidas en instantes previos a la aplicación de cambios
- Administración y Prestaciones de acuerdo a premisas definidas en el planeamiento global del proyecto.

### **6. Instalación del primer controlador de dominio y catalogo global**

Como ya se sabe se contara con una red de circuitos virtuales lo que nos permite un entorno híbrido LAN/WAN. Sin embargo la velocidad de los enlaces es un factor crítico de éxito. El enlace por si solo nos garantiza conectividad, pero la velocidad del enlace no permite mayor o menor eficiencia.

En el caso particular de la institución se contará con enlaces distribuidos de 64KBPS y un enlace principal de 256KBPS (Inicialmente será de 128KBPS). Otro elemento que nos permitirá definir el planeamiento de estos servicios es el hecho que en las redes publicas se utilizara una parte del ancho de banda para la transmisión de voz. De todo esto se concluye que el análisis de tráfico y la minimización del consumo del ancho de banda son aspectos fundamentales.

Las premisas para el análisis son:

- El ancho de banda nunca es suficiente.
- El margen de error por parte de la disponibilidad del servicio en cuanto se refiere a la responsabilidad del CPI es alta.

Tareas adicionales en esta etapa, son las de migrar un servidor basado en el sistema operativo Windows 2000 con una configuración independiente. En este servidor es donde residirá el Directorio Activo además del Catalogo Global. Las labores de esta sub tarea, están definidas en el cuadro de tareas y tiempos que se describen más adelante

#### **i. Factores críticos de éxito de la etapa**

- Distribución del Directorio Activo Optima
- Ancho de Banda Limitado
- Estabilidad del servicio

#### **ii. Objetivos a cumplirse**

- ~ 100% funcionalidad
- Prestaciones superiores a las obtenidas en instantes previos a la aplicación de cambios
- Administración y Prestaciones de acuerdo a premisas definidas en el planeamiento global del proyecto.

## **7. Instalación de VPNS**

En los circuitos que conecten redes a través de la red pública INTERNET, será necesario instalar un VPN que garantice la seguridad de las mismas así como la seguridad de todo el flujo de información que fluye por dichos enlaces.

En esta etapa se establece una comunicación segura entre las redes.

### **i. Factores críticos de éxito de la etapa**

- Interoperabilidad entre redes.
- Localización de todos los objetos de red sin ningún inconveniente, esto siempre limitado por la velocidad del enlace contratado.
- Seguridad para el flujo de información
- Estabilidad del servicio
- Tiempos de respuesta aceptables para la infraestructura utilizada

### **ii. Objetivos a cumplirse**

- Lograr la total interoperabilidad entre redes.
- Establecer los túneles seguros para transporte de información

## **8. Migración a servidores locales**

Los servidores conectados a redes publicas, deberán ser migrados para poder integrarse a la estructura de Directorio Activo.

Debido a que estos servidores están distribuidos y conectados mediante una red privada, las consideraciones de seguridad son mínimas. Se deberá dar énfasis al hecho de que un requisito anteriormente explicados sostiene que un factor importante de éxito a considerar es la autonomía de funcionamiento. Mediante el planeamiento se configuraran todos los servicios a fin de poder lograr este objetivo.

Las tareas más importantes en esta fase son:

- Backup de la información de cada servidor
- Migración de los servidores actualmente con sistema operativo Windows 2000 Server hacia el esquema integrado y cambio de idioma.
- Reestablecimiento, de la información
- Aplicación de las seguridades, políticas y restricciones.
- Revisión y supervisión de su funcionamiento.

### **i. Factores críticos de éxito de la etapa**

- Disponibilidad de todos los recursos para la migración
- Estabilidad del hardware que se esta utilizando en este momento

## **ii. Objetivos a cumplirse**

- Lograr una migración sin traumas
- Transparencia al usuario
- 0% de tiempo de parada del sistema
- Funcionalidad al 100% de todos los servicios

## **9. Supervisión de la configuración implantada**

Esta etapa busca lograr la estabilidad final de los cambios realizados. Como ya se sabe, cuando se hacen cambios como los descritos, es muy importante hacer un seguimiento a fin de detectar fenómenos o problemas no previstos en la etapa de planeamiento previa.

No se descarta una labor de afinamiento y optimización de algunos procesos. Es muy importante considerar que la estabilidad de la instalación estará siempre vinculado a los factores críticos de cada fase y también a los objetivos que se esperan al culminar cada fase.

### **i. Factores críticos de éxito de la etapa**

- Disponibilidad de todos los recursos humanos comprometidos en la instalación de todos los servicios
- Correcto, adecuado y oportuno feed-back por parte del usuario

### **ii. Objetivos a cumplirse**

- Funcionalidad al 100% de todos los servicios contratados.
- 100% de satisfacción de los usuarios del FrontEnd y del BackEnd

La Caja Municipal Cusco S.A. cuenta actualmente con la siguiente infraestructura:

## **OFICINAS**

**Oficina Principal.** Asimismo es la sede de la jefatura de sistemas y también donde se centralizan la mayor cantidad de operaciones y la carga de tareas administrativas.

**Oficinas Sucursales Adicionales.** Las oficinas sucursales en donde opera la CMAC son: *Afligidos, Wanchaq.*

**Oficinas Sucursales en Provincias.** Las oficinas en provincias son Abancay, Andahuaylas, Quillabamba, Sicuani y Juliaca

## **INTERCONEXIONES.**

**Oficina principal.** La oficina principal esta conectada con enlace DIGIRED con la sucursal de Wanchaq a 128KBPS

**Oficinas Provinciales.** Las oficinas de provincias poseen un enlace que las conectan con la red Internet a 128 KBPS. El tipo de enlace es INFOINTERNET

**Fibra Óptica.** La sucursal de Afligidos esta conectada mediante un enlace de fibra óptica a la oficina principal.

## SERVIDORES.

<b>Oficina Principal</b>	
Servidor de Correo/FireWall	<b>ESPN0101</b>
Servidor de VPN Autenticación/Raiz de Servicios de Directorio/WINS/DHCP	<b>ESPN0102</b>
Servidor de Datos	<b>ESPN0201</b>
Servidor de Desarrollo	<b>ESPN0301</b>
<b>Sucursal Afligidos</b>	
Servidor de Datos	<b>AFLG0201</b>
<b>Sucursal Wanchaq</b>	
Servidor de Datos	<b>WNCH0201</b>
<b>Sucursal Abancay</b>	
Servidor de Datos	<b>ABCY0201</b>
<b>Sucursal Andahuaylas</b>	
Servidor de Datos	<b>ANDH0201</b>
<b>Sucursal Quillabamba</b>	
Servidor de Datos	<b>QUIL0201</b>
<b>Sucursal Sicuani</b>	
Servidor de Datos	<b>SICN0201</b>

### Diseño y planeamiento de Directorio activo (ADS)

El directorio activo para la CMAC-CUSCO, ha sido diseñado en base a una centralización de la administración de la red y también con el objeto de maximizar la seguridad. De acuerdo a lo ya explicado anteriormente

### PLANEAMIENTO ESTRUCTURAL.

Para esta fase se han considerado las siguientes variables.

- 1 Forest. Determinado por la magnitud de la empresa y la diversificación de actividades



- 1 Tree. Determinado por la magnitud de la empresa.
- 1 Dominio. A fin de permitir un modelo de tolerancia a fallos y una fácil administración se decidió utilizar un único dominio en la institución. De acuerdo a un análisis del tráfico se ha considerado una estructura descentralizada a fin de poder
- 1 MASTER DOMAIN CONTROLLER ubicado en el servidor **ESPN0102**, el cual posee los roles de IM FSMO
- 1 DOMAIN CONTROLLER ubicado en el servidor **ESPN0201**, el cual posee los roles de FSMO, DNM, SM, PDC, RID,
- 1 DOMAIN CONTROLLER ubicado en el servidor **AFLG0201**

Se decidió utilizar el mismo nombre de dominio que se tiene en INTERNET con el objeto de poder compatibilizar direcciones INTRANET e INTERNET a futuro, siendo el dominio raíz:

**cmac-cusco.com.pe**

## **DETERMINACIÓN DE CATALOGO GLOBAL Y EL CONTROLADOR DE DOMINIO.**

En las oficinas sucursales y en otros entornos distribuidos la mayor decisión es decidir donde localizar los controladores. Se solicitó que las sucursales tuvieran un grado de autonomía en caso de las comunes interrupciones de los enlaces. Ello significa permitir que las sucursales puedan operar en forma independiente. Para ello se optó por un único dominio con controladores de dominio distribuidos en cada sucursal.

## **DISEÑO DEL DNS.**

Para poder considerar autenticaciones con el menor tráfico posible en los escenarios WAN, es necesario planificar la configuración de estos servicios. Cada servidor ubicado en una sucursal posee este servicio, para resolución de nombres, de la Lan a la cual sirve

## **DETERMINACIÓN DEL NÚMERO DE SITES.**

Esta definición se realizó de acuerdo a los siguientes factores:

- Numero de localizaciones independientes
- Conectividad y disponibilidad entre servidores
- Numero de lugares sin controladores de dominio.

Se han creado 7 sitios determinados por el tipo de conexión:

**Site-Cusco:** ESPN0102, ESPN0201 y AFLG0201. Compuesto por los 3 servidores que se encuentran en la red principal de la oficina central. Se ha considerado el servidor de Afligidos debido a que este al estar conectado en fibra optica, se comporta exactamente como un servidor local. Estos 3 servidores son los responsables de suministrar la infraestructura estructural y “columnar” de todo el esquema

**Site-Wanchaq:** WNCH0201. Este servidor conforma la sucursal que se conecta con la oficina principal (ESPINAR) a través de un enlace DIGIRED de 128KBPS

**Site-Abancay:** ABCY0201. Este servidor conforma la sucursal que se conecta a INTERNET a través de un enlace INFOINTERNET de 128KBPS.

**Site-Andahuaylas:** ANDH0201. Este servidor conforma la sucursal que se conecta a INTERNET a través de un enlace INFOINTERNET de 128KBPS.

**Site-Sicuani:** SICN0201. Este servidor conforma la sucursal que se conecta a INTERNET a través de un enlace INFOINTERNET de 128KBPS.

**Site-Quillabamba:** QUIL0201. Este servidor conforma la sucursal que se conecta a INTERNET a través de un enlace INFOINTERNET de 128KBPS.

Estos sites determinan también el esquema de replicación. Cada site posee un servidor que es el encargado de coleccionar los cambios del grupo. Dicho servidor se comunica con cada contraparte de cada site para poder replicar los cambios. Esto hace que la replicación no tenga un cuello de botella

**DNS.** Se han instalado servicios DNS en cada servidor de sucursal sin excepciones. Adicionalmente el Controlador Master de Dominio es decir el servidor ESPN0102, también posee este servicio.

Cada servidor DNS atiende peticiones de miembros o clientes de cada segmento de red. Todos los servidores actualizan la información de las diferentes zonas en forma dinámica. Estos servidores ayudan en el funcionamiento de cada controlador de dominio. Esto significa que cada servidor DNS compara información de sus contrapartes y mantienen una comunicación y asimismo una base de datos única, tanto como para nombres de dominio como para la estructura de directorio activo.

**WINS.** Este servicio ha sido instalado en todos los servidores de sucursales y provincias debido a que la gran mayoría de equipos clientes utilizan como sistema operativo Windows 95. Debido a que este sistema operativo no puede utilizar DNS como medio de resolución de nombres. Es necesario este servicio para poder entregar los nombres correctos.

NOTA: Este servicio solo se debe mantener cuando existan equipos Windows 95. Los equipos de la plataforma Windows 2000 no utilizan este servicio para resolución de nombres.

El servicio maestro WINS esta instalado en el servidor ESPN0102. Este servicio esta encargado de ser el responsable de mantener la relación de nombres mediante la replicación con el resto de servidores. ESPN0102 inicia una sesión de replicación con cada uno de los servidores que tienen este servicio, creándose una topología de replicación estrella. Se ha elegido esta topología a fin de no incrementar el tráfico

Existe un servidor WINS en cada servidor de cada sucursal con la excepción de la sucursal AFLG0201 el cual debido a que está conectado a alta velocidad utiliza el servidor ESPN0102.

Cada servidor WINS solo resuelve nombres del segmento en donde esta instalado. Ello con el fin de evitar el traspaso de los servicios en los enlaces de baja velocidad. Esto quiere decir que un cliente de un segmento de red/sucursal que desea hacer uso de algún servicio lo hace mediante el uso del servidor de la sucursal.

Para mayor información de los parámetros de configuración, por favor vease la ficha técnica de cada servidor.

**DHCP.** Este servicio ha sido instalado también en cada segmento de red/sucursal, y se encarga de administrar las direcciones TCP/IP

Para este caso no es necesario tener un servidor con un servicio DHCP en especial, y no existe comunicación entre los servidores en relación a este servicio. Se han utilizado direcciones de la clase 10.x.x.x las cuales están perfectamente definidas por los estándares TCP/IP para redes internas.

**RRAS.** Este servicio juega un papel sumamente importante en la infraestructura de toda la configuración. Debido a que la interconexión entre sucursales locales se realiza a través de routers en modo BRIDGING. Se ha decidido aislar las redes físicas mediante el uso de 2 adaptadores de red por cada servidor de cada sucursal. Igualmente se utiliza el mismo número de adaptadores de red para el caso de las sucursales de provincias pero en este caso como método para aislar la red interna de la física.

A continuación se determina la tabla final de ruteo.

#### **Servidor ESPN0102 10.0.0.2 Red Interna 10.0.0.0**

##### **Rutas estáticas en Servidor ESPN0102**

<b>Sucursal</b>	<b>Red</b>	<b>Mascara</b>	<b>Gateway</b>	<b>Métrica</b>
WNCH0201	10.0.4.0	255.255.255.0	10.0.0.14	1

Debido a que esta habilitado el IP Forwarding en los servidores de las sucursales locales, una vez alcanzada la red de destino, esta es reenviada por la dirección WAN al adaptador de LAN de sucursal

#### **Rutas estáticas en ABCY0201 10.0.0.13 Red Interna 10.0.3.0**

<b>WAN</b>	<b>Red</b>	<b>Mascara</b>	<b>Gateway</b>	<b>Métrica</b>
LAN-WAN	10.0.0.0	255.255.0.0	10.0.0.13 (*)	1

#### **Rutas estáticas en ANDH0201 10.0.0.16 Red Interna 10.0.6.0**

<b>WAN</b>	<b>Red</b>	<b>Mascara</b>	<b>Gateway</b>	<b>Métrica</b>
LAN-WAN	10.0.0.0	255.255.0.0	10.0.0.16 (*)	1

### Rutas estáticas en QUIL0201 10.0.0.15 Red Interna 10.0.5.0

WAN	Red	Mascara	Gateway	Métrica
LAN-WAN	10.0.0.0	255.255.0.0	10.0.0.15 (*)	1

### Rutas estáticas en SICN0201 10.0.0.17 Red Interna 10.0.7.0

WAN	Red	Mascara	Gateway	Métrica
LAN-WAN	10.0.0.0	255.255.0.0	10.0.0.17 (*)	1

**NOTA:** Nótese la mascara 255.255.0.0 debido a que con este ruteo se alcanzan también las redes internas de las sucursales locales en Cusco.

**VPN.** El componente RRAS es también el responsable de establecer los canales seguros, debido a que estos utilizan RRAS como núcleo de origen y también como definición del tipo de conexión. Mediante este método RRAS inicia una conexión VPN basada en un protocolo seleccionado por el mismo para alcanzar el destino según la red que se esta requiriendo.

Se requiere un usuario del tipo machine para iniciar la conexión en ambos lados y continuación se indica la relación de usuarios creados.

Sucursal	Red	Usuario	Destino
ABCY0201	10.0.3.0	LINKABCY	200.37.212.176
ANDH0201	10.0.6.0	LINKANDH	200.37.212.16
QUIL0201	10.0.5.0	LINKQUIL	200.60.126.144
SICN0201	10.0.7.0	LINKSICN	200.60.74.160
ESPN0102	10.0.0.0	LINKCUSC	200.37.212.243

El proceso de conexión se detalla a continuación. Para ello indicamos un ejemplo de conexión.

Para establecer el túnel seguro entre ABANCAY y CUSCO se requiere una conexión en el servidor ABCY0201 la cual será iniciada por un usuario LINKCUSC. Del mismo modo en Cusco se establece el túnel mediante una conexión inversa la cual será iniciada por el usuario LINKABCY. De esta manera se realiza una doble autenticación de ambos extremos. Cuando la conexión se establece el túnel se habilita y el reenvío de paquetes se concreta.

Es muy importante indicar que Windows 2000 selecciona la ruta más disponible de acuerdo a las tablas de ruteo y las múltiples identidades de los adaptadores de cada uno de los servidores. Esto significa que de acuerdo a la métrica correspondiente se podrá establecer una ruta de un servidor a otro servidor basado en el costo de conexión más pequeño.

El proyecto tuvo tres etapas bien definidas:

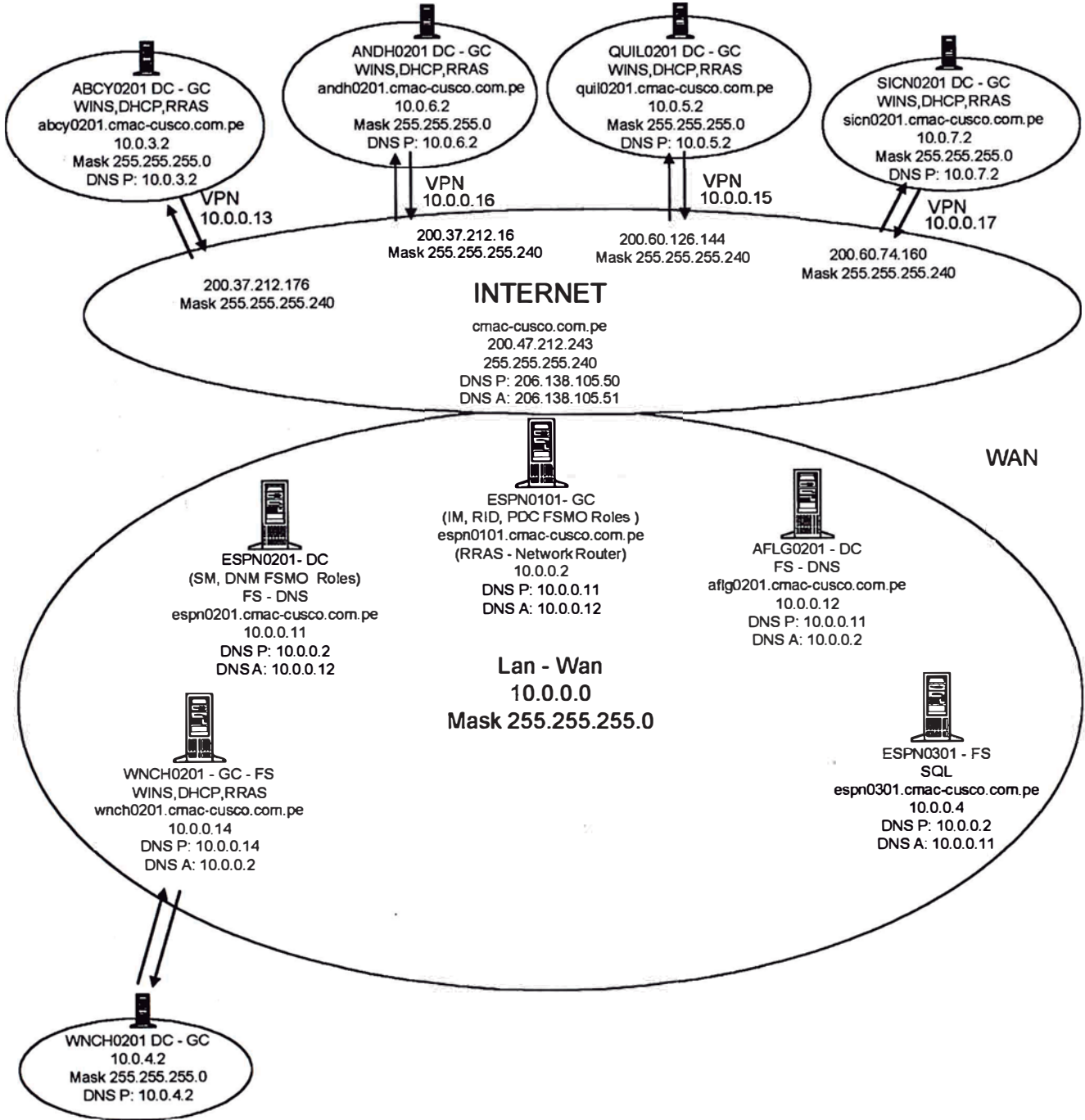
1. Interconexión entre Oficina Principal y las Agencias de Abancay y Andahuaylas
2. Interconexión entre Oficina Principal y el resto de agencias: Sicuani, Quillabamba y Wanchaq
3. Independencia de la interconexión y los servicios de Correo Electrónico e Internet

Para el análisis de los tiempos empleados en la ejecución del proyecto ver cuadro correspondiente en los anexos.

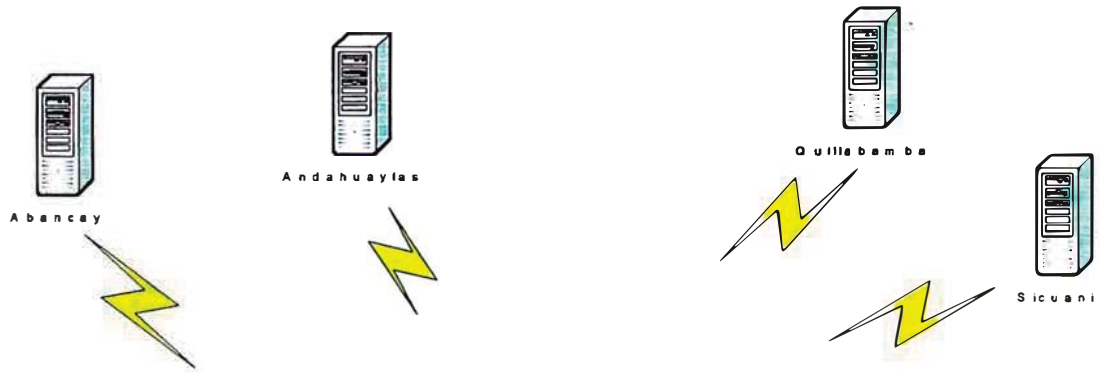
# Caja Municipal Cusco

## Configuración TCP/IP y DNS

### Posicionamiento del Rol FSMO



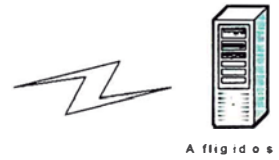




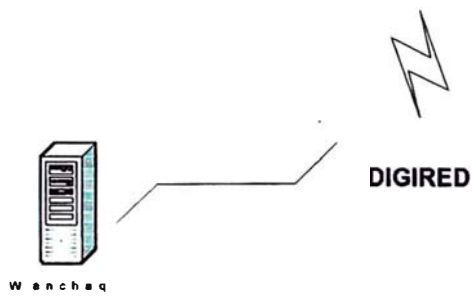
**INTERNET**



**Red Privada**



**Afigidos**



**DIGIRED**

**Wanchaq**

## **CAPITULO IV**

### **COSTOS Y BENEFICIOS**

#### **1. COSTOS REALIZADOS**

Los costos a que dieron lugar este proyecto son:

##### **1. COSTO DE EQUIPOS DE COMUNICACIÓN**

Ver cuadro N° 02 de Costos de equipos en el anexo

##### **2. COSTO DE SERVICIOS DE LINEA DEDICADA**

Ver cuadro N° 03 de Costos de línea dedicada en el anexo

##### **3. COSTO DE SERVICIOS DE ESPECIALISTAS EN COMUNICACIONES**

Trabajos de configuración de routers y  
apoyo de expertos en comunicaciones

US\$ 4500.00

**\* incluido IGV**

##### **4. COSTO TOTAL INVERTIDO**

* Equipos de comunicación	US\$ 22,644.84
* Instalación de líneas dedicadas	US\$ 4,956.00
* Contratación de especialistas	US\$ 4,500.00

**TOTAL INVERSIÓN**

**US\$ 32,100.84**

## **2. BENEFICIOS**

### **2.1. A NIVEL DE COSTOS FIJOS**

- Inversión bastante menor en comparación a los costos brindados por los proveedores de estos mismos servicios.
- Reducción significativa de costos por llamadas telefónicas a nivel de todas las agencias de la institución como si fueran anexos.
- Traslado significativo de los costos telefónicos por llamadas remotas a los costos por operaciones por transmisión de datos

### **2.2. A NIVEL INSTITUCIONAL**

- Significativa mejora en el Servicio y Atención al Cliente de la institución que se refleja inmediatamente en las ventanillas de atención al tener información en tiempo real en todos los servicios, reduciendo el tiempo de 30' a 45' en una operación financiera entre una agencia y otra a solo 45" a 1.30' en los peores casos.
- Se eleva la Imagen institucional
- Mejora la Calidad de atención al Cliente en todas las áreas financieras y administrativas de la institución por contar con información en tiempo real.
- Obtención de una mejor calificación financiera por parte de los organismos reguladores.

### **2.3. A NIVEL TECNICO**

- Fortalece la implementación y equipamiento informático de la institución
- Estructura de una red privada virtual de voz y datos a nivel de toda la institución escalable.
- Reordenamiento de procesos técnicos en el tratamiento de la información ON-LINE
- Brindar un mejor soporte técnico a toda la institución en tiempo real.

### **2.4. ESTABLECE UNA METODOLOGIA**

- Para la administración de instalación de una nueva agencia
  - i. Procesos de adquisición de equipos y recursos
  - ii. Manejo de costos promedios para los presupuestos de inversión a futuras agencias
  
- Para la instalación técnica de una nueva agencia
  - i. Solicitud de requerimiento de línea dedicada
  - ii. Equipos de comunicación necesarios
  - iii. Costos de instalación
  - iv. Procedimiento técnicos para la operatividad de la agencia y su conexión a la red actual de la institución

## **CAPITULO V**

### **CONCLUSIONES Y RECOMENDACIONES**

Podemos mencionar las siguientes conclusiones y recomendaciones:

- Para el desarrollo del presente proyecto debe estandarizarse toda la plataforma informática de la institución con un mismo Sistema Operativo. Para este caso en particular se optó por la plataforma Microsoft con sus productos: Windows 2000 Server en los servidores, Exchange 2000 para correo e Internet, ISA Server para los FireWall y el Windows 2000 Professional o Windows 98 en las estaciones de trabajo.
- La tecnología de tuneles seguros (VPN) utilizada es una solución Microsoft para el tipo de redes virtuales privadas basadas en redes públicas.
- Los enlaces son del tipo Infointernet proporcionados por Telefónica Data y enlaces DIGIRED proporcionado por Telefónica Del Perú.
- El proveedor de los enlaces debe certificar su viabilidad técnica en los puntos donde se desee instalar una agencia remota.
- Se debe tener bien definidos los requerimientos de hardware para esta solución: Servidores, routers, anexos telefónicos de la central y memorias.

- Debemos definir el ancho de banda idóneo del enlace para el uso de la voz y data en función del tráfico de información existente en la institución y así determinar los costos fijos que se van a asumir a partir de su instalación. En este proyecto hemos optado por 32 Kbps para voz y 96 Kbps para la data.
- Para fortalecer las políticas de seguridad informática es necesario contar con un software antivirus adicional a los FireWall instalados.
- Contar con expertos en comunicaciones y configuración de routers para fortalecer el Soporte Técnico de la nueva arquitectura instalada.
- Realizar periódicamente monitoreos y estadísticas de las transacciones de voz y data en la red para establecer un adecuado ancho de banda y garantizar la performance en las comunicaciones.
- La arquitectura instalada permite y garantiza una escalabilidad informática a bajo costo en los ámbitos territoriales donde se requiera una nueva agencia remota y que el proveedor del enlace tenga las condiciones técnicas para brindarlo.
- El presente proyecto ha permitido elevar significativamente la atención y servicios a los clientes en todas las agencias de la CMAC Cusco S.A. Asimismo, ha posibilitado que la institución obtenga información centralizada de todas sus agencias en tiempos reducidos, lo cual se ha plasmado en la obtención de una buena calificación financiera por parte de los organismos reguladores, facilitando de esta manera la cobertura de nuevos mercados para brindar nuestros servicios financieros.

## **BIBLIOGRAFÍA**

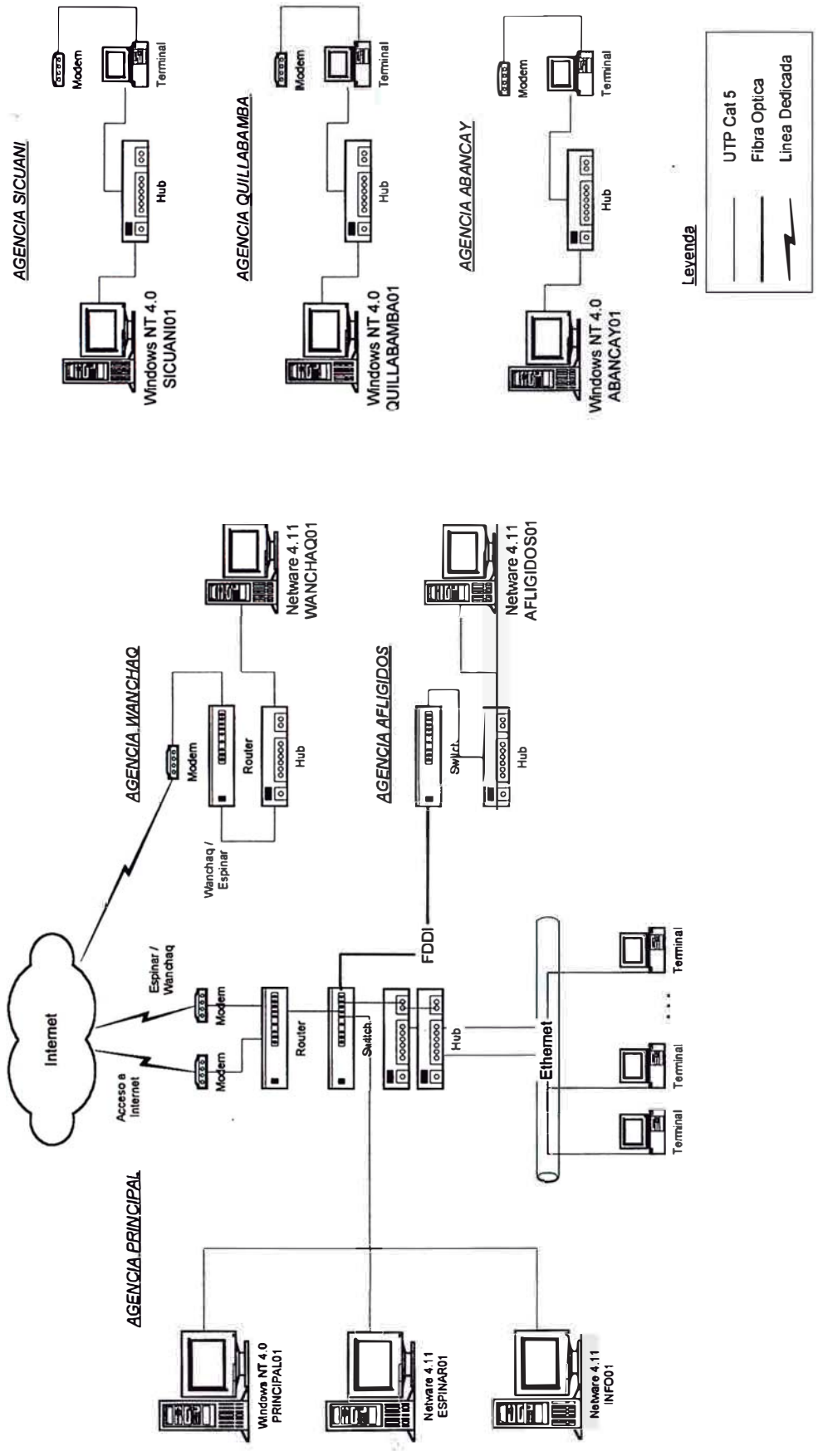
- Windows 2000 Server
- Exchange 2000
- ISA Server
- Instalación y Configuración de McAfee Antivirus
- Windows 2000 VPN Overview

## **ANEXOS**



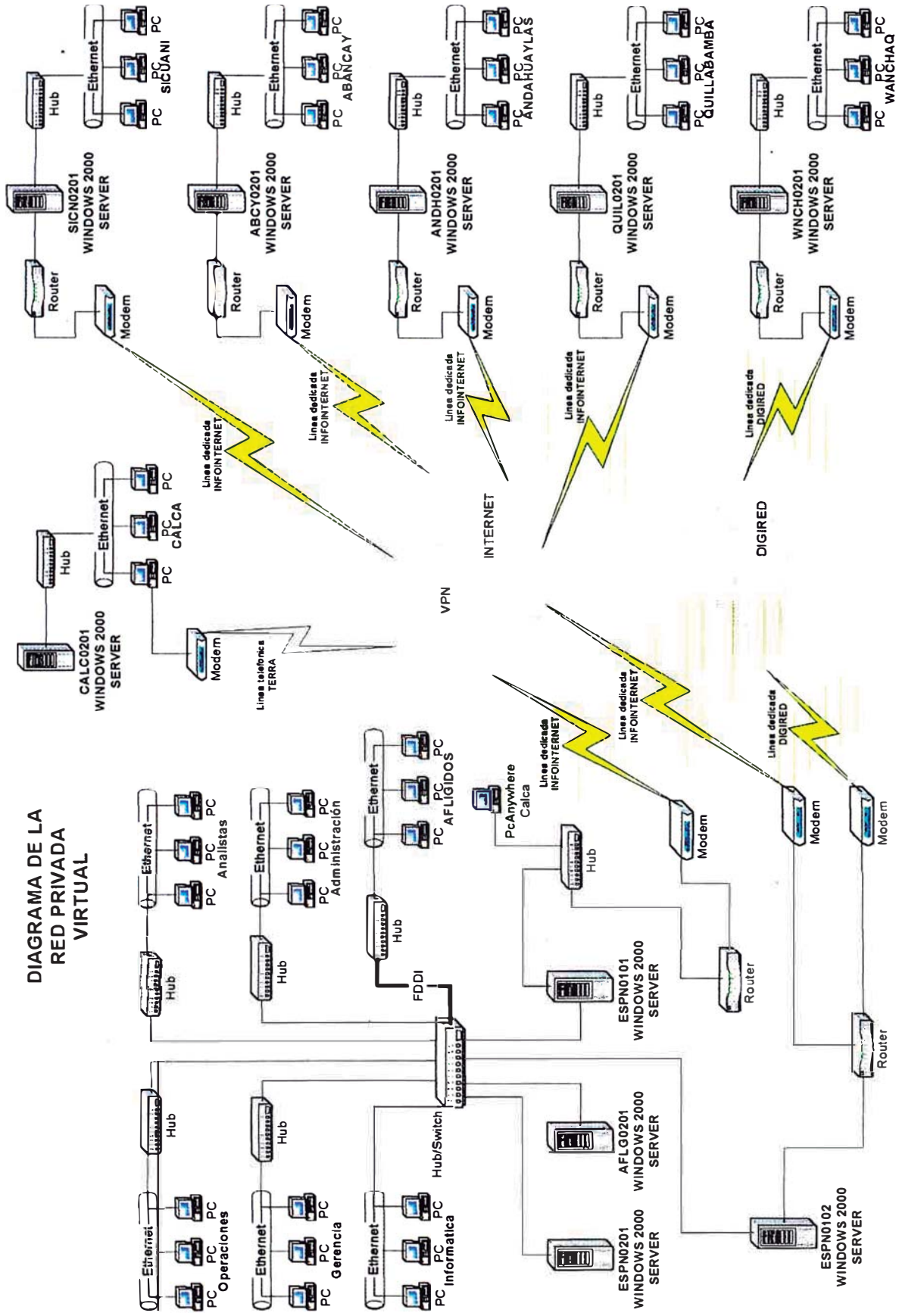
**DIAGRAMA ANTIGUO  
DE LA RED EN LA CMAC CUSCO S.A.**

# MAPA DE RED ANTIGUO CMAC-CUSCO



**DIAGRAMA ACTUAL**  
**DE LA RED PRIVADA EN LA CMAC CUSCO S.A.**

# DIAGRAMA DE LA RED PRIVADA VIRTUAL



**CUADRO N° 01**  
**ALTERNATIVAS TECNOLÓGICAS EN LA SOLUCIÓN PARA LAS CONEXIONES DE AGENCIAS**

Proveedor	Tipo de Enlace	Costos Instalación por punto	Costos Mensual por punto	Factibilidad	Tiempo de Instalación	Tipo de Red	Seguridad
<b>IMPSTAT</b>	<b>SATELITAL TIPO MALLA</b> Velocidad: 64 Kbps Voz: 02 canales Privado	\$4,130.00	\$2,246.72	Sistema CMAC's Proyecto Piloto (05 Cajas)	60 días	Privada	Si
<b>Telefónica del Perú</b>	<b>DIGIRED</b> Velocidad: 128 Kbps Local Velocidad: 64 Kbps Nac. Rango A Velocidad: 128 Kbps Nac. Rango A	\$1,416.00 \$2,950.06	\$555.78 \$1,272.96	100% 100%	30 días 30 días	Privada	Si
<b>Telefónica Data ( * )</b>	<b>INFOINTERNET</b> Velocidad: 64 Kbps Velocidad: 128 Kbps	\$708.00 \$708.00	\$355.18 \$582.92	100% 100%	30 días 30 días	Pública	No

**CUADRO N° 02 : COSTO DE EQUIPOS**

CANT	DESCRIPCION	COSTO		Disponi- bilidad
		UNITARIO	TOTAL	
	<b>Memorias</b>			
2	Memoria 128MB Kington, Proliant 3000 KTC9023/128	\$ 279.65	\$ 559.30	P/10dias
2	Memoria de 256MB Kington Proliant 800 6/550 KTC3614/256	\$ 206.80	\$ 413.60	P/10dias
1	Memoria de 128MB Kington Proliant 1600 6/600 KTC3614/128	\$ 131.60	\$ 131.60	Stock
1	Memoria de 128MB Kington Proliant 800 6/550 KTC3614/128	\$ 131.60	\$ 131.60	Stock
	<b>Equipos Sede Principal</b>			
1	Router Cisco 2610 Ethernet modular Router w/Cisco IOS IP Softwaree	\$ 1,930.00	\$ 1,930.00	Stock
1	Tarjeta NM-2V= Two Slot Voice/fax Network Module-Spare, conexión WAN, 2 Slots de Voz, 1 Fax	\$ 1,644.44	\$ 1,644.44	Stock
1	Cable WAN	\$ 95.56	\$ 95.56	Stock
2	VIC-2FXO Two-port Interface Card -FXO-Spare	\$ 386.67	\$ 773.33	20 dias
	<b>TOTAL SEDE PRINCIPAL</b>		<b>\$ 5,679.43</b>	
	<b>Equipos Sede de Agencia</b>			
5	Router Cisco 1750-2V 10/100 Modular Router w/2 Voice Channels, IOS IP/VOICE	\$ 2,220.00	\$ 11,100.00	20 dias
5	Tarjeta VIC-FXS 2 puertos de voz	\$ 386.67	\$ 1,933.33	20 dias
5	Cable WAN	\$ 95.56	\$ 477.78	Stock
	<b>TOTAL SEDE AGENCIA</b>		<b>\$ 13,511.11</b>	
	<b>SUB-TOTAL GENERAL</b>		<b>\$ 19,190.54</b>	
	<b>IGV</b>		<b>3,454.30</b>	
	<b>TOTAL GENERAL</b>		<b>\$ 22,644.84</b>	

### CUADRO N° 03: COSTO DE INSTALACION DE LINEAS DEDICADAS

#### **COSTO DE INSTALACION DE LINEAS DEDICADAS**

<b>CANTIDAD</b>	<b>UBICACIÓN</b>	<b>COSTO INSTALACION POR PUNTO</b>	<b>TOTAL</b>
1	Sede Principal	\$708.00	\$708.00
4	Agencias Provincia	\$708.00	\$2,832.00
1	Agencia Wanchaq	\$1,416.00	\$1,416.00
<b>COSTO TOTAL</b>			<b>\$4,956.00</b>
* Pago único e Incluido IGV			

#### **COSTO MENSUAL POR SERVICIO DE TRANSMISION**

<b>CANTIDAD</b>	<b>UBICACIÓN</b>	<b>ANCHO DE BANDA</b>	<b>COSTO</b>
1	Sede Principal	256 Kbps - Infointernet	\$1,054.92
1	Sede Principal	64 Kbps - Infointernet	\$355.18
1	Abancay	128 Kbps - Infointernet	\$623.04
1	Andahuaylas	128 Kbps - Infointernet	\$623.04
1	Quillabamba	128 Kbps - Infointernet	\$623.04
1	Sicuani	64 Kbps - Infointernet	\$376.42
1	Agencia Wanchaq	128 Kbps - DIGIRED	\$555.78
<b>COSTO TOTAL</b>			<b>\$4,211.42</b>
* Pago Mensual e Incluido IGV			

#### **COSTO MENSUAL POR LLAMADAS TELEFONICAS REMOTAS**

<b>CANTIDAD</b>	<b>UBICACIÓN</b>	<b>COSTO PROMEDIO NUEVOS SOLES</b>	<b>COSTO US\$</b>
1	Sede Principal	S/. 4,000.00	\$1,126.76
7	Agencias	S/. 12,600.00	\$3,549.30
<b>COSTO PROMEDIO MENSUAL</b>			<b>\$4,676.06</b>
* Pago Mensual por llamadas telefónicas e Incluido IGV			

**PLAN DE ACTIVIDADES REALES PARA EL PROYECTO DE INTERCONEXION DE LA CMAAC CUSCO S.A. - 2001/2002**

ACTIVIDADES	2001		2002																		
	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
<b>1. Proyecto de Interconexión entre Agencias</b>																					
1.1. Análisis de Alternativas																					
1.2. Elaboración del Proyecto																					
1.3. Presentación del Proyecto																					
1.4. Aprobación del Proyecto 1ra Etapa. Abancay y Andahuaylas																					
2. Proceso de adquisición de Equipos de Comunicación																					
2.1. Buena pro y Compra de equipos																					
3. Proceso de contacto con Experto Solución Proveedor Microsoft																					
3.1. Selección y Contrato del experto																					
4. Ejecución del proyecto en su Primera Etapa																					
4.1. Revisión del Plan de trabajo y ajustes de actividades																					
4.2. Solicitud de enlaces Intranet para Abancay y Andahuaylas																					
4.3. Instalación de enlaces en Abancay y Andahuaylas																					
4.4. Trabajo/Adecuación Oficina Principal al VPN y definición del TUNEL																					
4.5. Verificación de enlaces operativos 100%																					
4.6. Trabajo Adecuación Agencia Abancay al VPN, TUNEL y Voz																					
4.7. Trabajo Adecuación Agencia Andahuaylas al VPN, TUNEL y Voz																					
4.8. Adecuación de Software Financiero para Interconexión																					
4.8. Verificación de Enlaces del Software Financiero y VPN																					
4.10. Oficina Principal, Abancay y Andahuaylas con VPN Voz y Data																					
5. Fin de proyecto en su primera etapa																					
6. Proyecto de Interconexión 2da. Etapa. Quillabamba y Sicuani																					
6.1. Aprobación del Proyecto 2da Etapa																					
7. Proceso de adquisición de Equipos de Comunicación																					
7.1. Buena pro y Compra de equipos																					
8. Ejecución del proyecto en su Segunda Etapa																					
8.1. Revisión del Plan de trabajo y ajustes de actividades																					
8.2. Solicitud de enlaces Intranet para Quillabamba y Sicuani																					
8.3. Instalación de enlace en Quillabamba																					
8.4. Verificación de enlace Quillabamba operativo 100%																					
8.5. Trabajo Adecuación Agencia Quillabamba al VPN, TUNEL y Voz																					
8.6. Adecuación de Software Financiero para Interconexión																					
8.7. Verificación de Enlaces del Software Financiero y VPN																					
8.8. Agencia Quillabamba con VPN Voz y Data																					
8.3. Instalación de enlace en Sicuani																					
8.4. Verificación de enlace Sicuani operativo 100%																					
8.5. Trabajo Adecuación Agencia Sicuani al VPN, TUNEL y Voz																					
8.6. Adecuación de Software Financiero para Interconexión																					
8.7. Verificación de Enlaces del Software Financiero y VPN																					
8.8. Agencia Sicuani con VPN Voz y Data																					
9. Ajustes y Estabilidad de la Red Interconectada																					
9.1. Ajuste al Software Financiero para operaciones con Quillabamba																					
9.2. Solicitud de Cambio de Ancho de Banda Agencia Quillabamba																					
9.3. Cambio de Ancho de Banda Agencia Quillabamba																					
9.4. Ajuste al Software Financiero para operaciones con Quillabamba																					
10. Estabilidad Software Financiero para operaciones con Quillabamba																					
10.1. Estabilidad Óptima del Sistema Financiero Interconectado																					
10.2. Institución totalmente interconectada al VPN, TUNEL y Voz																					
11. Agencia Wanchaq. Cambio Radio Enlace a la Red Actual																					
11.1. Aprobación de Gerencia																					
11.2. Solicitud de enlace DIGIRED para Wanchaq																					
11.3. Instalación de enlace en Wanchaq																					
11.4. Verificación de enlace Wanchaq operativo 100%																					
11.5. Trabajo Adecuación Agencia Wanchaq al TUNEL y Voz																					
11.6. Adecuación de Software Financiero para Interconexión																					
11.7. Verificación de Enlaces del Software Financiero y VPN																					
11.8. Agencia Wanchaq a la red con Voz y Data																					
12. Mejoramiento de la Red Interconexión e Intranet y Correo Electrónico																					
12.1. Aprobación de Gerencia																					
12.2. Solicitud de nuevo enlace INFOINTERNET para Correo e Intranet																					
12.3. Instalación de nuevo enlace en Oficina Principal																					
12.4. Verificación de nuevo enlace operativo 100%																					
12.5. Trabajo Adecuación nuevo enlace y nuevo DNS																					
12.6. Verificación del nuevo enlace y servicios de Intranet y Correo																					
13. Red de la CMAACUSCO S.A. completamente instalada con mejoras																					

\* Los tiempos reflejan las fechas reales en las cuales se ejecutaron estas actividades