ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

PROPUESTA TÉCNICA ECONÓMICA PARA LA IMPLANTACIÓN DE UNA INTERRED SEGURA PARA SOPORTE DE APLICACIONES E-BUSINESS PARA EMPRESAS MEDIANAS DE AGUA POTABLE

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN REDES DE INFORMACIÓN

CABEZAS SÁNCHEZ SANDRA PATRICIA

sandra.cabezas@leveltech.com.ec

DIRECTOR: ING. JUAN HERRERA, MSc.

Juan.herrera@leveltech.com.ec

Quito, Septiembre 2009

DECLARACIÓN

Yo Sandra Patricia Cabezas Sánchez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Sandra Patricia Cabezas Sánchez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Sandra Patricia Cabezas Sánchez, bajo mi supervisión.

Ing. Juan Herrera, Msc.

DIRECTOR DE PROYECTO

DEDICATORIA

A mis amados padres Ruth y Eduardo que con su inmenso amor me enseñaron principios de vida y con sus sabios consejos me guiaron para culminar con este objetivo.

A mis queridos hermanos James, Henry, John, Charles, Mónica y Ruth que con su ejemplo de lucha me enseñaron que todo se consigue en base al esfuerzo, sacrificio y dedicación.

Sandra

AGRADECIMIENTOS

A Dios, que me dio la vida y gracias a El tuve el ánimo y fuerza suficientes a través de mi familia para concluir con este objetivo.

A mis padres, Ruth y Eduardo por su amor, comprensión y aliento en esta etapa de mi vida.

A mis amigos, quienes desinteresadamente aportaron su conocimiento y experiencia para terminar este proyecto; en especial a Fernando y Diego Padilla. Gracias amigos.

Al Ing. Juan Herrera S., porque gracias a sus consejos nunca me dejó desmayar y me enseñó que a pesar de las dificultades siempre existe una oportunidad de surgir y encontrar un camino para llegar al éxito.

Sandra

CONTENIDO

DECLARACIÓN _____ *i*

CERTIFICACIÓN _____ *ii*

DEDICATORIA _____ *iii*

AGRADECIMIENTOS _____ *iv*

CONTENIDO _____ *v*

CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA _____ *1*

1.1 DESCRIPCIÓN DEL PROBLEMA _____ **1**

1.2 JUSTIFICACIÓN DEL DISEÑO _____ **3**

CAPÍTULO 2. DISEÑO DE LA INTERRED E INTRANET SEGURA _____ *5*

2.1 ANÁLISIS DE LA INFRAESTRUCTURA ACTUAL DE RED DE EMPRESAS MEDIANAS DE AGUA POTABLE _____ **5**

2.1.1 SITUACIÓN ACTUAL DE LAS EMPRESAS MEDIANAS DE AGUA POTABLE _____ 5

2.2 ANÁLISIS DE REQUERIMIENTOS DE INTERRED E INTRANET _____ **12**

2.2.1 ANÁLISIS DE REQUERIMIENTOS DE CORREO ELECTRÓNICO _____ 12

2.2.2 ANÁLISIS DE REQUERIMIENTOS DE LA APLICACIÓN E-BUSINESS _____ 14

2.2.3 CONECTIVIDAD ENTRE MATRIZ Y AGENCIAS _____ 15

2.3 DETERMINACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INTERRED E INTRANET _____ **16**

2.3.1 OBJETIVO _____ 17

2.3.2 ALCANCE _____ 17

2.3.3 RESPONSABILIDAD _____ 17

2.3.4 POLÍTICAS DE CUENTAS DE USUARIO Y CLAVES _____ 17

2.3.5 POLÍTICAS DE SEGURIDAD PARA ESTACIONES DE TRABAJO _____ 19

2.3.6 POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES _____ 22

2.3.7 POLÍTICAS DE SEGURIDAD PARA REDES _____ 24

2.3.8 POLÍTICAS DE BACKUP _____ 27

2.3.9 POLÍTICAS DE COMPRA, CONTROL Y ADMINISTRACIÓN DE ANTIVIRUS _____ 28

2.3.10 POLÍTICAS DE SEGURIDAD LÓGICA _____ 31

2.4 REDISEÑO DE LAS REDES LAN Y WAN DE EMPRESAS MEDIANAS DE AGUA POTABLE ___ 33

2.4.1 CONSIDERACIONES DE REDISEÑO DE LAS REDES LAN ___ 33

2.4.2 CONSIDERACIONES DE REDISEÑO DE LA RED WAN ___ 36

2.5 DISEÑO DE LA INTERRED E INTRANET PARA APLICACIONES E-BUSINESS ___ 38

2.5.1 SEGURIDAD ___ 38

2.5.2 FUNCIONALIDAD DE LA APLICACIÓN E-BUSINESS ___ 39

2.5.3 DISEÑO DE LA INTERRED E INTRANET ___ 40

CAPÍTULO 3. DISEÑO DE LA ARQUITECTURA VPN ___ 42

3.1 ANÁLISIS DE REQUERIMIENTOS PARA LA VPN ___ 42

3.1.1 VENTAJAS ___ 42

3.1.2 CARACTERÍSTICAS ___ 43

3.1.3 NECESIDADES DE LA EMPRESA ___ 43

3.1.4 USUARIOS DE LA VPN ___ 44

3.1.5 RESTRICCIONES ___ 44

3.1.6 REQUERIMIENTOS DE HARDWARE ___ 45

3.1.7 REQUERIMIENTOS DE SOFTWARE ___ 46

3.2 ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD PARA APLICACIONES E-BUSINESS ___ 46

3.2.1 SEGURIDAD DE CONTROL DE ACCESO ___ 46

3.2.2 ENCRIPTACIÓN DE CLAVE ___ 48

3.2.3 COMUNICACIONES VÍA INTERNET ___ 49

3.3 ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD PARA LA EMPRESA PROVEEDORA DE SERVICIOS DE INTERNET ___ 50

3.4 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD PARA LA VPN ___ 51

3.4.1 OBJETIVO ___ 52

3.4.2 ALCANCE ___ 52

3.4.3 RESPONSABILIDAD ___ 52

3.4.4 POLÍTICAS DE SEGURIDAD ___ 52

3.5 ANÁLISIS DE COSTOS DE EMPRESAS PROVEEDORAS DE SERVICIOS DE INTERNET ___ 53

3.5.1 CONSIDERACIONES ___ 53

3.5.2 ANÁLISIS DE COSTOS ___ 54

3.6 DISEÑO DE LA ARQUITECTURA VPN PARA SOPORTE REMOTO A LAS APLICACIONES E-BUSINESS ___ 60

CAPÍTULO 4. PREPARACIÓN DE LA PROPUESTA TÉCNICA ECONÓMICA PARA UNA INTERRED SEGURA ____ *62*

4.1 COMPARACIÓN DE PROVEEDORES DE HARDWARE, SOFTWARE Y COMUNICACIONES __ **62**

4.1.1 PARÁMETROS DE CALIFICACIÓN DE CALIDAD ____ 62

4.1.2 PROVEEDORES DE HARDWARE ____ 63

4.1.3 PROVEEDORES DE SOFTWARE ____ 67

4.1.4 PROVEEDORES DE COMUNICACIONES ____ 68

4.2 ANÁLISIS DE COSTOS Y ALTERNATIVAS DE HARDWARE, SOFTWARE Y COMUNICACIONES ____ **70**

4.2.1 ALTERNATIVAS DE HARDWARE ____ 70

4.2.1.1 Antenas ____ 70

4.2.2 ALTERNATIVAS DE SOFTWARE ____ 73

4.2.3 ALTERNATIVAS DE COMUNICACIONES ____ 76

4.3 ANÁLISIS FINANCIERO PARA ELABORAR LA PROPUESTA TÉCNICA ECONÓMICA ____ **77**

4.3.1 ANÁLISIS FINANCIERO PARA UNA INFRAESTRUCTURA DE INTERRED CON ENLACES WIRELESS _ 77

4.3.2 ANÁLISIS FINANCIERO PARA UNA INFRAESTRUCTURA DE INTERRED CON ENLACES DEDICADOS A TRAVÉS DE INTERNET ____ 82

4.3.3 ANÁLISIS DE LAS SOLUCIONES ____ 83

4.4 ANÁLISIS DE COSTO BENEFICIO DE LA MEJOR PROPUESTA ____ **85**

4.4.1 HARDWARE ____ 85

4.4.2 SOFTWARE ____ 86

4.4.3 COMUNICACIONES ____ 86

4.4.4 BENEFICIO DE LA MEJOR PROPUESTA ____ 87

4.5 GENERACIÓN DEL DOCUMENTO PROPUESTA TÉCNICA ECONÓMICA ____ **88**

4.5.1 OBJETIVOS ____ 89

4.5.2 ALCANCE ____ 89

4.5.3 BENEFICIOS ____ 90

4.5.4 INFRAESTRUCTURA TÉCNICA REQUERIDA ____ 90

4.5.5 DISEÑO DE LA INTERRED ____ 91

4.5.6 FACTORES DE ÉXITO ____ 92

4.5.7 PLAZO DE IMPLANTACIÓN ____ 92

4.5.8 COSTO DE LA INVERSIÓN ____ 93

4.5.9 SOPORTE TÉCNICO ____ 93

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES ____ *94*

5.1 CONCLUSIONES ____ **94**

5.2 RECOMENDACIONES ____ **96**

BIBLIOGRAFÍA ____ *102*

ANEXO 1: PROVEEDORES DE SERVICIOS DE INTERNET AUTORIZADOS EN EL ECUADOR105

ANEXO 2: DATOS DE CUENTAS DE USUARIO POR PERMISIONARIO (ISP) ____ *119*

ANEXO 3: DECRETO 1014 ____ *122*

ANEXO 4: ESPECIFICACIONES TÉCNICAS DE EQUIPOS ____ *125*

ANEXO 5: PROFORMAS ____ *136*

INDICE DE FIGURAS

Figura 2.1 Configuración Física de la Matriz de la Empresa de Agua Potable 9

Figura 2.2 Configuración Física de las Redes LAN en las Agencias de Agua Potable sin conexión a la Matriz 10

Figura 2.3 Diseño de la Interred e Intranet Segura para aplicaciones E-Business..... 41

Figura 3.1 Arquitectura VPN para Soporte de Aplicaciones E-Business..... 61

Figura 4.1 Diseño de la Interred para la Empresa de Agua Potable..... 91

Figura 4.2 Diseño de la VPN con comunicación al Proveedor de la aplicación E-Business..... 92

INDICE DE TABLAS

Tabla 2.1 Características de los Computadores de la Red Física Actual 7
Tabla 2.2 Listado de Impresoras de la Red Actual 8
Tabla 2.3 Equipos de Comunicación de la Red Actual 8
Tabla 2.4 Requerimientos de Hardware para Internet Explorer 7.0 y Mozilla FireFox 13
Tabla 3.1 Requisitos de Hardware para Instalar Client VPN 45
Tabla 3.2 Calidad de Servicio de los Proveedores de Internet en Ambato 55
Tabla 3.3 Costos de Acceso a Internet ADSL- Andinanet 56
Tabla 3.4 Costos de Acceso a Internet ADSL - Telconet 57
Tabla 3.5 Costos de Acceso a Internet Cable MODEM - TV Cable 57
Tabla 3.6 Costos de Acceso a Internet ADSL - Interactive 58
Tabla 3.7 Costo de Acceso a Internet ADSL - Porta 58
Tabla 4.1 Esquema Comparativo de Proveedores de Hardware de Comunicaciones 66
Tabla 4.2 Proveedores de Software para Empresas de Agua Potable 68
Tabla 4.3 Proveedores de Internet en Ecuador 69
Tabla 4.4 Costos de Antenas de 12, 14 y 15 dbi 71
Tabla 4.5 Costos de Access Point 2.4 Ghz 72
Tabla 4.6 Costos de Radios 72
Tabla 4.7 Costos de Firewall / Gateway 73
Tabla 4.8 Costos de Licencias de Antivirus por Año 75
Tabla 4.9 Costo de Software para el Servidor de la aplicación E-Business 75
Tabla 4.10 Costo de Enlace Dedicado por mes 76
Tabla 4.11 Costos de Implementación de Infraestructura de Interred Propia con enlaces Wireless 79
Tabla 4.12 Proyección del Costo de Infraestructura Propia con enlaces Wireless 80
Tabla 4.13 Costo Mensual por arrendamiento de la Infraestructura de Interred 81
Tabla 4.14 Proyección a 3 años del Costo por Arrendamiento de Infraestructura de Interred 82
Tabla 4.15 Costos de Enlaces Dedicados 83
Tabla 4.16 Proyección del Costo por Enlace Dedicado a 3 años 83
Tabla 4.17 Comparación de Costos de las Soluciones con Proyección a 3 años 84
Tabla 4.18 Costo Total del Proyecto 85
Tabla 4.19 Costos de Hardware para calcular la mejor propuesta 86
Tabla 4.20 Costos de Software para calcular la mejor propuesta 86
Tabla 4.21 Porcentaje de Ahorro por Implementación de una Infraestructura de Interred con enlaces wireless Propia respecto de las otras soluciones proyectado a 3 años 88

RESUMEN

El presente proyecto se orienta al diseño de una infraestructura de Interred segura para Empresas medianas de Agua Potable y su soporte para aplicaciones E-Business, que incluye la definición de políticas de seguridad para su operación.

Tiene por objetivo preparar una Propuesta Técnica y Económica para la adquisición de una arquitectura de operación para empresas medianas de Agua Potable. La arquitectura contempla la interconexión con un proveedor de servicios de la aplicación E-Business a través de una VPN.

El primer capítulo presenta la descripción de la problemática actual de las empresas de Agua Potable y su justificación para la implementación de una infraestructura de Interred segura.

En el segundo capítulo se realiza un análisis de la situación actual de los recursos informáticos en los ámbitos físico y lógico. Se realiza un análisis de los requerimientos de Interred e Intranet, se determina las políticas de seguridad para su operación. Además, se realiza el rediseño de las redes LAN y WAN como apoyo para la comunicación de la Matriz y Agencias, con el fin de obtener información actualizada y en línea, y se propone el esquema de diseño de la Interred e Intranet para aplicaciones E-Business.

En el tercer capítulo se realiza el análisis de requerimientos, definición de políticas de seguridad para el diseño de una arquitectura VPN para que la Compañía proveedora de la aplicación E-Business brinde soporte a la aplicación. Adicionalmente se determinan los requerimientos de seguridad que debe cumplir la aplicación E-Business e incluye los costos de acceso a servicios de Internet como análisis preliminar a la propuesta Técnica Económica a generar.

El capítulo cuarto considera los aspectos físicos y económicos que implican en la preparación de la Propuesta Técnica Económica para una Interred segura.

Se finaliza en el quinto capítulo con las Conclusiones y Recomendaciones.

CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

“Cada día la tecnología avanza más, es importante utilizarla a ésta como aliada que permita integrar todos los procesos de negocio, sean estos administrativos, financieros, comerciales y técnicos en una sólida estructura que brinde información consolidada y oportuna a las diferentes áreas de negocio de las Empresas de Agua Potable y Alcantarillado.

Una de las principales debilidades de las Empresas Medianas de Agua Potable y Alcantarillado es no disponer de procesos debidamente formalizados, automatizados e integrados, razón por la cual, la toma de decisiones en la alta Gerencia se torna un problema. Es muy común disponer de información aislada, en varios reportes de diferentes aplicaciones y el gran reto para el negocio es cómo integrar toda esa información para brindar un mejor servicio a sus clientes.

Una vez que las Empresas Medianas de Agua Potable y Alcantarillado hayan automatizado y optimizado sus procesos de negocio, éstas serán más competitivas y podrán realizar mayores inversiones en redes de expansión e instalación de nuevos clientes. De ahí la importancia de disponer de un Sistema Informático Integrado que apoye la gestión operativa de las Empresas.

Actualmente, Empresas Medianas de Agua Potable y Alcantarillado de nuestro país ya se encuentran automatizando sus procesos de negocio, como son:

- EMAPA – Ibarra
- EMAPA – Ambato
- EAPA SAN MATEO – Esmeraldas
- EMAPAD - Durán

Entre las principales".[1]

Otra debilidad de las Empresas Medianas de Agua Potable y Alcantarillado, es no disponer de una Infraestructura de red, robusta y segura que permita mantener la conectividad y concatenar toda la información generada durante su actividad en toda la organización.

Las Empresas Medianas de Agua Potable y Alcantarillado con la finalidad de dar un mejor servicio de recaudación al cliente, se han orientado a abrir sucursales con su propio diseño de red LAN; generando la necesidad de comunicación entre éstas y la Matriz; sin embargo, la inversión en comunicación informática para soporte de la infraestructura entre la Matriz y sus Sucursales es limitada.

Por otro lado, la tendencia del desarrollo de las aplicaciones informáticas se orienta a la utilización de los conceptos E-Business que integre los procesos de negocio previamente definidos, optimizados y automatizados en un Sistema Informático Integrado; esto implica que debe existir una infraestructura de red segura que las soporte para su operación.

En el caso de las empresas medianas de Agua Potable, se está optando por este tipo de aplicaciones, pero no cuentan con la infraestructura adecuada para su operación, lo que ocasiona que la información generada en las sucursales no llegue a tiempo a la Matriz y exista inconsistencia en la información, debido a que no se actualiza de forma inmediata; de ahí la necesidad de definir enlaces WAN para la comunicación entre sucursales y la Matriz, en una ciudad determinada.

La infraestructura operativa apropiada para correr aplicaciones E-Business debe contar con políticas de seguridad que protejan la información generada de intrusos internos y externos a la organización.

---

[1] HERRERA, Juan, ¿Cómo fortalecer tecnológicamente a las empresas de Agua Potable y Alcantarillado?, ANDESAPA, No.1, julio 2008.

El objetivo de esta Tesis, es proporcionar una propuesta técnica y económica para implementar una Interred segura para soporte de aplicaciones E-Business en Empresas de Agua Potable y Alcantarillado medianas.

1.2 JUSTIFICACIÓN DEL DISEÑO

Las Empresas de Agua Potable y Alcantarillado medianas tienen procesos similares, aunque cada una tiene su propia forma de operar y gestionar los mismos procesos.

Una vez definidos, optimizados y automatizados sus procesos de negocio en una aplicación E-Business (Sistema) que los integre, las empresas medianas de Agua Potable y Alcantarillado serán más competitivas y con la posibilidad de incrementar sus inversiones para ampliar el negocio.

Las ventajas de la implementación y optimización de los procesos de negocio en aplicaciones E-Business son:

- Reducción de costos
- Nuevos canales de venta y recaudación
- Disminución de tiempos de proceso
- Reasignación de personal a actividades de análisis de información

Con la Integración de procesos, las empresas medianas de Agua Potable y Alcantarillado obtendrán información oportuna y real de los datos de cada proceso a través de reportes.

Las empresas medianas de Agua Potable y Alcantarillado a más de disponer de aplicaciones E-Business, que integre la información de la gestión de la Empresa,

es necesario que cuenten con una infraestructura de red que asegure que la información generada por la Matriz y sus sucursales se consolide en tiempo real.

En la actualidad, la infraestructura de red de las empresas medianas de Agua Potable y Alcantarillado disponen de redes locales para la Matriz y sus sucursales en forma independiente y se encuentran en un ambiente de grupo de trabajo.

Adicionalmente carecen de seguridades en la red y no se han definido políticas de seguridad, lo que le hace vulnerable a ataques internos y externos, por lo que la información estaría en riesgo.

Esta Tesis propone un Diseño de una Interred Segura para soporte de aplicaciones E-Business utilizando tecnologías de Intranet y VPN para obtener:

- Conectividad entre la Matriz y sus sucursales con el fin de utilizar una aplicación E-Business que integre todos los procesos de negocio.
- Comunicaciones seguras entre la Matriz y sus sucursales a fin de asegurar la confidencialidad de la información generada por medio de las actividades de la Empresa.

Comunicación en línea con la Empresa Proveedora de las aplicaciones E-Business y la Matriz de las Empresas Medianas de Agua Potable y Alcantarillado con el fin de obtener soporte técnico y mantenimiento de sus aplicaciones E-Business con las debidas seguridades para el efecto.

CAPÍTULO 2. DISEÑO DE LA INTERRED E INTRANET SEGURA

2.1 ANÁLISIS DE LA INFRAESTRUCTURA ACTUAL DE RED DE EMPRESAS MEDIANAS DE AGUA POTABLE

Las empresas medianas de Agua Potable desde que se conformaron como empresas independientes de sus respectivos Municipios, surgieron nuevas necesidades con el fin de dar una mejor atención al Cliente, por lo que han encontrado en la tecnología el apoyo necesario para automatizar sus procesos de comercialización, recaudación e infraestructura. Sin embargo, se han visto limitadas por la infraestructura que disponen actualmente, que no les permite integrar los datos generados por su gestión entre sí, ya que no disponen de una conectividad entre la Matriz y las Agencias que conforman la Empresa.

2.1.1 SITUACIÓN ACTUAL DE LAS EMPRESAS MEDIANAS DE AGUA POTABLE

Actualmente, las empresas medianas de Agua Potable se conforman de una Matriz y de una a cuatro Agencias de Recaudación.

La red física de la Empresa consta de redes LAN independientes para la Matriz y cada Agencia de Recaudación sin conectividad entre ellas, lo cual no permite integrar inmediatamente los datos que se generan entre sí.

El problema principal es la consolidación de información hacia la Matriz, por lo cual actualmente buscan nuevas alternativas de solución para integrar los datos que se generan en forma aislada desde las Agencias a la Matriz.

2.1.1.1 Estructura de la Red LAN

Actualmente toda la red física de la Empresa consta de una red LAN en la Matriz y una red LAN en cada Agencia de Recaudación. Todas las redes LAN se encuentran bajo un ambiente de grupo de trabajo (workgroup).

La Matriz dispone de acceso a Internet.

Los computadores actuales de una de las empresas medianas de Agua Potable y sus características son:

AGENCIA	NOMBRE	PROCESADOR	MEMORIA RAM	DISCO DURO	SISTEMA OPERATIVO
MATRIZ	Comercial	Pentium IV	2 GB	146 GB	Windows 2000 Server
MATRIZ	ACom-1	Pentium III	226 MB	40 GB	Windows 98
MATRIZ	ACom-2	Pentium IV	512 MB	60 GB	XP Profesional
MATRIZ	ACom-3	Pentium II	128 MB	20 GB	Windows 98
MATRIZ	ACom-4	Pentium II	64 MB	20 GB	Windows 98
MATRIZ	ACom-5	Pentium III	256 MB	40 GB	Windows 98
MATRIZ	ACom-6	Pentium IV	256 MB	40 GB	XP Profesional
MATRIZ	ST-1	Pentium II	128 MB	20 HD	Windows 98
MATRIZ	ST-2	Pentium IV	256 MB	40 GB	XP Profesional
MATRIZ	MAT-CR1	Pentium IV	512 MB	60 GB	XP Profesional
MATRIZ	MAT-CR2	Pentium IV	512 MB	60 GB	XP Profesional
MATRIZ	TEC-1	Pentium III	256 MB	20 GB	Windows 98
MATRIZ	PLA-1	Celeron	256 MB	40 GB	Windows 98
MATRIZ	PLA-2	Celeron	128 MB	20 GB	Windows 98
MATRIZ	FIN-1	Pentium IV	512 MB	60 GB	XP Profesional
MATRIZ	FIN-2	Pentium III	256 MB	20 GB	Windows 98
MATRIZ	CTB-1	Pentium III	256 MB	40 GB	XP Profesional
MATRIZ	CTB-2	Pentium III	512 MB	60 GB	XP Profesional

AGENCIA	NOMBRE	PROCESADOR	MEMORIA RAM	DISCO DURO	SISTEMA OPERATIVO
MATRIZ	CTB-3	Pentium III	256 MB	20 GB	Windows 98
MATRIZ	SGR-1	Celeron	512 MB	40 GB	XP Profesional
MATRIZ	SGR-2	Celeron	512 MB	40 GB	XP Profesional
MATRIZ	ADM-1	Pentium II	256 MB	20 GB	Windows 98
MATRIZ	RRHH-1	Pentium III	256 MB	40 GB	XP Profesional
MATRIZ	RRHH-2	Celeron	512 MB	40 GB	Windows 98
AGENCIA 1	AG1-CR1	Pentium IV	512 MB	60 GB	XP Profesional
AGENCIA 1	AG1-CR2	Pentium IV	512 MB	60 GB	XP Profesional
AGENCIA 2	AG2-CR1	Pentium IV	512 MB	60 GB	XP Profesional
AGENCIA 3	AG3-CR1	Pentium IV	512 MB	60 GB	XP Profesional
AGENCIA 3	AG3-CR2	Pentium IV	512 MB	60 GB	XP Profesional
AGENCIA 4	AG4-CR1	Pentium IV	512 MB	60 GB	XP Profesional

Tabla 2.1 Características de los Computadores de la Red Física Actual

El computador ***"Comercial"***, es el servidor del Sistema Comercial actual y el punto de acceso a Internet.

Las impresoras existentes se muestran en la **Tabla 2.2.**

MARCA	MODELO	CANTIDAD
HP	LaserJet 1000	1
HP	LaserJet 2420	1
HP	LaserJet 4L	1
EPSON	LX – 300	6
EPSON	FX – 980	8
EPSON	FX – 1180	1
SAMSUNG	ML – 1610 Series	1

Tabla 2.2 Listado de Impresoras de la Red Actual

Los equipos de comunicación se muestran en la **Tabla 2.3.**

MARCA	TIPO	MODELO	No. PUERTOS
3COM	Switch	SuperStack 3 Baseline	24
3COM	Switch	SuperStack 3 Baseline	16

Tabla 2.3 Equipos de Comunicación de la Red Actual

Estos equipos de comunicación están instalados en un rack en la Matriz, y existen hubs para conectar los computadores de cada departamento; los hubs se conectan con los switches. Las Agencias no disponen de switches, y sólo las Agencias 1 y 3 cuentan con hubs uno para cada una.

Adicionalmente, La Matriz cuenta con cableado estructurado y un enlace a Internet Banda Ancha 1000 kbps compartición 2:1 a través de Cable módem.

La configuración física de la Red Actual de la Matriz y de las Agencias se muestra en las **Figura 2.1. y Figura 2.2.** respectivamente.

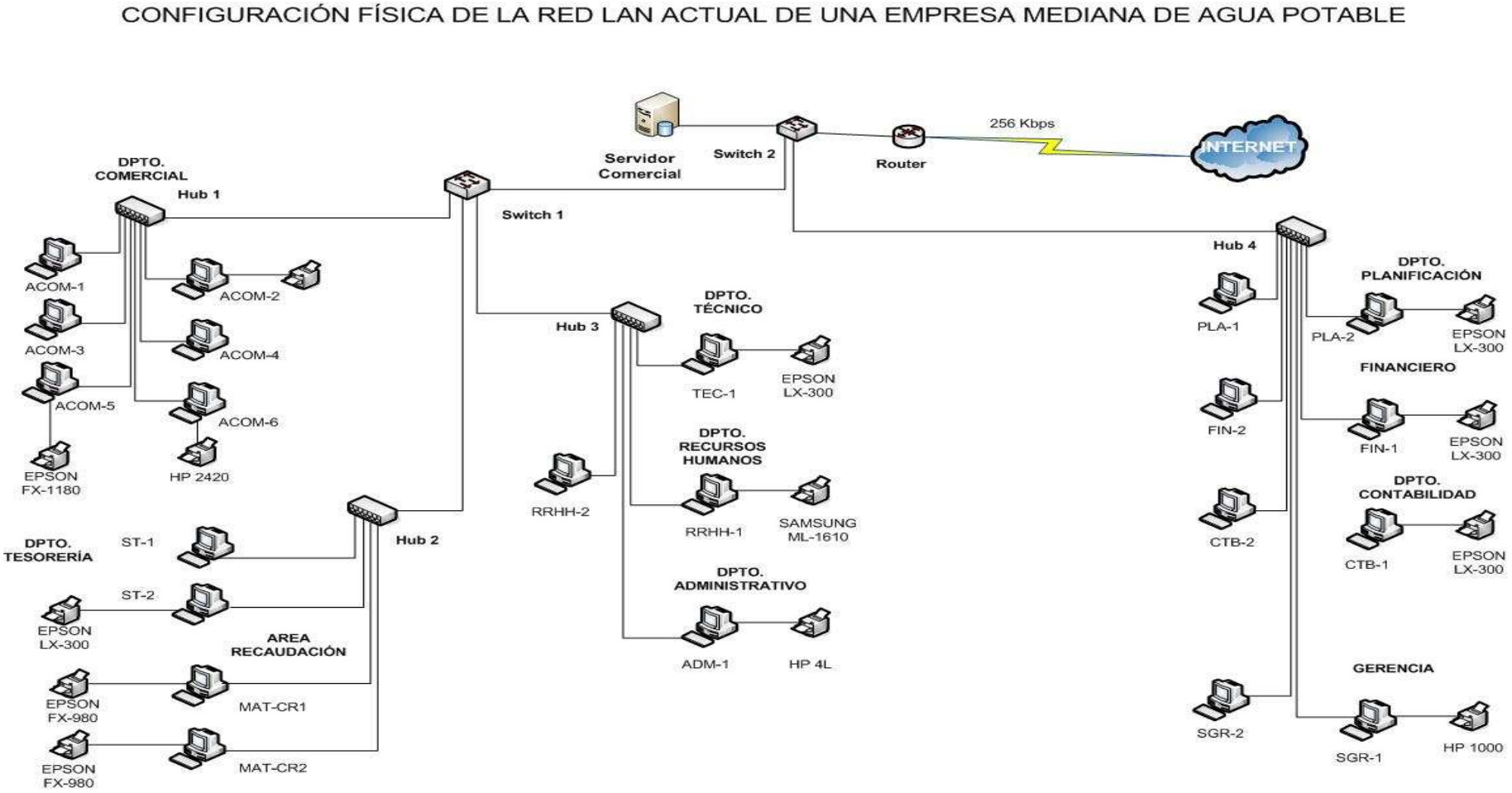


Figura 2.1 Configuración Física de la Matriz de la Empresa de Agua Potable
Fuente: La Autora

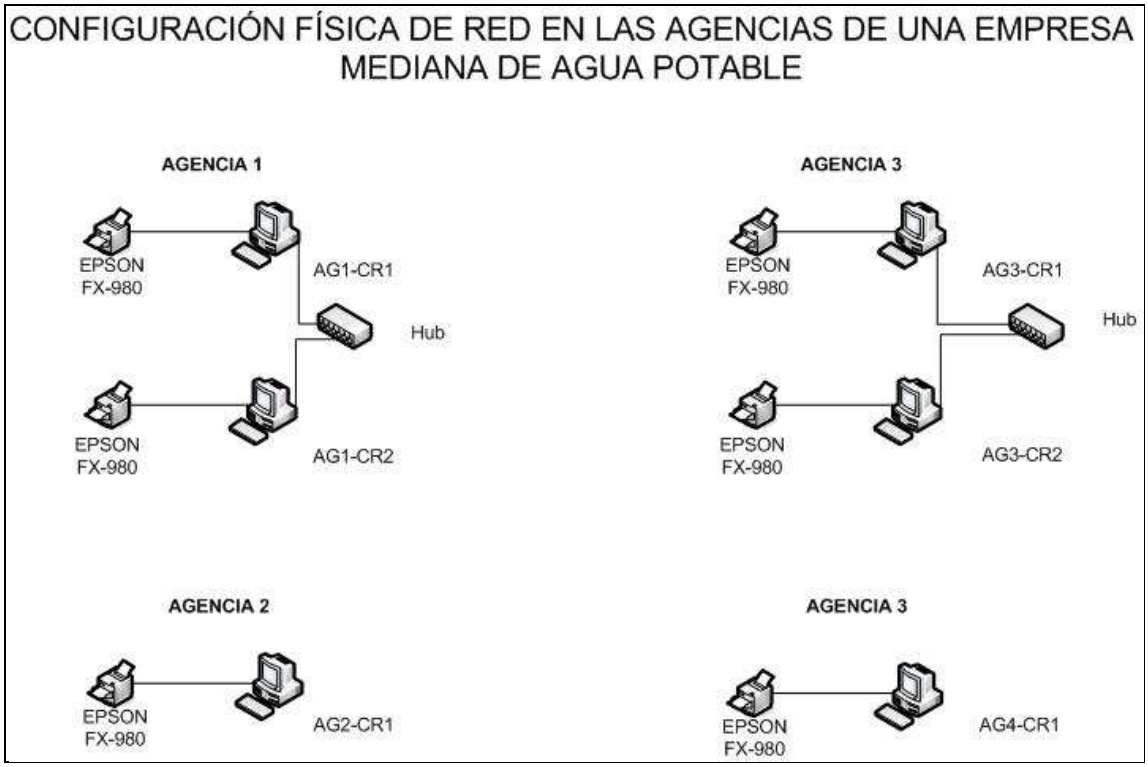


Figura 2.2 Configuración Física de las Redes LAN en las Agencias de Agua Potable sin conexión a la Matriz

Fuente: La Autora

2.1.1.2 Seguridades

2.1.1.2.1 Seguridades Físicas

Respecto a la seguridad que tiene las instalaciones de una Empresa de Agua Potable se indica lo siguiente:

- Existe guardianía las 24 x 7 x 365 (24 horas al día, 7 días a la semana y 365 días al año).
- Puertas metálicas y Lanfor para acceso a las instalaciones.
- Disponen de sistemas de aire acondicionado.
- No hay cámaras de seguridad.
- Tampoco detectores de humo.

En cuanto al área destinada para los equipos de cómputo se encontró lo siguiente:

- Dispone de un sistema de aire acondicionado.
- Para el servidor existe un UPS con una duración de hasta 4 horas en caso de que el fluido eléctrico no esté disponible.
- Los computadores en general disponen de reguladores de voltaje.
- Para casos de incendio cuentan con un extinguidor.
- No existen cámaras de seguridad.
- Es un área totalmente accesible.

2.1.1.2.2 Seguridades Lógicas

- No existe configurado un dominio, la red se encuentra en ambiente de trabajo.
- No existen políticas de acceso a Internet, todos los usuarios tienen acceso sin restricción alguna.
- No existen políticas de seguridad para el uso de los sistemas existentes.
- No existe control sobre las impresiones. Todo el personal tiene acceso a imprimir en cualquier impresora disponible exponiendo información sensible a cualquier persona.
- No existen restricciones para la configuración de red en los computadores, todo usuario es administrador de equipo.
- No existen políticas de uso de claves, se puede obtener fácilmente una con el consentimiento del usuario.
- El servidor no cuenta con todos los parches de seguridad instalados.
- A pesar de existir un computador que hace las veces de servidor para actualizaciones de antivirus, los computadores no están correctamente

configurados para obtener la última actualización del mismo, por lo que existe gran probabilidad de contagio de la red.

2.2 ANÁLISIS DE REQUERIMIENTOS DE INTERRED E INTRANET

Las empresas medianas de Agua Potable están formando una estructura física conformada por una Matriz y una o varias Agencias como puntos de Atención al Cliente y Recaudación.

2.2.1 ANÁLISIS DE REQUERIMIENTOS DE CORREO ELECTRÓNICO

2.2.1.1 Funcionalidad

El servicio de correo electrónico es un requerimiento básico de comunicación entre el personal, proveedores, contratistas, socios y clientes. A través de este servicio entregamos y obtenemos proformas, pedidos, reuniones de trabajo, cronogramas de actividades, entrega de documentos contractuales, etc.

Este servicio debe estar disponible las 24 horas del día, 7 días a la semana y 365 días al año, es decir un servicio ininterrumpido sin tomar en cuenta días festivos o feriados.

Este servicio debe ser accesible desde internet, así el personal no dependerá del computador de la Empresa y podrá acceder a su correo en casos de emergencia desde su hogar con tan solo disponer del servicio de Internet.

Al ser un servicio accesible desde Internet se deberá implementar una comunicación segura a través de SSL.

2.2.1.2 Hardware

Este servicio podrá ser utilizado por cualquier funcionario de la Empresa en cualquier estación de trabajo incluyendo las estaciones de trabajo de cualquier Agencia sin ningún inconveniente.

La Tabla 2.4 muestra las características de los requerimientos mínimos de hardware que deberán tener las estaciones de trabajo para implementar Internet Explorer 7.0 y Mozilla Firefox.

COMPONENTE DEL SISTEMA	REQUERIMIENTOS DE HARDWARE IE 7.0	REQUERIMIENTOS DE HARDWARE MOZILLA FIREFOX
PROCESADOR	Se recomienda procesador Pentium	Se recomienda procesador Pentium 500 mhz o superior
ESPACIO EN DISCO	12 MB Windows XP	52 MB Windows XP, 2003 Server, Vista o Windows 2000
MEMORIA RAM	Min. 64 MB RAM	Recomendado 128 MB RAM

Tabla 2.4 Requerimientos de Hardware para Internet Explorer 7.0 y Mozilla FireFox

Fuente: Sitio de Descarga Internet Explorer 7.0 y Mozilla FireFox

2.2.1.3 Software

Es importante indicar que el servidor de correo electrónico se basa en LINUX.

Como el servicio de correo electrónico podrá ser accedido por medio de Internet se requiere un navegador Web compatible con los sistemas operativos disponibles.

Internet Explorer 7.0 y Mozilla FireFox puede ser instalado sobre Windows XP, XP Profesional y Windows 2003 Server.[2]

2.2.1.4 Comunicaciones

Si el servicio es solicitado desde la Matriz no existe un requerimiento adicional de comunicación ya que se utilizará la red LAN.

Si el servicio es solicitado desde una Agencia deberá existir un enlace de comunicación directa hacia la Matriz.

[2] Fuente: Sitio de descarga de Microsoft y Mozilla FireFox.

Si el servicio es solicitado desde una ubicación fuera de la infraestructura de la empresa, se deberá tener una conexión al servicio de Internet como dial-up, xDSL, cable Modem o cualquier otra.

2.2.2 ANÁLISIS DE REQUERIMIENTOS DE LA APLICACIÓN E-BUSINESS

2.2.2.1 Funcionalidad

Este requerimiento es la aplicación que utilizarán todos los usuarios del área Comercial y de Tesorería de la Matriz y las Agencias. Debe tener las siguientes funcionalidades:

- Integrar todos los procesos comerciales de la Empresa de Agua Potable.
- Permitir que las secciones: Lecturas, Clientes, Acometidas y Medidores, Facturación, Recaudación y Atención al Cliente trabajen en forma paralela.
- Proveer información actualizada y en línea de toda la gestión comercial para Matriz y Agencias.
- Permitir el acceso de las Agencias a la aplicación por medio de una Identificación y Clave.
- Aplicar restricciones de acceso a los diferentes módulos de la aplicación por medio de perfiles.

2.2.2.2 .Hardware

Los requerimientos mínimos para que la Aplicación E-Business son los siguientes:

2.2.2.2.1 Servidor:

- Sistema Operativo: Windows 2003 Server
- Base de Datos: Microsoft SQL Server 2005
- Procesador: Intel Xeon de 3.2 Ghz o superior
- Memoria RAM: 4 GB mínimo
- Disco Duro: 60 GB libre mínimo

2.2.2.2.2 Estaciones de Trabajo:

- Sistema Operativo: Windows XP Profesional, Service Pack 3
- Procesador Pentium IV de 2.0 Ghz o superior
- Memoria RAM: 1 GB mínimo
- Disco Duro: 20 GB libre mínimo

2.2.2.2.3 Red de Datos

- Ethernet a 100 Mbps
- Opcional: Enlaces dedicados de 128 Kbps para conectar Matriz con Agencias, siempre para tener la información en línea y en tiempo real en todas sus ubicaciones.

2.2.2.3 Software

La aplicación E-Business está desarrollada en Punto Net y para que pueda instalarse correctamente en el servidor en general se necesita el siguiente software adicional:

- Framework 2.0
- Internet Information Services
- IuWebControls
- Crystal Reports v11
- Parches de Seguridad del Sistema Operativo
- Antivirus

Las estaciones de trabajo necesitan un browser que podría ser Internet Explorer 7.0 o Mozilla FireFox.

2.2.3 CONECTIVIDAD ENTRE MATRIZ Y AGENCIAS

2.2.3.1 Funcionalidad

Este requerimiento implica que cada red LAN de las agencias se conecte directamente a la Red LAN de la Matriz con el fin de obtener información actualizada y en tiempo real.

2.2.3.2 Hardware

Los requerimientos para integrar las redes LAN de la Matriz y Agencias es el siguiente:

- Equipos de Radio 2.4 Ghz (de uso general) en cada Agencia.
- Firewall para la Matriz

2.2.3.3 Software

Se necesitará el software de configuración de los equipos de enlace de Radio para implementar la Interred entre la Matriz y Agencias.

2.3 DETERMINACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INTERRED E INTRANET

Determinar las políticas de seguridad para una empresa es lo más importante para resguardar la información y los recursos tecnológicos que dispone.

Las políticas que se recomiendan en esta sección están orientadas para un uso apropiado de los recursos informáticos de la empresa además de la responsabilidad que está inmersa en la aplicación de las mismas y las consecuencias de su abuso.

Los recursos informáticos de una empresa son: servidores, estaciones de trabajo, redes, infraestructura y equipos de comunicación, sistemas informáticos, impresoras, tecnologías que permitan el acceso, distribución y generación de información dentro y fuera de la empresa y la información contenida en cada equipo.

La responsabilidad del Administrador de la Interred e Intranet es hacer cumplir las políticas de seguridad que determine la empresa y en el caso extremo aplicar las sanciones correspondientes si éstas no se cumplen.

2.3.1 OBJETIVO

Establecer políticas de seguridad para el uso correcto de los recursos informáticos, lo que se va a proteger y lo que se trata de proteger en la empresa y definir las responsabilidades y derechos del Administrador de la Interred e Intranet y establecer las consecuencias de su abuso.

2.3.2 ALCANCE

Las Políticas de Seguridad son aplicables a todo el personal de la empresa de Agua Potable, a toda entidad externa que haga uso de los recursos informáticos de la empresa tales como: Consultores, Auditores, personal temporal, proveedores y otros.

El intentar violar los sistemas de seguridad y de control de personal se consideran actos graves de contravención a las políticas y normas de la empresa así como atentatorias a la seguridad y confidencialidad de la información de la empresa y sujeta a las leyes penales del Ecuador.

2.3.3 RESPONSABILIDAD

El Jefe de la sección de Procesamiento de Datos es el responsable de difundir, cumplir y hacer cumplir las Políticas de Seguridades y recomendar normas y alertas en el manejo de los programas, correo electrónico, Internet, sistemas de aplicación e información en general.

2.3.4 POLÍTICAS DE CUENTAS DE USUARIO Y CLAVES

- Las claves de usuario de nivel administrador deben cambiarse cada mes.
- Las claves de usuario de Intranet deben cambiarse cada mes.
- Las claves de usuario de Interred se mantienen hasta que el usuario solicite su cambio por medio del área de Informática.

2.3.4.1 Normas Generales para la creación de claves

Las claves se utilizan para varios propósitos: cuentas de usuario para acceso a la red, cuentas de acceso a e-mail, claves de acceso a aplicaciones, protectores de pantalla, etc. En cualquier caso es importante que la clave pueda resistir el criptoanálisis e ingeniería social.

Para crear una clave debe seguir las siguientes normas:

- Utilizar combinaciones de caracteres mayúsculas y minúsculas (a-z, A-Z)
- Incluir números, letras y caracteres especiales.
- Tener más de 8 caracteres

Se recomienda evitar el uso de nombres relacionados con personas tales como novio, esposo, hijos, mascotas, amigos, nombres mitológicos o astronómicos, términos informáticos, comandos, marcas, nombres relacionados con la empresa, fechas personales importantes o fechas en general, y patrones de letras o números tales como: “qwerty” “1234567” “abcdefge” como una clave.

2.3.4.2 Normas para Protección de Claves

- No utilizar la misma clave para las cuentas del Sistema Web, correo electrónico u otros.
- Las claves son confidenciales, no debe compartirla con nadie bajo ninguna circunstancia.
- No exponer las claves en ningún medio de comunicación como por ejemplo: decir las claves por teléfono, escribir las claves en un e-mail, escribir las claves en papel.
- No almacenar las claves en un archivo en ningún sistema informático (incluyendo PDA’s o dispositivos similares).
- No revelar las claves anteriormente utilizadas.

2.3.4.3 Uso de Clave para Usuarios de Acceso Remoto

El acceso remoto de los usuarios a los servicios de red se lo hace utilizando autenticación de claves públicas y privadas, incluidas en los protocolos de comunicación.

2.3.5 POLÍTICAS DE SEGURIDAD PARA ESTACIONES DE TRABAJO

- EL Jefe de Informática, al entregar un equipo de informática o una cuenta a un usuario debe obtener la firma de un documento donde declara conocer las Políticas de Seguridades, la asignación y estado de los equipos, como aceptación de su responsabilidad con relación al uso de los recursos asignados.
- Los equipos sólo deben usarse para actividades de trabajo y no para otros fines ajenos a los objetivos de la empresa, tales como juegos, almacenar archivos personales o investigaciones que no forman parte de los procesos de la empresa.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de Informática.
- Reportar inmediatamente cualquier falla en los computadores o en la red; pues podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- No fumar, comer o beber mientras se está usando un computador.
- No pegar adhesivos o publicidad sobre los equipos.
- No se pueden mover los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la organización se requiere una autorización escrita.

- Proteger los equipos de riesgos del medio ambiente como polvo, incendio y agua.
- Proteger los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. El usuario deberá activar el protector de pantalla manualmente cada vez que se ausente de su puesto de trabajo.
- Si un computador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla.
- Borrar los datos confidenciales cuando ya no se necesiten y no sean de utilidad.
- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PC’s que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la empresa.

- Los usuarios no deben copiar a un medio removible (como un diskettes, memorias flash, cd’s, etc), el software o los datos residentes en las computadoras de la empresa, sin previa autorización de la gerencia.
- No pueden extraerse datos fuera de la sede de la empresa sin previa autorización de la gerencia.
- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos.
- Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la empresa.
- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que su uso sea debidamente probado por el área de Informática.
- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
- El Jefe de Informática debe asignar un código para cada equipo y sus componentes para su identificación y control de inventario; además debe garantizar que esté siempre legible. Los usuarios no deben destruir el código.
- El Jefe de Informática debe mantener actualizados los inventarios de los equipos.
- El Jefe de Informática debe instalar y activar un antivirus en todos los equipos, el cual debe mantenerlo actualizado.
- El Jefe de Informática debe garantizar que los servidores, los equipos de comunicación y el rack de cableado estructurado están protegidos contra daños y robo. Debe restringir el acceso a personas no autorizadas a la ubicación de los mismos.

2.3.6 POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES

2.3.6.1 Uso de los Sistemas de Comunicación

- Los sistemas de comunicación de la empresa sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y no interfiera con las actividades del empleado ni con la gestión de la empresa.
- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la empresa y en tal sentido deben usarse las horas no laborables.
- Los usuarios no deben usar los sistemas informáticos para insultar o molestar a ningún usuario. El lenguaje en las comunicaciones debe ser respetuoso y en los parámetros de la cordialidad.

2.3.6.2 Confidencialidad y Privacidad

- El Jefe de Informática debe garantizar que no exista información confidencial en las estaciones de trabajo antes de ser enviadas para su reparación. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante de la empresa de agua potable.
- Los empleados y funcionarios de la empresa no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La empresa se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para

lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

- Es política de la organización no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones pueden ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.
- Los usuarios que manejan datos confidenciales de la organización los deben borrar de sus equipos cuando ya no sean de utilidad.
- La información de la organización clasificada como confidencial o de uso restringido, debe guardarse y transmitirse utilizando herramientas que hayan sido probadas y autorizadas.
- Cada usuario es responsable de identificar el tipo de información que está transmitiendo o guardando, con un texto o leyenda al pie del documento.
- Los usuarios que sospechen cualquier actividad ilegal o fraudulenta deben notificar inmediatamente al Jefe Informática.

2.3.6.3 Reenvío de Mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la empresa, se debe ejercer cierta cautela al reenviar los mensajes. En todo caso no debe reenviarse información confidencial de la empresa sin la debida aprobación.

2.3.6.4 Borrado de Mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

2.3.7 POLÍTICAS DE SEGURIDAD PARA REDES

2.3.7.1 Modificaciones

Todos los cambios en los servidores y equipos de red de la empresa, incluyendo la instalación del nuevo software, el cambio de direcciones IP's, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

2.3.7.2 Cuentas de los Usuarios

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta su responsabilidad con relación al uso de la misma.
- La solicitud de una nueva cuenta o el cambio de privilegios debe ser pedida por escrito y debe ser debidamente aprobada.
- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Jefe de Informática determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Jefe de Informática debe revocar rápidamente la cuenta o

los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

- Cuando un empleado es despedido o renuncia a la empresa, debe desactivarse su cuenta antes de que deje el cargo.

2.3.7.3 Contraseñas y Control de Acceso

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas anteriormente utilizadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

  La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión.

- El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña.
- Si el sistema de control de acceso no está funcionando apropiadamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la empresa, pudiendo ser causal de despido.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
- Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.
- Los servidores de red y los equipos de comunicación (routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

2.3.8 POLÍTICAS DE BACKUP

2.3.8.1 Responsabilidad de la Empresa y los Usuarios

- Periódicamente, los usuarios deben sacar respaldos de sus archivos guardados en las estaciones de trabajo y servidores, en otros medios magnéticos y/o sistemas diferentes, los mismos que deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones, para que, en caso de cualquier eventualidad, el usuario pueda rever sus datos.
- Los usuarios de las estaciones de trabajo son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Jefe de Informática es el responsable de hacer copias de respaldo periódicas. Los gerentes de las distintas direcciones y áreas son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).
- Los usuarios tienen la responsabilidad de leer las noticias anunciadas en el login de su cuenta (noticias que informan sobre paradas eventuales del sistema, mantenimiento de hardware y software) y así prever rescates.

2.3.8.2 Backups y Restauración

Un backup general que incluye el área de usuario, es efectuado una vez por mes. En caso de remoción accidental de un archivo, es posible restaurarlo a partir del backup general efectuado. Pero nada garantiza que el archivo pueda ser restaurado y tampoco que la fecha de remoción coincida con la fecha más próxima del backup general.

2.3.8.3 Seguridad e Integridad de Datos

- En el caso de que ocurran fallas de disco o sistema, los discos serán restaurados a partir del backup más reciente. De esta forma el usuario deberá estar al tanto de que archivos actualizados o creados, entre la fecha de falla y del backup más reciente, pueden ser perdidos.

- La empresa garantiza que los archivos de los usuarios están protegidos al acceso de otros usuarios, siempre y cuando el usuario no altere el permiso de acceso a sus archivos.
- Se obtiene un backup semanal de las bases de datos operativas de tal forma que se garantice la operación de las aplicaciones existentes.

2.3.9 POLÍTICAS DE COMPRA, CONTROL Y ADMINISTRACIÓN DE ANTIVIRUS

2.3.9.1 Compra de Antivirus

El antivirus deberá cumplir con las siguientes características:

- Deberá actualizar los patrones o firmas, por lo menos una vez por semana.
- La empresa que los promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta no mayor a 48 horas, el cual me pueda orientar, en mi idioma, en caso de que yo contraiga una infección.
- Deben contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico, el cual no se basa en firmas virales sino en el comportamiento de un archivo, y así poder detener amenazas incluso de posibles virus nuevos.
- Se deben poder adaptar a las necesidades de diferentes usuarios.
- Deben poder realizar la instalación remota tanto en una red LAN como en una WAN.
- Deben constar de alguna consola central en donde se puedan recibir reportes de virus, mandar actualizaciones y personalizar a distintos usuarios.
- Deben ser verdaderamente efectivos para la detección y eliminación correcta y exacta de los distintos virus que puedan amenazar a los sistemas.

- Deben de permitir la creación de discos de emergencia o de rescate de una manera clara y satisfactoria.
- No deben de afectar el rendimiento o desempeño normal de los equipos, y de ser preferible lo que se desea es que su residente en memoria sea de lo más pequeño.
- El número de falsos positivos que se den tanto en el rastreo normal como en el heurístico debe de ser el mínimo posible.
- Su mecanismo de auto-protección debe de poder alertar sobre una posible infección a través de las distintas vías de entrada, ya sea Internet, correo electrónico, red o discos flexibles, etc.
- Deben de tener posibilidad de chequear el arranque, así como los posibles cambios en el registro de las aplicaciones.

2.3.9.2 Seguridad contra Infección de Virus Informáticos

2.3.9.2.1 Controles

- Control de acceso físico a los equipos.
- Control de entradas a los programas de la computadora a través de claves de acceso (passwords).
- Registro, verificación y control de los diskettes, cd's, memorias flash que se conecten a la computadora.
- Se recomienda algún programa de tipo menú que restrinja los programas que se pueden ejecutar a sólo los autorizados a cada usuario.

2.3.9.2.2 Bloqueos

- Uso del candado o llave de encendido, si la computadora lo tiene.
- Deshabilitar el acceso desde unidades externas (diskettes, cd's puertos USB).
- Habilitación de la facilidad de palabra clave (password).

- Activar la protección anti-virus en BIOS.

2.3.9.3 Actualización Antivirus

- Instalar el antivirus y asegurar cada 15 días su actualización
- Utilizar o activar las diversas opciones de protección.
- Al actualizar el antivirus, verificar el PC completamente. En caso de detectar un virus, proceder a verificar todos nuestros soportes (diskettes, CD's, ZIP's, etc.)
- Comprar las versiones actualizadas de las vacunas.
- Leer la documentación y manuales de los antivirus.

2.3.9.4 Servicios en Línea (navegación – correo electrónico)

- Para bajar páginas de Internet, archivos ejecutables, etc., definir siempre en nuestra PC una carpeta o directorio para recibir el material. De ese modo sabemos que todo lo que bajemos de Internet siempre estará en una sola carpeta. Nunca ejecutar o abrir antes del escaneo.
- Nunca abrir un adjunto de un e-mail sin antes chequearlo con el antivirus. Si el adjunto es de un desconocido que no avisó previamente del envío del material, directamente borrarlo sin abrir.
- Verificar contra virus todo programa que se transfiera.
- Verificar contra virus todo archivo autodescomprimible (aunque sea de datos).

2.3.9.5 Medios de Almacenamiento Externo

Estos son puntos muy importantes, prácticamente todos los virus se introducen a una computadora por medio de CD's y memorias flash.

- Verificar contra virus todos los, CD's y memorias flash que se introduzcan en la computadora, aunque sólo sean de datos.
- No ejecutar programas de origen dudoso.

- No meter, cd’s o memorias flash extraños.
- Nunca arranque desde CD’s en la operación normal de su computadora.
- Nunca dejar puestos CD’s al apagar la computadora.
- Proteja contra escritura sus discos del sistema, así como sus discos de programas de aplicación.
- Que los usuarios sólo manejen CD’s de datos y nunca de programas.
- Instalar nuevos paquetes en una máquina que sirva para estudio de comportamiento y que esté un tiempo en observación.
- Mantener copias respaldo, tanto de los programas, como de los datos.
- Hacer por separado los respaldos de datos y de programas.
- Revisar todo CD y memoria flash que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido ingresado en la disquetera de otra PC.

2.3.9.6 Otros

- Capacitar a los usuarios en protección contra virus.
- Mantenerse informado, o sea leer sobre el tema

2.3.10 POLÍTICAS DE SEGURIDAD LÓGICA

2.3.10.1 De la Administración y monitoreo de los Servidores

- La administración de los servidores debe realizarse únicamente por el personal aprobado por el Área de Sistemas, a fin de mantener consistencia con las Políticas de Seguridad.
- Deben existir únicamente dos cuentas de usuario de administrador del sistema operativo en los equipos de cómputo o servidores donde residirán los sistemas.

- El Jefe de Informática debe implantar un sistema de autorización y control de acceso a los archivos compartidos para disminuir la posibilidad de que los usuarios no autorizados puedan leer, escribir, modificar, crear, o borrar datos importantes.
- En caso de intento o infiltración o contravención a la seguridad o sistemas informáticos de la organización, el Jefe de Informática deberá capturar, grabar y guardar la información o el hecho sospechoso.
- Es necesario la utilización de sistemas de seguridad Firewall, para detección de intrusos; y el personal encargado de la administración del Firewall deberá ser aprobado por el Área de Sistemas. Se deberá manejar bitácoras que registre intentos de acceso autorizados y no autorizados.
- El Jefe de Informática debe revisar periódicamente los logs y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones. A los mismos que los debe conservar por un periodo de por lo menos tres meses.
- El Jefe de Informática debe garantizar que los servidores estén conectados a UPS, y que estos respondan efectivamente en caso de necesitarlos.

2.3.10.2 De la asignación de Claves de Monitoreo

- La administración de la contraseña del o los equipos de cómputo o servidores es responsabilidad del Jefe de Informática .
- La contraseña de administración y configuración del Firewall, deberá ser de conocimiento del Jefe de Informática.
- Las Unidades no debe escribir ni colocar la contraseña de la cuenta de administración y configuración del sistema de seguridad en lugares donde pueda ser descubierta por terceros.

2.3.10.3 De las Políticas de Seguridad que se aplicarán en el Firewall

- Las políticas de seguridad del o los Firewalls serán instrumentadas y puestas en operación por el Jefe de Informática.

2.3.10.4 Sobre las Licencias y Copyrights

- El Jefe de Informática debe garantizar que todo software que se adquiera para la organización debe estar debidamente licenciado.
- Los usuarios deben asumir que todo el software de la organización está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- Toda otra información que también posea derechos de autor y esté en formato electrónico y que haya sido obtenida de otro equipo, se debe usar con la autorización pertinente.
- Todo software que se use ya sea para fines administrativos o investigativos debe estar debidamente licenciado, con un número de licencias que se corresponda con el número de usuarios a utilizarlo. La utilización del software "libre" (Open source, freeware, Trial, etc.) debe estar aprobado por el Área de Informática.

2.4 REDISEÑO DE LAS REDES LAN Y WAN DE EMPRESAS MEDIANAS DE AGUA POTABLE

2.4.1 CONSIDERACIONES DE REDISEÑO DE LAS REDES LAN

2.4.1.1 Aspectos Operativos

Las actividades diarias del personal de la Matriz implican el uso de Internet y aplicaciones varias que apoyan la gestión de procesos.

2.4.1.1.1 Acceso a Internet

La Gerencia General (Presidencia Ejecutiva), áreas Contables y Financieras y en general los Directivos o Jefaturas de la Empresa, necesitan del acceso a Internet como medio de comunicación con otras Entidades para desempeñar sus actividades diarias sin abandonar sus puestos de trabajo.

En general las actividades que realizan a través de Internet son:

- Administración de los procesos de compras a través del Portal “Compras Públicas”.
- Transferencias Bancarias por concepto de pago de proveedores y servicios por el Sistema de Pagos Interbancario del Banco Central del Ecuador (SPI-BCE).
- Manejo de las cuentas Bancarias que mantienen las empresas con diferentes Instituciones Bancarias.
- Consultas de Información Legal al SRI, Portal del BCE, Ministerio de Finanzas, costos de materiales, etc.
- Comunicación con proveedores, socios, clientes y personal de la Empresa a través de correo electrónico.

2.4.1.1.2 Aplicaciones

Los últimos cambios que han tenido las empresas medianas de Agua Potable han generado nuevas necesidades. Entre ellas el integrar los procesos comerciales que actualmente se los ha gestionado manualmente en unos casos y en otros utilizando pequeñas aplicaciones aisladas. Por lo que se decidió implementar una aplicación que integre los procesos comerciales.

A esta nueva aplicación tendrán acceso la Gerencia y las áreas Comercial, Tesorería y Contabilidad, permitiendo unir esfuerzos para mejorar la calidad y cantidad de actividades diarias enfocadas a la atención al Cliente.

Además se requiere que los datos generados en las Agencias estén actualizados y en línea.

Para lograr este objetivo se implantará lo siguiente:

- Configurar la red LAN de la Matriz bajo un ambiente de dominio.
- El servidor de controlador de dominio servirá también como servidor de archivos.
- Se configurará un servidor de Internet que a la vez funcionará como firewall.
- Se configurará un nuevo servidor para la nueva aplicación Comercial y como servidor de base de datos. (El servidor ya existe en la Empresa)
- Se configurará un computador como servidor de antivirus.
- Se establecerán políticas y restricciones al servidor de archivos para que las tareas de respaldo se realicen en forma adecuada.
- Se establecerán permisos de impresión sobre las impresoras que soporten impresión en red.
- Se mantendrá el esquema de impresoras definidos en las figuras 2.1 y 2.2.
- Se contratará los servicios de acceso Internet a través de una conexión de Banda Ancha de 1000 kbps con compartición de 2 a 1.
- Se restringirá el acceso a Internet al personal que no lo requiera.
- Se añadirá un Access Point para que los equipos portátiles de Consultores o Proveedores de Servicios puedan acceder a la red actual con los debidos permisos y accesos.

2.4.1.2 Infraestructura Requerida

Para la implementación del nuevo diseño de Red la empresa cuenta con:

- Una infraestructura sobre la cual se puede implantar un ambiente de dominio, por lo que se aprovechará el cableado estructurado existente.

- Adicionar Access Point para el acceso a la red de equipos portátiles de Consultores o Proveedores de Servicios de la empresa.

- Será necesario añadir nuevas tomas eléctricas y puntos de red para los nuevos computadores que se comprarán a corto plazo para el área de Atención al Cliente.

- Al momento se reutilizarán los switches y patch panel existentes, sin ningún problema para el desempeño en el tráfico de la red.

2.4.2 CONSIDERACIONES DE REDISEÑO DE LA RED WAN

Las empresas medianas de Agua Potable mantienen varias Agencias. En las mismas se ha estructurado su propia red LAN.

Por la naturaleza del negocio se requiere que las Agencias se encuentren en constante comunicación con la Matriz a fin de disponer información actualizada y en línea.

2.4.2.1 Aspectos Operativos

Desde que las empresas de Agua Potable han empezado a crecer y han estructurado su atención al público en Agencias a más de la Matriz, surgió la necesidad de tener una comunicación entre sí.

Lamentablemente, por las limitaciones económicas no se ha implementado una comunicación directa entre la Matriz y sus Agencias lo que ocasiona los siguientes problemas:

- La consolidación en la Matriz de los datos generados en las Agencias no es tan efectiva, se demora.

- Actualizar la información para recaudar en las Agencias después de la consolidación en la Matriz se demora al menos una semana, lo que ocasiona que un usuario que cancela su deuda en la Matriz no pueda reflejarse inmediatamente en la Agencia y viceversa.

La necesidad de comunicación entre la Matriz y Agencias requiere ser atendida lo más pronto posible, ya que al no poder actualizar diariamente las Bases de Datos en cada Agencia con la información consolidada provoca que varios usuarios puedan pagar dos veces la misma planilla y con ello surgen los reclamos de los clientes al pensar que la Empresa le cobra “injustamente” dos veces.

Es importante que se establezca la comunicación entre la Matriz y Agencias puesto que la nueva aplicación controlará los procesos del negocio que se generen en forma simultánea entre la Matriz y sus Agencias y mantendrá automáticamente actualizada toda la información que requiere para dar atención al cliente con información en línea.

Los enlaces desde as Agencias con la Matriz serán el eje fundamental sobre el cual se apoyen los servicios que permitirán tener información actualizada. Entre estos servicios se mencionan a:

- Nueva Aplicación E-Business
- Correo Electrónico
- Antivirus para protección de los equipos

2.4.2.2 Infraestructura Requerida

Para implementar los aspectos operativos mencionados en la sección 2.4.2.1 se propone lo siguiente:

- Por la sensibilidad de la información se sugiere enlaces de Radio para que cada Agencia se comunique directamente a la Matriz.
- El personal de Recaudación de las Agencias requiere acceso a la nueva aplicación mencionada en la sección 2.4.2.1. Esta nueva aplicación está en ambiente WEB con implementación de comunicaciones seguras.

Se recomienda en lo posible que los enlaces de radio no utilicen infraestructura pública alguna. La encriptación en las comunicaciones las implementarán las aplicaciones de correo electrónico y la nueva aplicación mediante SSL.

Se utilizará enlace VPN para la conectividad con el Proveedor de la aplicación E-Business con las debidas seguridades.

2.5 DISEÑO DE LA INTERRED E INTRANET PARA APLICACIONES E-BUSINESS

El diseño de la Interred para aplicaciones E-Business se analizará desde el punto de vista Lógico, el cual incluye las seguridades y funcionalidad de la aplicación.

2.5.1 SEGURIDAD

Para la operación de la aplicación E-Business se define una arquitectura tecnológica que requiere:

- Un servidor independiente para la aplicación E-Business. Las características de hardware del servidor se listaron en la sección 2.2.2.2.1 y el software que debe instalarse se lista en la sección 2.2.2.2.3. Es importante que el Sistema Operativo Windows 2003 Server tenga todos los parches de seguridad actualizados ya que evita que el servidor se exponga a ataques ya sea de la red interna o externa por virus o códigos maliciosos.

- Disponer de un servidor de red como mecanismo centralizado de seguridad de la red basado en Active Directory (Directorio Activo) de Microsoft, lo que asegura que todo usuario de la red esté plenamente identificado.

- Instalación de un Firewall para protección de la red interna, con el fin de evitar ataques externos a la red y disminuir el riesgo de no disponibilidad de los servicios de la misma, protegiendo los activos intangibles más valiosos que consiste en información contenida en los servidores y estaciones de trabajo.

- Definición de una futura DMZ para acceso al servidor de la aplicación E-Business desde Entidades Bancarias, con las que se firmen acuerdos para que funcionen como Cajas Recaudadoras en línea de la Empresa de Agua Potable y así obtener información actualizada y en línea. Este método asegura que el servidor de Base de Datos de la aplicación E-Business no se exponga directamente, ya que se implementa un segundo servidor de Base de Datos de la aplicación que constantemente replique los datos provenientes de Entidades Bancarias al servidor de Base de Datos en producción.

- Este esquema plantea integrar las redes LAN de la Matriz y Agencias por medio de enlaces dedicados a través de Radios de 2.4 Ghz, lo que asegura tener una red Privada que no necesita de un medio público (Internet) para comunicarse entre sí, por lo que no requiere encriptación de la información para ser transmitida.

- Por otro lado, la necesidad de las empresas de Agua Potable es integrar a la Recaudación algunas entidades Bancarias por medio de convenios y acuerdos, que les permitan acceder a los datos de la Empresa por medio de un canal público (Internet), para lo cual es necesario utilizar el protocolo ***https***, el cual proporciona confidencialidad de los datos con encriptación a través de certificados digitales que se transmiten por un medio público.

2.5.2 FUNCIONALIDAD DE LA APLICACIÓN E-BUSINESS

La aplicación E-Business tiene las siguientes funcionalidades:

- El acceso es por medio de una Identificación y una clave y, el acceso a la aplicación está restringido por el perfil al cual pertenece el usuario.

- Cada Agencia tiene asignado uno o varios usuarios.

- Cada perfil tiene las opciones asignadas de acuerdo a la actividad que desempeña el usuario de la aplicación.

- Todos las Agencias se conectan directamente al Servidor Central de la Aplicación y al Servidor de Base de Datos de la Aplicación E-Business.

2.5.3 DISEÑO DE LA INTERRED E INTRANET

La Figura 2.3 presenta un esquema del Diseño de Intranet e Interred Segura soporte de aplicaciones E-Business.

Como se puede observar se detalla los servidores que podrían ser implementados para dar robustez a la red LAN de la Matriz con los servicios necesarios para la Intranet.

Adicionalmente muestra la comunicación directa con las Agencias formando una Interred lo que asegura que la información y aplicación siempre estará en línea y actualizada.

Por otro lado, se puede apreciar la conectividad por medio de VPN con la Empresa proveedora del Software de la Aplicación E-Business, la misma que a través de este canal seguro pueda brindar soporte remoto a la Empresa de Agua Potable cuando ésta lo requiera.

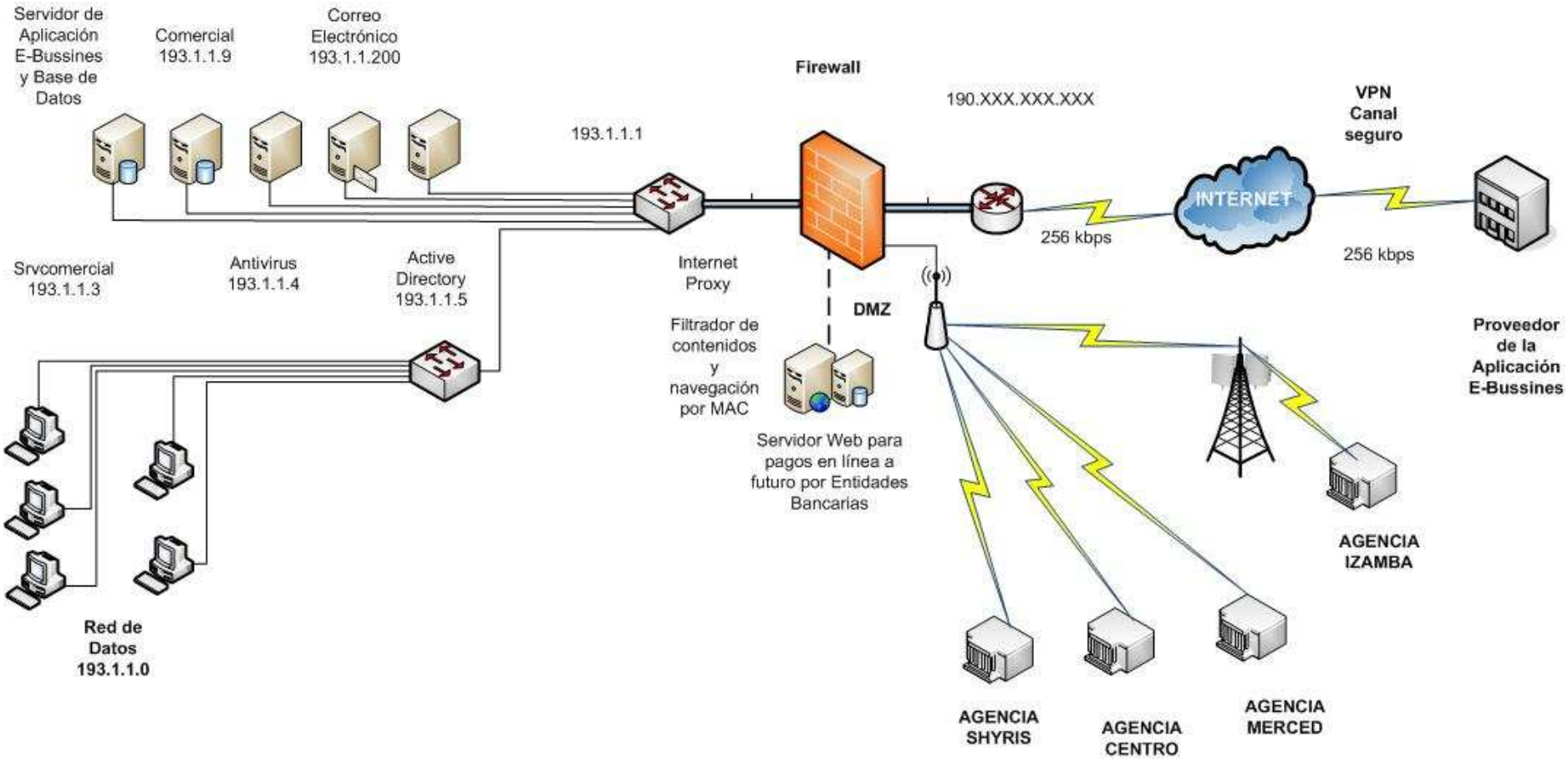


Figura 2.3 Diseño de la Interred e Intranet Segura para aplicaciones E-Business

Fuente: La Autora

CAPÍTULO 3. DISEÑO DE LA ARQUITECTURA VPN

3.1 ANÁLISIS DE REQUERIMIENTOS PARA LA VPN

Las VPN (Virtual Private Network) son redes privadas que funcionan sobre una infraestructura de red pública (Internet) utilizando procesos de encapsulamiento y encriptación para envío de los paquetes a distintos puntos remotos con la misma seguridad, administración y políticas de calidad de servicio que se aplican para las redes privadas.

La VPN ofrece confidencialidad e integridad en el envío de paquetes mediante un *"túnel"* previamente definido en la red pública, con esquemas de encriptación y autenticación para el transporte.

3.1.1 VENTAJAS

Una VPN ofrece las siguientes ventajas: [3]

- Conectividad extendida geográficamente
- Costos de operación menores que en una WAN tradicional
- Reduce los tiempos y costos de tránsito para usuarios remotos
- Aumenta la productividad
- Simplifica la topología de red
- Provee oportunidades de trabajo en redes globales
- Hace posible el soporte a esos trabajadores remotos
- Provee un retorno de inversión más rápido que una WAN tradicional

[3] Cómo funciona una VPN, http://ipref.wordpress.com/2009/04/28/vpn/, agosto 2009.

3.1.2 CARACTERÍSTICAS

Una VPN tiene las siguientes características:

- Confidencialidad: Se obtiene por medio de procesos de encriptación de los datos, los mismos que codifican los datos y sólo pueden ser descifrados por la computadora destino.
- Integridad: IPSec asegura que el paquete encriptado no pueda ser alterado en su trayecto, si se detecta alguna alteración el paquete es desechado.
- Autenticación de origen de datos: Verifica la identidad de la fuente de los datos evitando así ataques que intentan suplantar la identidad del transmisor.
- Data Tunneling/Traffic Flow Confidentiality: Tunneling es el proceso que encapsula un paquete dentro de otro y lo envía sobre un medio público (Internet).

Los protocolos más utilizados son PPTP/MPPE, IPSec, LPT2/IPSEC.

3.1.3 NECESIDADES DE LA EMPRESA

Contar con un servicio de soporte para la nueva aplicación E-Business, por lo que se propone contratar este servicio con la Compañía que la desarrolló.

Cabe señalar que este método de comunicación será utilizado por la Compañía que desarrolló la nueva aplicación para brindar soporte, o si requiere, realizar alguna actualización de la nueva aplicación.

La VPN es un medio de comunicación que se podrá utilizar para implementar un enlace permanente con la Compañía que brindará el Soporte Técnico de la aplicación E-Business, para facilitar las tareas de mantenimiento y actualización de la misma.

Este servicio se requiere en la Matriz.

3.1.4 USUARIOS DE LA VPN

Los usuarios que utilizarán este canal para realizar tareas de soporte y mantenimiento de los recursos informáticos serán el personal de la Compañía que desarrolló la aplicación E-Business con las debidas seguridades y responsabilidades que implica este acceso y sólo ellos serán los encargados de realizar las tareas para las cuales fueron contratadas.

Casi todas las tareas de soporte y mantenimiento serán realizadas en forma remota por la Compañía proveedora de la aplicación E-Business.

3.1.5 RESTRICCIONES

Se establece normas del control de acceso y utilización del servicio de VPN.

Las restricciones que se aplican son las siguientes:

- El enlace será únicamente utilizado para actividades de soporte y mantenimiento de la nueva aplicación y tareas de mantenimiento de los recursos informáticos a cargo de la Compañía proveedora de la aplicación E-Business.
- Toda actividad de soporte y mantenimiento de la nueva Aplicación o mantenimiento a los recursos informáticos deberán ser solicitadas previamente por la Empresa de Agua Potable.
- La Empresa de Agua Potable no podrá acceder a ningún recurso de la Compañía contratada para las actividades de soporte y mantenimiento de la aplicación E-Business.

El servidor VPN de la Empresa de Agua Potable deberá configurarse para cumplir con estas restricciones.

3.1.6 REQUERIMIENTOS DE HARDWARE

3.1.6.1 Requerimientos del Servidor VPN de la Empresa de Agua Potable

El dispositivo recomendado para la implementación de la VPN es:

- Un dispositivo VPN Server que a la vez brinde la opción de configurarse como Firewall.
- Mínimo un Puerto Ethernet LAN y Puerto WAN

Este dispositivo tiene las siguientes funcionalidades:

3.1.6.2 Requerimientos del Cliente VPN de la Compañía proveedora de la aplicación E-Business

El cliente VPN puede ser instalado en cualquier computador que cumpla con las siguientes características:

COMPUTADOR	REQUERIMIENTOS DE HARDWARE
PROCESADOR	Pentium II, III o IV
MEMORIA RAM	128 MB o superior
SISTEMA OPERATIVO	WINDOWS 2000: Profesional, Server o Advanced Server SP 3 o superior Windows XP
ESPACIO EN DISCO DURO	20 MB

Tabla 3.1 Requisitos de Hardware para Instalar Client VPN [4]

[4] Client VPN v 8.0.0 – Release Notes

3.1.7 REQUERIMIENTOS DE SOFTWARE

3.1.7.1 Software del Servidor VPN

El software del servidor está en el propio equipo y se accede por medio de una interfaz web.

El servidor debe configurarse mediante una Interfaz de Gestión amigable (vía web).

Se requiere configurar los servicios de servidor VPN.

3.1.7.2 Software del Cliente VPN

Se requiere el software Client VPN.

Este software se instalará y luego se configurará el canal de enlace entre el Servidor y Cliente. Previamente el Servidor deberá estar configurado para admitir conexiones remotas con una identificación, para luego configurar los accesos para el cliente.

3.2 ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD PARA APLICACIONES E-BUSINESS

3.2.1 SEGURIDAD DE CONTROL DE ACCESO

Una aplicación E-Business necesita tener un módulo de seguridad con el fin de que nadie pueda suplantar la identidad de un usuario y así obtener información de la Empresa; por lo tanto una aplicación de esta naturaleza debe cumplir con los siguientes requerimientos:

Identificación de Usuarios (ID).- Cada funcionario de la Empresa de Agua Potable debe tener una identificación para el ingreso a la aplicación E-Business. No existirán ID duplicadas lo que asegura que una ID le pertenece a un sólo usuario.

Políticas de Clave de Acceso.- Con la finalidad de dar robustez a una clave de acceso, la aplicación E-Business debe implementar políticas de claves tales como:

- Longitud de Clave con un mínimo de 6 caracteres
- Combinación de números y letras mayúsculas y/o minúsculas
- La clave esté compuesta por un mínimo de 4 letras y 2 números

Caducidad de Claves de acceso.- Cada usuario debe cambiar su clave de ingreso al sistema periódicamente a fin de que ésta no pueda ser sustraída por medios como “Ingeniería Social” para fines maliciosos.

Reseteo de Claves de acceso.- Es una facultad del Administrador de la aplicación E-Business y se usa con el fin de resetear una clave en caso de olvido o bloqueo de la misma.

Cambio de Clave Personal.- Todos los usuarios de la aplicación E-Business deben tener acceso a cambiar su clave personal en cualquier momento puesto que si existe la menor sospecha de sustracción de clave el usuario podrá cambiarla inmediatamente.

Definición de Perfiles.- La aplicación E-Business debe contar con un método de restricción de acceso a los procesos de la aplicación con el propósito de asegurar que un usuario solo realice las actividades relacionadas a su cargo.

Auditoría de transacciones.- Es importante mantener un registro de los cambios a datos sensibles de la Empresa, por lo que un módulo de Auditoría de Transacciones ayudará a verificar la identidad del usuario que realizó dicho cambio en caso de duda sobre variación de datos tales como: Parámetros del Sistema, Administración de usuarios, etc.

3.2.2 ENCRIPTACIÓN DE CLAVE

“La criptografía ayuda a proteger los datos para que no puedan ser vistos, proporciona mecanismos para la detección de datos modificados y facilita un medio de comunicación seguro en canales que, de otra forma, no serían seguros”.[5]

Existen varios métodos de encriptación de clave tales como:

DES (Data Encryption Standar), es un sistema de cifrado de bloques de 64 bits. Utiliza operaciones lógicas simples (transposiciones, desplazamientos y XOR´s). La clave de cifrado es de 56 bits.

TDES (Triple Data Encryption Estándar), es un algoritmo que realiza el cifrado DES tres veces utilizando un clave de 192 bits.

VALORES HASH, un valor hash es una representación numérica de un segmento de datos. Si aplica un algoritmo hash a un párrafo de texto simple y cambia solo una letra del párrafo, el valor hash subsiguiente producirá un valor distinto. Si el valor hash es criptográficamente seguro, su valor cambiará significativamente. Por ejemplo, si se cambia únicamente un solo bit de un mensaje, una función hash segura puede generar un resultado que difiera en un 50 por ciento. Muchos valores de entrada pueden aplicar un algoritmo hash al mismo valor de salida. Sin embargo, técnicamente es poco factible encontrar dos entradas distintas cuyo valor hash sea el mismo.

AES (Advanced Encryption Standar), es el predecesor de TDES, es un algoritmo de cifrado de bloques, el tamaño del bloque es de 128 bits y la clave es de 128, 192 o 256 bits.

El método de encriptación de Clave que la aplicación E-Business utiliza son Valores hash pues tiene altas probabilidades de que al cambiar un solo bit el

[5] Información general sobre criptografía, http://msdn.microsoft.com/es-es/library/92f9ye3s.aspx, noviembre 2007

resultado lo altere en el 50% por lo que resultará casi imposible descifrar la clave. Complementariamente a este método de encriptación de clave se ejecutan dos procedimientos adicionales que transforman el resultado de la encriptación a un campo de un tamaño específico y lo guarda como un hexadecimal, haciendo que la encriptación de la clave sea más difícil de descifrar.

3.2.2.1 Encriptación de Clave en Base de Datos

Para que las claves de los usuarios de la aplicación no sean visibles a cualquier persona, es necesario aplicar un algoritmo de encriptación de datos antes de que ésta sea almacenada en la BDD.

Los procedimientos de encriptación de clave aseguran que ningún funcionario de la Empresa pueda descifrarla, en caso de acceder permitida o fraudulentamente a la Base de Datos de la aplicación.

3.2.3 COMUNICACIONES VÍA INTERNET

Actualmente las empresas de Agua Potable se están apoyando en las Instituciones Bancarias para que éstas se constituyan en Cajas Recaudadoras de la Empresa con la finalidad de receptar los pagos del Cliente por concepto del servicio de Agua Potable, por lo que se requiere comunicar la Institución Bancaria con la Matriz a través de Internet.

3.2.3.1 Protocolo HTTPS

El protocolo HTTPS (Hypertext Transfer Protocol Secure) crea un canal seguro sobre una red insegura. Se utiliza para brindar confidencialidad a los datos a través de métodos de encriptación utilizando certificados digitales que se transmiten por un enlace público (Internet).

3.3 ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD PARA LA EMPRESA PROVEEDORA DE SERVICIOS DE INTERNET

Los Proveedores de Internet o ISP, son empresas que ofrecen el acceso a servicios de Internet por un costo mensual.

Actualmente existen varias formas de conectarse a Internet y los ISP de acuerdo a la cobertura ofrecen conexiones de:

- Dial-up, es una conexión hacia los nodos de Internet utilizando los canales telefónicos de una Empresa de Telecomunicaciones.
- Banda Ancha, es la utilización de la capacidad adicional de la infraestructura de cobre de los portadores o proveedores de servicios que permite alcanzar velocidades de conexión superiores al dial-up.
    - xDSL (Utiliza par de cobre del abonado telefónico)
    - Cable Módem (Utiliza cable coaxial de la televisión por cable)
    - PLC (Utiliza la infraestructura del Sistema de Energía Eléctrica)

De acuerdo a la velocidad de conexión los ISP ofrecen gran cantidad de propuestas para el cliente. Sin embargo, cada una de estas propuestas tienen inmerso el concepto de compartición y generalmente las propuestas más baratas son aquellas que tienen una compartición más alta, por ejemplo: 1:8 que significa que para el mismo canal se conectarán hasta 8 usuarios y en horas de mayor demanda se siente el retardo en la comunicación.

3.3.1.1 Requerimientos de Seguridad

Los requerimientos de Seguridad que el ISP debe proporcionar son:

- Disponer de personal para que administre la seguridad de Nodo.
- Disponer de filtros para detección de virus en la red para detener la propagación de los mismos en lo posible.

- Detección temprana de intentos de ataque. Seguridad ante la intrusión.
- Uso de criptografía para el transporte seguro de datos.
- Asegurar la privacidad en:
    - Transacciones comerciales, financieras y comercio electrónico.
    - Transporte seguro de información confidencial. Firma Digital.
    - Confidencialidad en la trasferencia de ficheros.
- Proveer filtros de navegación a páginas no autorizadas.
- Equipos de Hardware como Routers y Firewalls que eviten intentos de ataque provenientes del Internet.

3.4 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD PARA LA VPN

"Si bien Internet permite ahorros considerables como mecanismo de transporte, también permite posibles amenazas a la seguridad. Las empresas de hoy afrontan el desafío de tener que proteger plenamente los datos de las ubicaciones remotas, al mismo tiempo que administran y distribuyen políticas críticas de seguridad en esas mismas ubicaciones".[6]

Es importante determinar las políticas de seguridad para la conectividad a través de VPN con la finalidad de resguardar los recursos informáticos y la información.

[6] Symantec Gareway Security, http://eval.symantec.com/mktginfo/enterprise/fact_sheets/25657-DS00147-SL_SGS400_fs.pdf, Agosto 2009

3.4.1 OBJETIVO

Establecer políticas de seguridad para el establecimiento de VPN con la Compañía proveedora de la aplicación E-Business, definir responsabilidades y consecuencias del uso mal intencionado.

3.4.2 ALCANCE

Las políticas de seguridad son aplicables entre la Compañía proveedora de la aplicación E-Business y la Empresa de Agua Potable.

3.4.3 RESPONSABILIDAD

Las políticas de seguridad serán implementadas en el servidor VPN de la Empresa de Agua Potable y estará a cargo del Jefe de Informática.

3.4.4 POLÍTICAS DE SEGURIDAD

3.4.4.1 Configuración del Enlace

- La Compañía proveedora de la aplicación E-Business será la encargada de la configuración del servidor VPN en la Empresa de Agua Potable y en sus propios servidores necesarios para implementar el enlace.

3.4.4.2 Utilización del Enlace

- El enlace VPN será utilizado para comunicar a la Compañía proveedora de la aplicación E-Business para tareas de soporte y mantenimiento de la aplicación.
- La Compañía proveedora de la aplicación establecerá la comunicación VPN previa solicitud por parte de la Empresa de Agua Potable para actividades de soporte técnico en temas concernientes a la aplicación.
- Para instalación de nuevas versiones o modificaciones a la aplicación la Compañía proveedora de la aplicación podrá establecer la comunicación VPN previa notificación al Jefe de Informática.

- La Compañía proveedora de la aplicación designará al personal adecuado para las tareas de soporte y mantenimiento de la aplicación a través de la comunicación VPN y empleará el enlace para atender las solicitudes de la Empresa de Agua Potable.

3.5 ANÁLISIS DE COSTOS DE EMPRESAS PROVEEDORAS DE SERVICIOS DE INTERNET

En nuestro país el organismo que se encarga de controlar y supervisar la operación y desempeño de los ISP's es la Superintendencia de Telecomunicaciones.

Los ISP´s autorizados para ofrecer servicios de Internet se listan en el **ANEXO 1.**

Los Proveedores de Servicios de Internet ofrecen varios servicios a más del acceso a Internet, entre ellos: Hosting, Correo, FTP, DNS, etc.

3.5.1 CONSIDERACIONES

Para este análisis se considerará lo siguiente:

- ISP autorizados por la Superintendencia de Telecomunicaciones (Ver **ANEXO 1**) para brindar servicio de acceso a Internet en el Ecuador.
- Tecnología de acceso a Internet: Banda Ancha
    - xDSL
    - Cable Módem
- Compartición del Canal
- Ancho de Banda
- Disponibilidad
- Soporte Técnico

3.5.2 ANÁLISIS DE COSTOS

Para realizar el análisis de costos para la contratación del servicio de Internet se deberá tomar en cuenta además del costo el beneficio que pueda ofrecer el Proveedor de Servicios de Internet.

Un factor importante es el presupuesto referencial asignado por las empresas para la contratación del servicio, aunque éste no debería ser el factor determinante, sino más bien el beneficio que puede obtener considerando que la información sensible de la Empresa será encriptada para su envío a través de un medio público (Internet).

Actualmente la Corporación Nacional de Telecomunicaciones del Ecuador CNT, es la propietaria de la mayor infraestructura para transmisión de datos en el Ecuador.

Se evaluará la calidad del servicio y los costos de acceso a Internet en una muestra de Proveedores de Internet para la ciudad de Ambato.

3.5.2.1 Parámetros de Calidad de Servicio

3.5.2.1.1 Disponibilidad

Es el acceso ininterrumpido a los servicios que prestan los Proveedores de Internet. Es la capacidad del canal para enrutar paquetes de datos a su destino. Es importante que el canal esté disponible, pues la saturación del canal implica retardo y pérdida de paquetes.

3.5.2.1.2 Confiabilidad

Se mide por el porcentaje de paquetes perdidos durante la trayectoria a su destino bajo condiciones normales de funcionamiento del servicio.

3.5.2.1.3 Soporte Técnico

Es la calidad de atención al cliente que el ISP pueda ofrecer ante la presencia de algún incidente en el servicio, tales como: daños en la última milla, equipos de comunicación en el ISP, módems, la conexión deja de funcionar.

3.5.2.1.4 Tiempo de Respuesta

Es el tiempo que el ISP tarda en responder y solucionar un problema cuando éste se atribuye al ISP y no se encuentra fuera de los límites del mismo.

3.5.2.1.5 Cobertura

Describe la zona geográfica donde el ISP presta los servicios de acceso a Internet.

La Tabla 3.2 indica los parámetros de calidad de servicio más relevantes que se debe tomar en cuenta para seleccionar un ISP y la posterior contratación del servicio.

PARÁMETRO . ISP	ANDINANET	TELCONET	TV CABLE	PORTA	INTERACTIVE
DISPONIBILIDAD	99.9%	99.9%	99.6%	99.9%	99.6%
CONFIABILIDAD	Pérdida de paquetes < 1%	Pérdida de paquetes cercanos al 0%	Pérdida de paquetes < 1%	Pérdida de paquetes < 1%	Pérdida de paquetes < 1%
SOPORTE TÉCNICO	8 x 7 x 365 días	24 x 7 x 365 días	24 x 7 x 365 días	24 x 7 x 365 días	12 x 7 x 365 días
TIEMPO DE RESPUESTA	2 a 8 horas	30 min a 2 hrs.	2 horas	-	Depende del plan
COBERTURA	Todo el país	Sierra, GYE	UIO, GYE, AMB	UIO, GYE, AMB	UIO,GYE,AMB (Andinadatos)

Tabla 3.2 Calidad de Servicio de los Proveedores de Internet en Ambato

Fuente: Información de ISP

3.5.2.2 Costos de Acceso a Internet

El costo de acceso a Internet está asociado a la capacidad del canal de transmisión y al nivel de compartición.

Existen diferentes capacidades del canal y depende del Proveedor.

Los niveles de compartición son: 1:1, 2:1, 4:1, 8:1 y en algunos casos 16:1

Las Tablas 3.3, 3.4, 3.5, 3.6 y 3.7 presentan los costos de acceso a Internet para ADSL y Cable MODEM que los ISP ofrecen a clientes Corporativos.

ISP: Andinanet – ADSL

CANAL (Kbps) / .....COMPARTICIÓN	1:1	2:1	4:1	8:1	16:1
100 / 75	USD $ 72	USD $ 58	USD $ 50	USD $ 46	USD $ 44
220 / 75	USD $ 116	USD $ 86	USD $ 69	USD $ 60	USD $ 55
300 / 550	USD $149	USD $107	USD $ 84	USD $ 72	USD $ 65
550 / 150	USD $ 274	USD $ 198	USD $ 156	USD $ 133	USD $ 120
700 / 300	USD $ 354	USD $ 257	USD $ 204	USD $ 174	USD $ 158
1100 / 300	USD $ 514	USD $ 363	USD $ 278	USD $ 232	USD $ 207
1600 / 300	USD $ 738	USD $ 518	USD $ 396	USD $ 328	USD $ 291

Tabla 3.3 Costos de Acceso a Internet ADSL- Andinanet

Fuente: Andinanet

ISP: Telconet - ADSL

CANAL (Kbps) / .....COMPARTICIÓN	1:1	2:1	4:1	8:1	16:1
150	USD $ 74	USD $ 54	USD $ 44	USD $ 39	USD $ 37
300	USD $ 122	USD $ 83	USD $ 64	USD $ 54	USD $ 50
600	USD $210	USD $132	USD $ 94	USD $ 74	USD $ 65
800	USD $ 282	USD $ 178	USD $ 126	USD $ 100	USD $ 88
1200	USD $ 420	USD $ 265	USD $ 187	USD $ 148	USD $ 130

Tabla 3.4 Costos de Acceso a Internet ADSL - Telconet

Fuente: Telconet

ISP: TV Cable - Cable MODEM

CANAL (Kbps) / .....COMPARTICIÓN	2:1	4:1	8:1
150	USD $ 60	USD $ 48	USD $ 35
300	USD $ 81	USD $ 65	USD $ 46
600	USD $ 94	USD $ 75	USD $ 53
800	USD $ 123	USD $ 98	USD $ 67
1000	USD $ 150	USD $ 120	USD $ 84
2000	USD $ 300	USD $ 240	USD $ 147

Tabla 3.5 Costos de Acceso a Internet Cable MODEM - TV Cable

Fuente : TV Cable

ISP: Interactive - ADSL

CANAL (Kbps) / .....COMPARTICIÓN	1:1	2:1	4:1	8:1
100 / 75	USD $ 135	USD $ 104	USD $ 69	USD $ 48
300 / 300	USD $ 213	USD $ 158	USD $ 105	USD $ 74
500 / 150	USD $ 370	USD $ 285	USD $ 190	USD $ 133
1100 / 300	USD $ 643	USD $ 495	USD $ 330	USD $ 231
1600 / 300	USD $ 952	USD $ 733	USD $ 489	USD $ 342

Tabla 3.6 Costos de Acceso a Internet ADSL - Interactive

Fuente: Interactive

ISP: Porta - ADSL

CANAL (Kbps) / .....COMPARTICIÓN	1:1	2:1	4:1	8:1
256	USD $ 168	USD $ 120	USD $ 80	USD $ 48
512	USD $ 262	USD $ 187	USD $ 125	USD $ 74
760	USD $ 408	USD $ 292	USD $ 195	USD $ 133
1024	USD $ 588	USD $ 420	USD $ 280	USD $ 231

Tabla 3.7 Costo de Acceso a Internet ADSL - Porta

Fuente: Porta

3.5.2.3 Evaluación y Recomendación

De las tablas 3.2 a 3.7 se recomienda lo siguiente:

Respecto a la calidad del Servicio:

- Los ISP Telconet y TV Cable son los que mejor calidad ofrecen aunque difieren en el tiempo de disponibilidad en el 0.3%.

- Telconet y TV Cable ofrecen igual Soporte Técnico y tiempos de respuesta ante incidentes.

- Los ISP Telconet y Porta tienen infraestructura propia. Telconet tiene varios años de experiencia en el mercado y TV Cable en la ciudad de Ambato es reciente lo que indica que el ancho de banda tiene pocas probabilidades de saturación en la actualidad.

Respecto al costo de Acceso a Internet, la Empresa de Agua Potable ha considerado que el ancho de banda más adecuado considerando el número de estaciones que se conectarán al servicio es de 2000 kbps con un nivel de compartición de 2:1, por lo que se consideró lo siguiente:

- Los ISP Telconet y TV Cable tienen el precio más bajo en el mercado.

3.5.2.3.1 Recomendación

Se recomienda que el Proveedor del Servicio de Internet que debe contratar la Empresa de Agua Potable es **TV Cable,** por lo siguiente:

- Tiene cobertura para la ciudad de Ambato

- El servicio de Soporte Técnico y tiempo de respuesta en caso de algún incidente en el servicio es adecuado para la gestión de la Empresa.

- La confiabilidad y disponibilidad se encuentran en un rango aceptable de servicio.

- El costo del servicio de Acceso a Internet para un ancho de banda de 2000 kbps para el nivel de compartición 2:1 es el menor del mercado.

- Dado que en la ciudad de Ambato TV Cable es uno de los ISP más recientes se considera que el canal de comunicación no se encuentra saturado.

3.6 DISEÑO DE LA ARQUITECTURA VPN PARA SOPORTE REMOTO A LAS APLICACIONES E-BUSINESS

El diseño de la arquitectura VPN para soporte a la aplicación E-Business de la Empresa de Agua Potable implica lo siguiente:

- Definición y Configuración del Dispositivo VPN
- Definición y Configuración del Firewall
- Establecimiento de las políticas de seguridad de VPN
- Definición y Configuración del Cliente VPN en la Compañía Proveedora de la aplicación

El siguiente esquema es el diseño de la arquitectura VPN para brindar soporte y mantenimiento a la aplicación E-Business:

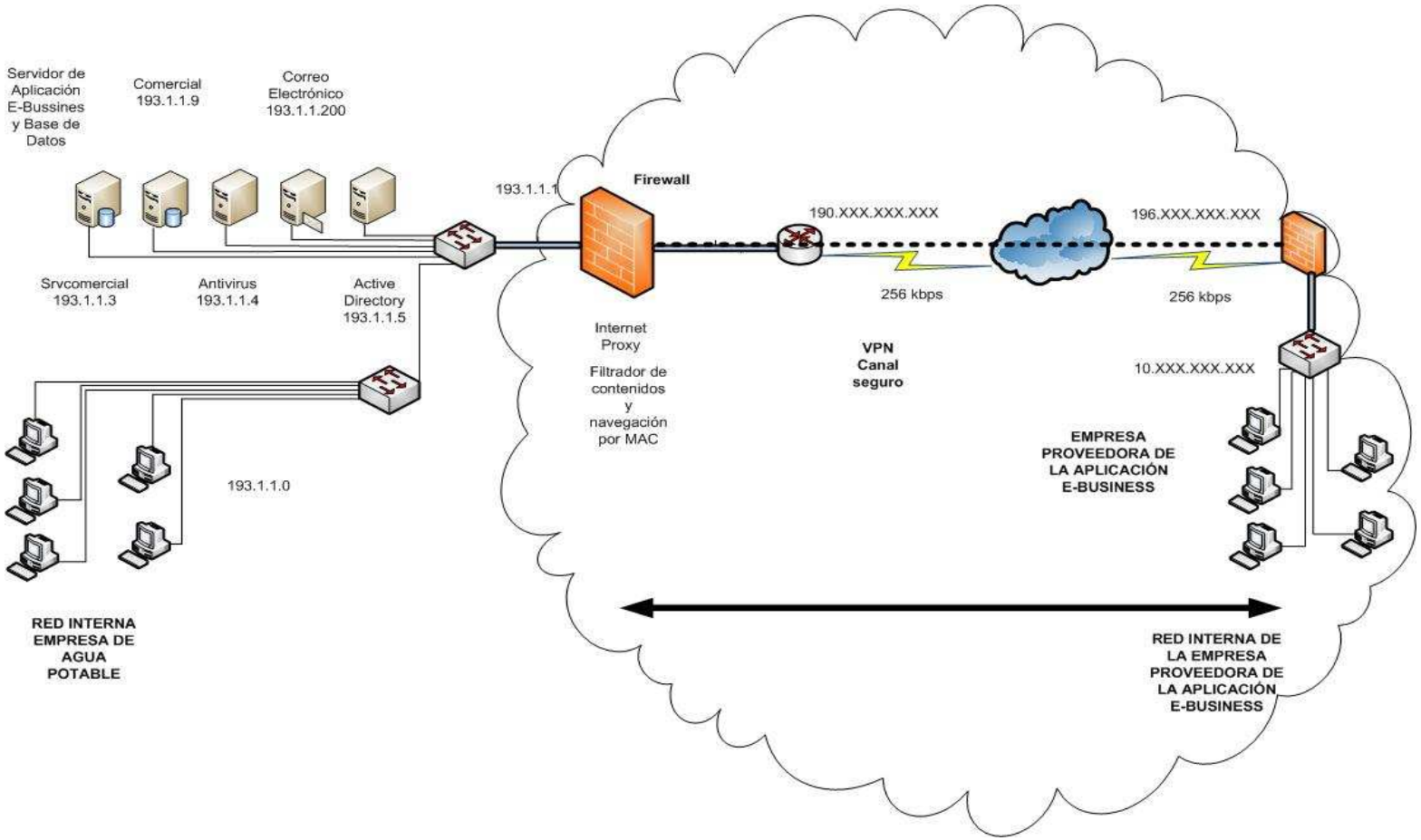


Figura 3.1 Arquitectura VPN para Soporte de Aplicaciones E-Business

Fuente: La Autora

CAPÍTULO 4. PREPARACIÓN DE LA PROPUESTA TÉCNICA ECONÓMICA PARA UNA INTERRED SEGURA

Con el objetivo de preparar adecuadamente una propuesta para la inversión de un proyecto, se debe considerar todos los elementos que aporten a la consecución de este objetivo como son las alternativas de solución con sus costos correspondientes para la implementación de la infraestructura de Interred segura soporte de aplicaciones E-Business.

En este capítulo se analizará los diferentes factores que intervienen para generar una Propuesta Técnica Económica para una Interred segura.

Para este caso de estudio, el análisis del costo del proyecto se enfocará en los costos totales que se generan para la implementación del mismo.

4.1 COMPARACIÓN DE PROVEEDORES DE HARDWARE, SOFTWARE Y COMUNICACIONES

4.1.1 PARÁMETROS DE CALIFICACIÓN DE CALIDAD

Para comparar los proveedores de hardware, software y comunicaciones se consideran como parámetros de calificación de calidad: Servicio, Soporte Técnico, Presencia en el mercado y Experiencia.

4.1.1.1 Servicio

Los servicios que ofertan como proveedor, fabricante e investigador de nuevas tecnologías para proveer hardware, software y comunicaciones.

4.1.1.2 Soporte Técnico

Como parte del servicio de un proveedor de hardware, software y comunicaciones, se evalúa el soporte técnico especializado que pueda brindar en los distribuidores autorizados en el Ecuador.

4.1.1.3 Presencia en el Mercado

Las continuas investigaciones permiten a los fabricantes de hardware y software y comunicaciones ofrecer constantemente una gran variedad de dispositivos de hardware accesible, software y servicio de comunicaciones que permita a las empresas seleccionar el dispositivo, software y servicio de comunicación que se ajuste a sus necesidades.

4.1.1.4 Experiencia

El tiempo que el Proveedor se ha mantenido en el mercado brindando soluciones ágiles y con tecnología de punta con el fin de solventar los requerimientos de las empresas.

4.1.2 PROVEEDORES DE HARDWARE

En el mercado existen innumerables proveedores de hardware por lo que se han considerado las marcas que en los últimos años su presencia ha marcado la diferencia entre otras.

CALIDAD / FABRICANTE	SERVICIO / PRODUCTOS	PRESENCIA	EXPERIENCIA	SOPORTE TÉCNICO
DLINK	• **Garantía Extendida**: Hasta 2 años • **Instalación:** De acuerdo a los requerimientos del usuario final • **Configuración:** De acuerdo a los requerimientos del usuario final • **Asesoría Técnica y Capacitación:** Con personal especializado en función de los requerimientos del cliente. • **Soporte**: 1 año • **Mantenimiento:** 1 año	Desde 1986 se desarrolló al mercado global. Tiene más de 90 distribuidores en el mundo.	Uno de los principales líderes mundiales en proveer hardware de red,conectividad y comunicación de datos desde 1986.	Ofrece canales de comunicación: • 1800-035-465 • Soporte en línea • Preguntas y Respuestas Frecuentes (FAQ´s) • Formularios de preguntas a Soporte
SYMANTEC	• Software de Antivirus • Hardware de Comunicaciones para redes.	Está presente en el mercado desde 1982.	Líder a nivel mundial en proveer Hardware y Software de	Provee soporte Técnico a toda hora en su portal web para los productos que se ofertan por los canales de correo electrónico,

CALIDAD / FABRICANTE	SERVICIO / PRODUCTOS	PRESENCIA	EXPERIENCIA	SOPORTE TÉCNICO
	• Equipos de protección de Redes • Soporte Técnico por medio de correo electrónico • Preguntas y Respuestas Frecuentes (FAQ's)	Tiene varios distribuidores alrededor del mundo puesto que sus clientes depositan su confianza en los productos que ofertan gracias a su calidad.	conectividad de redes y comunicaciones. Con una experiencia de 27 años en el mercado.	telefónico.
UBIQUITI	• Soluciones para interconexión de redes por Wireless • Soluciones ISP WiMax • Soluciones Wi-Fi indoor / Outdoor	Desde hace varios años no especifica el portal Web. Dispone de oficinas en el mundo en Europa, Asia y América.	No especifica el Portal Web	Brinda las 24 horas del día a través de canales como: • correo electrónico • Skype • Vía Telefónica • Chat
MIKROTYK	• Soluciones inalámbricas en Hardware y software. • Routers inalámbricos	Está en el mercado desde 1997, presente en el mercado en Europa y	12 años de experiencia en proporcionar	Por medio de canales como: • Correo • Vía telefónica

CALIDAD / FABRICANTE	SERVICIO / PRODUCTOS	PRESENCIA	EXPERIENCIA	SOPORTE TÉCNICO
	• Software con características de Firewall, router, administrador de ancho de banda, VPN, Access Point, etc. lo que hace de sus productos una herramienta de mucha ayuda y económica al momento de implementar seguridad en las redes.	América	soluciones inalámbricas.	• Chat

Tabla 4.1 Esquema Comparativo de Proveedores de Hardware de Comunicaciones

Fuente: Portales Web de Fabricantes

4.1.3 PROVEEDORES DE SOFTWARE

Actualmente, en el país existen algunas empresas de Desarrollo de Software, orientadas a diferentes líneas de servicio, por lo que para este estudio se ha considerado las empresas que ofertaron sus servicios para el desarrollo de la aplicación E-Business para la Empresa de Agua Potable.

Por confidencialidad de la Empresa adjudicada se protegerá su identidad bajo el nombre de SPCS SOFTWARE.

. CALIDAD / EMPRESA (SW)	SERVICIO / PRODUCTOS	PRESENCIA	EXPERIENCIA	SOPORTE TÉCNICO
SPCS SOFTWARE	• Sistema Informático Integrado • Courier • Recuperación de Cartera • Facturación • Sistema Financiero, entre otros. • Asesoría en Infraestructura • Soporte Técnico VPN	Formalmente en el país desde hace 5 años.	5 años de Experiencia en Implantación de Sistemas. 5 años de experiencia en Sistemas de Courier, recuperación de Cartera, Facturación.	8 horas x 5 días por semana durante la vigencia de la Garantía Técnica del Producto.
BUILDER SOLUTIONS	• Desarrollo de Sistemas en cualquier ámbito.	Presente en el país desde mayo/2005	No indica Portal Web (Copyrigth 2006)	No indica en el Portal Web (Copyrigth 2006)
KRUGER	• Capacitación • Consultoría	Desde mayo / 1996	15 años de experiencia al	No indica en el portal.

. CALIDAD / EMPRESA (SW)	SERVICIO / PRODUCTOS	PRESENCIA	EXPERIENCIA	SOPORTE TÉCNICO
	• Software a la medida • Infraestructura • Procesos Electorales		servicio de distintas organizaciones de tipo financiero, comercial, industrial y de servicios. Respecto a Software para Empresas de Agua Potable no tiene experiencia (Portal Kruger-Clientes)	

Tabla 4.2 Proveedores de Software para Empresas de Agua Potable

Fuente: Catálogo de Software ComputerWorld, Portal de las Empresas, Superintendencia de Compañías

Según la tabla 4.2 la Empresa más opcionada para el desarrollo de la aplicación E-Business para la Empresa de Agua Potable es SPCS SOFTWARE por la experiencia y presencia en el mercado de empresas de Agua Potable comprobadas.

Adicionalmente, se deben considerar las Empresas desarrolladoras de Sistemas Operativos, Antivirus, software de oficina, etc., tales como Microsoft o Symantec que son empresas reconocidas a nivel mundial.

4.1.4 PROVEEDORES DE COMUNICACIONES

Los proveedores de comunicaciones que se han considerado son los Proveedores de Internet autorizados por la Superintendencia de Telecomunicaciones del Ecuador para la ciudad de Ambato.

CALIDAD / ISP	SOLUCIONES	PRESENCIA EN EL MERCADO	EXPERIENCIA	SOPORTE TÉCNICO
ANDINANET	Tecnología SDSL Compartición 1:1	Es el proveedor de Internet con más usuarios dedicados en el país (ver **ANEXO 3**)	9 años de experiencia en brindar servicio de acceso a Internet.	8 x 7 x 365 días
TELCONET	Tecnología SDSL Compartición 1:1	Tiene cobertura con una infraestructura propia en FO y cable cobre en 20 ciudades del país.	13 años de experiencia en telecomunicaciones en el país.	24 x 7 x 365 días
TV CABLE	Tecnología Cable Modem Compartición 1:1	Está presente en el país desde 1986. En 1987 inicia su operación con servicio de TV y en los últimos años ha despuntado como uno de los proveedores de Internet más solicitados.	En el ámbito del servicio de acceso a Internet tiene pocos años.	24 x 7 x 365 días
INTERACTIVE	Tecnología SDSL Compartición 4:1	Tiene varios años en el país ofertando servicios de acceso a Internet.	-	12 x 7 x 365 días

Tabla 4.3 Proveedores de Internet en Ecuador

Fuente: Portales de ISP's

De acuerdo a la Tabla 4.3 los proveedores de Internet más opcionados por el servicio ofertado, presencia en el mercado, experiencia y soporte Técnico son:

- Andinanet por poseer la infraestructura de comunicación más grande del país.
- Telconet por poseer una infraestructura propia y de calidad.
- TV Cable por ser el ISP más reciente en Ambato por lo que se deduce que el ancho de banda tiene pocas probabilidades de saturación a corto plazo.

De los tres ISP mencionados el más opcionado es TV Cable de acuerdo a las especificaciones que requiere la Empresa.

4.2 ANÁLISIS DE COSTOS Y ALTERNATIVAS DE HARDWARE, SOFTWARE Y COMUNICACIONES

La Empresa de Agua Potable de Ambato desde hace algunos años ha venido implementando en su infraestructura básica computadores y elementos de red con tecnología INTEL. Adicionalmente, por las especificaciones de Hardware que la Compañía proveedora de la aplicación E-Business sugirió la Empresa adquirió hace unos meses el nuevo servidor para la aplicación en mención.

4.2.1 ALTERNATIVAS DE HARDWARE

A continuación se listan los precios de equipos de comunicación necesarios para plantear la propuesta Técnica Económica.

4.2.1.1 Antenas

Los elementos de hardware necesarios para amplificar la señal de transmisión.

MODELO ANTENA	MARCA	COSTO UNITARIO (USD $)
12 dbi Omnidireccional 2.4 Ghz	Netkrom	135
12 dbi Omnidireccional 2.4 Ghz	Trednet	131
15 dbi Omnidireccional 2.4 Ghz	Hyperlynk	200
15 dbi Direccional 2.4 Ghz	Panel	100
Antena Sectorial Til-tek 2.4 Ghz 14dbi 120º Internet	Til-Tek	220

Tabla 4.4 Costos de Antenas de 12, 14 y 15 dbi

Fuente: Internet Mercado Libre

Para el diseño propuesto en la sección 2.5 y considerando que la distancia física de la Agencia Izamba con la Matriz sobrepasa los 3 kms se necesita una antenas de 15 dbi y dos para la Repetidora; en total son necesarias 3 antenas de 15 dbi direccionales (Sectoriales).

En la Matriz se colocará una antena Omnidireccional para captar las señales provenientes de las Agencias.

Para la Matriz se colocará una antena *Hyperlink de 15 dbi 2.4 Ghz Omnidireccional*, a diferencia de las otras propuestas en este documento esta antena tiene la capacidad de retransmitir la señal de Internet a varios km de distancia ideal para conectar oficinas y agencias a través de VPN's.

Para la Agencia Izamba y la Repetidora por encontrarse a una distancia mayor a 3 kms se instalará la antena *15 dbi Panel Direccional 2.4 Ghz*, pues la capacidad de transmisión de ésta puede enviar la señal a varios km de distancia y su comunicación es punto a punto con la Matriz.

4.2.1.2 Access Point

Es el equipo de comunicación inalámbrico para conectar la red de la Matriz con las redes de las Agencias.

MODELO	MARCA	COSTO UNITARIO (USD $)
RB411	Mikrotik	400
DWL-2700AP	D-Link	1,035
Readylink Wireless A.P 2.4/5ghz 802.11a+b+g – Isp	Readylink	1,160

Tabla 4.5 Costos de Access Point 2.4 Ghz

Fuente: Aldeberan

Se recomienda el uso del *AP Mikrotik RB411* ya que su sistema operativo le convierte en un router altamente sofisticado, es un firewall que brinda protección contra ataques externos a la red y es un manejador de ancho de banda.

4.2.1.3 Radios

Son los dispositivos que se instalarán en cada Agencia para establecer la comunicación con la Matriz.

MODELO	MARCA	COSTO UNITARIO (USD $)
Nano Station 2	Ubiquiti	150.00
Nano Station 5	Ubiquiti	166.00

Tabla 4.6 Costos de Radios

Para cada Agencia y la Repetidora se utilizarán los Radios Ubiquiti Nano Station 2 (2Ghz), por su diseño que combina un sistema de antena 4 hi-gain, avanzada arquitectura de radio, por su tecnología de firmware que permite gran rendimiento, estabilidad y el rendimiento de capacidad rivaling incluso en redes WiMax.

4.2.1.4 Firewall / Gateway

Es un sistema de seguridad, encargado de proteger una red de área local de accesos no autorizados desde una WAN a la que esté conectada.

MODELO	MARCA	COSTO UNITARIO (USD $)
SGS 360	Symantec	1,000
ZyWall USG 1000	ZyXel	3,676
ZyWall 35-35	ZyXel	570

Tabla 4.7 Costos de Firewall / Gateway

Fuente: Aldeberan

Los tres equipos de la Tabla 4.7 ofrece características de seguridad como Firewall de inspección en estado, permite configurar VPN, aplica políticas de seguridad, detección de intrusos, prevención de intrusos, filtros de contenido, es un Gateway de Internet (Proxy), puertos WAN, adicionalmente es un switch de 8 puertos. Sin embargo, los modelos Zywall de ZyXel para aplicar las características especiales como antivirus incorporado, aplicación de políticas, IDS, se requiere una suscripción para su aplicación por lo cual el costo referencial será mayor.

En el caso de Symantec Gateway Security 360, la aplicación tiene todo el software necesario para comenzar, adicionalmente incluye la licencia que elimina el problema de administrar las licencias y el costo mensual de suscripciones, por lo tanto se recomienda que el equipo Firewall a instalar sea el SGS 360.

4.2.2 ALTERNATIVAS DE SOFTWARE

4.2.2.1 Software de Aplicación E-Business

El 10 de abril del 2008 el Señor Presidente de la República del Ecuador establece mediante Decreto 1014 el uso de Software Libre en los sistemas y

equipamientos informáticos; esto implica que se deberá obtener el código fuente para realizar mejoras al mismo (Ver **ANEXO 3,** artículos 1 y 2).

Sin embargo, los estudios han demostrado que a pesar de que el software libre puede disminuir el costo inicial de desarrollo de un proyecto, sin embargo, el mantenimiento del mismo es mucho más caro que desarrollar una aplicación en plataforma de software propietario.

En nuestro país, las empresas desarrolladoras de software a medida utilizan la plataforma Microsoft pues el costo de mantenimiento de las aplicaciones es menor que el software desarrollado con herramientas Open Source.

Por otro lado, no se ha desarrollado una aplicación E-Business para empresas de Agua Potable con herramientas Open Source.

4.2.2.2 Software Propietario

El mismo Decreto 1014, artículo 4 faculta el uso de software propietario en casos de que no exista una aplicación desarrollada bajo herramientas Open Source (Ver **ANEXO 3**).

Por lo expuesto anteriormente, las empresas de Agua Potable están facultadas para adquirir software propietario para integrar sus procesos. En este caso la aplicación E-Business se desarrolla en plataforma Microsoft por la Compañía señalada en la sección 4.1.3.

El Costo por desarrollo e implementación de la aplicación E-Business no se incluye como parte del estudio para generar la Propuesta Técnica y Económica.

En cuanto al Sistema Operativo de servidores y estaciones de trabajo se presentan varias opciones de costo provenientes directamente del Proveedor o a través de sus distribuidores autorizados.

De la misma manera sucede con software de Antivirus, de Oficina, e incluso con software de desarrollo.

La tabla 4.5 muestra el costo de las licencias del software antivirus para el nuevo servidor que será implementado para la nueva aplicación E-Business.

SOFTWARE ANTIVIRUS	CANT.	COSTO UNITARIO (USD $)	COSTO TOTAL (USD $)
Symantec Endpoint Proteccion	30	54	1,620
Mcafee	30	44	1,320
Eset Smart Security	30	30	900

Tabla 4.8 Costos de Licencias de Antivirus por Año

Fuente: PinSoft

Los antivirus listados en la Tabla 4.4 tienen características similares, por lo que se recomienda a Eset Smart Security por ser el de menor costo para la Empresa de Agua Potable.

SOFTWARE	CANT.	COSTO UNITARIO (USD $)	COSTO TOTAL (USD $)
Sistema Operativo Windows 2003 Server	1	**853**	**853**
SQL Svr. Standard Edtn. 2005 Win 32 Spanish OLP NL Qualified	1	896	896
Eset Smart Security	30	30	900
Total (USD $):			**2,649**

Tabla 4.9 Costo de Software para el Servidor de la aplicación E-Business

Fuente: PinSoft

No se incluye licencias de IUWebControls, Framework 2.0 y Crystal Reports por cuanto la Empresa de Agua Potable ya las tenía adquiridas, por lo que no se consideran como parte de los costos de Software para el Servidor.

4.2.3 ALTERNATIVAS DE COMUNICACIONES

Las alternativas de comunicación que ofrecen los ISP autorizados para la ciudad de Ambato se muestran en la Tabla 4.10; se considera el ancho de banda (Canal), el nivel de compartición y precio.

ISP	ANDINANET	TELCONET	TV CABLE	INTERACTIVE
COMPARTICION / CANAL (Kbps)	1:1	1:1	1:1	4:1
128	USD $ 99	USD $ 100	-	USD $ 94
150	-	-	USD $ 140	-
256	USD $ 185	USD $ 180	-	USD $ 133
300	-	-	USD $ 200	-
384	-	-	-	USD $ 189
512	USD $ 318	USD $ 300	-	USD $ 245
600	-	-	USD $ 250	-
768	-	-	-	USD $ 335
1000	-	-	USD $ 400	-
1024	USD $ 557	USD $ 520	-	-
1500	-	USD $ 800	-	-
2048	USD $ 1007	USD $ 900	-	-

Tabla 4.10 Costo de Enlace Dedicado por mes

Fuente: ISP

De acuerdo a los requerimientos expuestos en la sección 2.5.1 se plantea un esquema de integración de las Redes LAN de las Agencias a la Matriz por medio de enlaces dedicados a través de Radios. A modo de estudio se evaluará esta solución.

Para aplicar esta solución se tomará en cuenta un enlace dedicado con un ancho de banda de 1000 a 1024 kbps.

En base a la Tabla 4.10 los ISP que cumplen con este requerimiento son: Andinanet, Telconet y TV Cable; los ISP en mención tiene características similares en cuanto a disponibilidad, confiabilidad, soporte y cobertura (ver Tabla 3.2).

El ISP que provee el servicio requerido y que tiene menor costo es TV Cable, por lo que el análisis financiero se evaluará con este proveedor.

4.3 ANÁLISIS FINANCIERO PARA ELABORAR LA PROPUESTA TÉCNICA ECONÓMICA

En esta sección se realizará el análisis financiero para implementar una Infraestructura de red segura soporte de aplicaciones E-Business.

Las soluciones se basan en tecnologías de interconexión de redes LAN de las Agencias a la Matriz a través de:

- Enlaces Wireless y
- Enlaces dedicados a través de Internet

4.3.1 ANÁLISIS FINANCIERO PARA UNA INFRAESTRUCTURA DE INTERRED CON ENLACES WIRELESS

Para Implementar una Interred con enlaces wireless se considera que existen dos clases de Infraestructuras de Interred:

- Propia y
- Arrendada

4.3.1.1 Infraestructura de Interred Propia

El costo de implementación para una infraestructura propia se calcula en base a los equipos de hardware que se recomiendan en la sección 4.2. y de acuerdo a la estructura de la Torre a construir.

Adicionalmente se debe tomar en cuenta el costo por autorización de uso de Frecuencia que se paga anualmente a la Superintendencia de Telecomunicaciones.

4.3.1.1.1 Características de la Torre

- Altura: 18 metros
  6 Tramos, cada tramo tiene 3 metros.
- Tipo: Tensores
  Se necesitan 6 tensores para sostener la Torre.

La Tabla 4.11 muestra los costos que incurren en la implementación de una infraestructura de Interred propia.

EQUIPO / MARCA	MATRIZ	SHYRIS	CENTRO	LA MERCED	IZAMBA	REPETIDORA	TOTAL	COSTO UNITARIO (USD $)	COSTO TOTAL (USD $)
Access Point - Mikrotik	1						1	400.00	400.00
Radio - Ubiquiti		1	1	1	1	2	6	150.00	900.00
Polos 2m	1	1	1	1	1	1	6	50.00	300.00
Cable UTP Cat 5 (mts)	50	50	50	50	50	100	350	1.10	385.00
Antena Omnidireccional	1						1	200.00	200.00
Antena 15 dbi Direccional					1	2	3	100.00	300.00
Autorización uso de Frecuencia Superintendencia Anual	1						1	500.00	500.00
Mano de Obra	1	1	1	1	1	1	6	150.00	900.00
Torre de Tensores: Costo: c/3 mts						6	6	250.00	1,500.00
Obra Civil						1	1	750.00	750.00
Mano de Obra de la Torre						1	1	750.00	750.00
TOTAL									**6,885.00**

Tabla 4.11 Costos de Implementación de Infraestructura de Interred Propia con enlaces Wireless

Fuente: La Autora

El costo de la infraestructura propia a los 3 años se muestra en la Tabla 4.12

EQUIPO / MARCA	COSTO PRIMER AÑO (USD $)	COSTO SEGUNDO AÑO (USD $)	COSTO TERCER AÑO (USD $)	SUBTOTAL (USD $)
Access Point – Mikrotik	400.00	0.00	0.00	400.00
Radio – Ubiquiti	900.00	0.00	0.00	900.00
Polos 2m	300.00	0.00	0.00	300.00
Cable UTP Cat 5 (mts)	385.00	0.00	0.00	385.00
Antena Omnidireccional	200.00	0.00	0.00	200.00
Antena 15 dbi Direccional	300.00	0.00	0.00	300.00
Autorización uso de Frecuencia Superintendencia	500.00	500.00	500.00	1,500.00
Mano de Obra	900.00	0.00	0.00	900.00
Torre de Tensores: Costo: c/3 mts	1,500.00	0.00	0.00	1,500.00
Obra Civil	750.00	0.00	0.00	750.00
Mano de Obra de la Torre	750.00	0.00	0.00	750.00
TOTAL	**6,885.00**	**500.00**	**500.00**	**7,885.00**

Tabla 4.12 Proyección del Costo de Infraestructura Propia con enlaces Wireless

Fuente: La Autora

4.3.1.2 Infraestructura de Interred Arrendada

El costo de implementación de una infraestructura de Interred arrendada es mensual.

Este valor se calcula en base a un porcentaje del Costo Total de implementación de una infraestructura. Generalmente este porcentaje es del 15%.

La Tabla 4.13 indica el costo mensual que el proveedor de la infraestructura de Interred facturaría a la Empresa de Agua Potable.

EQUIPO / MARCA	COSTO MENSUAL DEL ARRIENDO (USD $)
Access Point – Mikrotik	60.00
Radio – Ubiquiti	135.00
Polos 2m	45.00
Cable UTP Cat 5 (mts)	57.75
Antena Omnidireccional	30.00
Antena 15 dbi Direccional	45.00
Autorización uso de Frecuencia Superintendencia de Telecomunicaciones	42.00
Mano de Obra	135.00
Torre de Tensores: Costo: c/3 mts	225.00
Obra Civil	112.50
Mano de Obra de la Torre	112.50
TOTAL	**999.75**

Tabla 4.13 Costo Mensual por arrendamiento de la Infraestructura de Interred

Fuente: La Autora

La Tabla 4.14 indica la proyección a 3 años del costo que la Empresa de Agua Potable debe considerar si decide por esta solución.

EQUIPO / MARCA	COSTO MENSUAL DEL ARRIENDO (USD $)	COSTO DEL PRIMER AÑO DE ARRIENDO (USD $)	COSTO DEL SEGUNDO AÑO DE ARRIENDO (USD $)	COSTO DEL TERCER AÑO DE ARRIENDO (USD $)	COSTO TOTAL DEL ARRIENDO (USD $)
Access Point – Mikrotik	60.00	720.00	720.00	720.00	2,160.00
Radio – Ubiquiti	135.00	1,620.00	1,620.00	1,620.00	4,860.00
Polos 2m	45.00	540.00	540.00	540.00	1,620.00
Cable UTP Cat 5 (mts)	57.75	693.00	693.00	693.00	2,079.00
Antena Omnidireccional	30.00	360.00	360.00	360.00	1,080.00
Antena 15 dbi Direccional	45.00	540.00	540.00	540.00	1,620.00
Autorización uso de Frecuencia Superintendencia (Mes)	42.00	504.00	504.00	504.00	1,512.00
Mano de Obra	135.00	1,620.00	1,620.00	1,620.00	4,860.00
Torre de Tensores: Costo: c/3 mts	225.00	2,700.00	2,700.00	2,700.00	8,100.00
Obra Civil	112.50	1,350.00	1,350.00	1,350.00	4,050.00
Mano de Obra de la Torre	112.50	1,350.00	1,350.00	1,350.00	4,050.00
TOTAL	**999.75**	**11,997.00**	**11,997.00**	**11,997.00**	**35,991.00**

Tabla 4.14 Proyección a 3 años del Costo por Arrendamiento de Infraestructura de Interred

Fuente: La Autora

4.3.2 ANÁLISIS FINANCIERO PARA UNA INFRAESTRUCTURA DE INTERRED CON ENLACES DEDICADOS A TRAVÉS DE INTERNET

El costo mensual para Implementar una Interred con enlaces dedicados a través de Internet con los ISP seleccionados se indica en la Tabla 4.15.

AÑO	ANDINANET	TELCONET	TV CABLE
ANCHO DE BANDA	1024 kbps	1024 kbps	1000 kbps
COMPARTICION	1:1	1:1	1:1
COSTO MENSUAL	**USD $ 557.00**	**USD $520.00**	**USD $400.00**

Tabla 4.15 Costos de Enlaces Dedicados

Fuente: ISP

El proveedor seleccionado en la sección 4.2.3 es TV Cable. Los costos que implica el uso de esta solución en 3 años se indica en la Tabla 4.16

COSTO MENSUAL POR ENLACE DEDICADO (USD $)	CANTIDAD DE ENLACES DEDICADOS	COSTO MENSUAL POR ENLACES DEDICADOS TV CABLE (USD $)	COSTO DEL PRIMER AÑO POR ENLACE DEDICADO TV CABLE (USD $)	COSTO DEL SEGUNDO AÑO POR ENLACE DEDICADO TV CABLE (USD $)	COSTO DEL TERCER AÑO POR ENLACE DEDICADO TV CABLE (USD $)	COSTO TOTAL POR ENLACE DEDICADO TV CABLE (USD)
400	5	2.000	24.000	24.000	24.000	72.000

Tabla 4.16 Proyección del Costo por Enlace Dedicado a 3 años

Fuente: La Autora

4.3.3 ANÁLISIS DE LAS SOLUCIONES

A los costos de implantación para Infraestructura de Interred por medio de enlaces Wireless Propia y Arrendada, se considerará el costo de Enlace a Internet para la VPN recomendada en la sección 3.5.2.3.1, que sugiere la contratación de un Enlace de Acceso a Internet con la empresa TV Cable. El ancho de banda es de 2000 kbps para el nivel de compartición 2:1 con un costo mensual de USD $300=, y USD $ 3.600= anuales. (Ver Tabla 3.5 Costos de Acceso a Internet Cable MODEM – TV Cable).

De los costos de las soluciones presentadas en las secciones 4.3.1 y 4.3.2 se recomienda implementar una ***Infraestructura propia de Interred por medio de enlaces Wireless.***

Esta solución es la más conveniente por su costo de implementación.

La inversión para su implantación a pesar de ser alta al inicio del proyecto respecto al costo del arriendo de una infraestructura de Interred con enlace wireless arrendada y al costo de enlaces dedicados a través de Internet en el periodo de tres años es menor, lo que se aprecia en la Tabla 4.17

TIPO DE INFRAESTRUCTURA	ENLACES WIRELESS PROPIA + COSTO ENLACE A INTERNET PARA VPN (USD $)	ENLACES WIRELESS ARRENDADA + COSTO ENLACE A INTERNET PARA VPN (USD $)	ENLACES DEDICADO POR INTERNET (USD $)
COSTO DE IMPLANTACIÓN PRIMER AÑO	10,485	15,597	24,000
COSTO DE IMPLANTACIÓN SEGUNDO AÑO	500	15,597	24,000
COSTO DE IMPLANTACIÓN TERCER AÑO	500	15,597	24,000
TOTAL DE INVERSIÓN	**11,485**	**46,791**	**72,000**

Tabla 4.17 Comparación de Costos de las Soluciones con Proyección a 3 años

Fuente: La Autora

Para calcular el costo Total del Proyecto se debe añadir el costo por Licencias del Software para el nuevo servidor lo que se aplica a cualquiera de las soluciones.

Adicionalmente, se suman los costos por los Servicios Profesionales para la Implantación de la Infraestructura de con enlaces Wireless, como se detalla a continuación:

- Un Ingeniero en Electrónica, Telecomunicaciones y Redes, para supervisión de la implementación, responsable de la puesta en servicio y la integración de las redes inalámbricas. El costo por Servicios Profesionales es de USD $2,000=, incluído viáticos.

- Tres Técnicos especializados en instalación de Torres y equipos de comunicación. El costo por cada técnico es de USD $1,500=, incluído viáticos.

El tiempo para la implementación de la infraestructura con enlaces Wireless es de un mes.

ITEMS	VALOR (USD $)
COSTO DE IMPLANTACIÓN DE INFRAESTRUCTURA PROPIA CON ENLACE WIRELESS	11,485
COSTO DE LICENCIAS PARA SERVIDOR	2,649
FIREWALL SGS 360	1,000
DIRECCIÓN DEL PROYECTO (1 Ing. Electrónico, Telecomunicaciones y Redes)	2,000
PERSONAL DE APOYO (3 Técnicos)	4,500
COSTO TOTAL DEL PROYECTO	**21,634**

Tabla 4.18 Costo Total del Proyecto

Fuente: La Autora

4.4 ANÁLISIS DE COSTO BENEFICIO DE LA MEJOR PROPUESTA

De acuerdo a los costos obtenidos en la sección 4.3 se determina que las mejores opciones para hardware, software y comunicaciones son las siguientes:

4.4.1 HARDWARE

De las alternativas de hardware expuestas en la sección 4.2.1 se presentan a continuación las que son de menor costo:

TIPO DE HARDWARE	DESCRIPCIÓN	COSTO (USD $)
ANTENAS	Hyperlink de 15 dbi Onmidireccional 2.4 Ghz	200
	15 dbi Panel Direccional 2.4 Ghz	100
ACCESS POINT	AP Mikrotik RB411	400

TIPO DE HARDWARE	DESCRIPCIÓN	COSTO (USD $)
RADIOS	Nano Station 2	150
FIREWALL / GATEWAY	Symantec SGS 360	1,000
TOTAL		**1,850**

Tabla 4.19 Costos de Hardware para calcular la mejor propuesta

Fuente: La Autora

4.4.2 SOFTWARE

De las alternativas de software necesarias para la implementación de la infraestructura de Interred que por su funcionalidad y menor costo fueron consideradas, se presentan en la Tabla 4.20:

TIPO DE SOFTWARE	DESCRIPCIÓN	COSTO (USD $)
LICENCIA DE SISTEMA OPERATIVO	Sistema Operativo Windows 2003 Server	853
LICENCIA DE BDD	SQL Svr. Standard Edtn. 2005 Win 32 Spanish OLP NL Qualified	896
ANTIVIRUS (1 AÑO)	Eset Smart Security	900
TOTAL		**2,649**

Tabla 4.20 Costos de Software para calcular la mejor propuesta

Fuente: La Autora

4.4.3 COMUNICACIONES

De las alternativas de comunicaciones expuestas en la sección 4.2.3 la solución de menor costo para la implementación de una infraestructura de Interred con enlaces dedicados es por el ISP TV Cable. (Ver las Tablas 4.15 y 4.16).

AÑO	ANDINANET	TELCONET	TV CABLE
ANCHO DE BANDA	1024 kbps	1024 kbps	1000 kbps
COMPARTICION	1:1	1:1	1:1
COSTO MENSUAL	USD $ 557.00	USD $520.00	USD $400.00

Tabla 4.15. Costos de Enlaces Dedicados

Fuente: ISP

COSTO MENSUAL POR ENLACE DEDICADO (USD $)	CANTIDAD DE ENLACES DEDICADOS	COSTO MENSUAL POR ENLACES DEDICADOS TV CABLE (USD $)	COSTO DEL PRIMER AÑO POR ENLACE DEDICADO TV CABLE (USD $)	COSTO DEL SEGUNDO AÑO POR ENLACE DEDICADO TV CABLE (USD $)	COSTO DEL TERCER AÑO POR ENLACE DEDICADO TV CABLE (USD $)	COSTO TOTAL POR ENLACE DEDICADO TV CABLE (USD)
400	5	2.000	24.000	24.000	24.000	72.000

Tabla 4.16 Proyección del Costo por Enlace Dedicado a 3 años

Fuente: La Autora

4.4.4 BENEFICIO DE LA MEJOR PROPUESTA

Del análisis realizado en la sección 4.3 se determinó que existen tres posibles soluciones para implantar una infraestructura de Interred segura soporte de aplicaciones E-Business:

- Dos soluciones de Infraestructura de Interred con enlaces Wireless:
  - Propia y
  - Arrendada
- Una Infraestructura de Interred con enlaces dedicados por medio de Internet

De éstas la mejor propuesta es la implementación de una infraestructura de Interred propia con enlaces wireless, como se puede observar en la Tabla 4.17.

Ahora, si comparamos el porcentaje de ahorro de la propuesta de implantación de una Infraestructura de Interred propia con enlaces wireless proyectado a tres años respecto de las otras propuestas, tenemos:

TIPO DE INFRAESTRUCTURA	ENLACES WIRELESS PROPIA (USD $)	ENLACES WIRELESS ARRENDADA (USD $)	ENLACES DEDICADO POR INTERNET (USD $)	% AHORRO RESPECTO A INFRAEST. ARRENDADA	% AHORRO RESPECTO A INFRAEST. CON ENLACE DEDICADO POR INTERNET
TOTAL DE INVERSIÓN	7,885	35,991	72,000	355%	813%

Tabla 4.21 Porcentaje de Ahorro por Implementación de una Infraestructura de Interred con enlaces wireless Propia respecto de las otras soluciones proyectado a 3 años

Fuente: La Autora

Los beneficios de la implementación de una Infraestructura de Interred propia con enlaces wireless son intangibles y se resumen en:

- Información en línea actualizada y oportuna en las Agencias.
- Mejor atención al Cliente, debido a que la información está en línea y actualizada en todas las agencias y éstas a más de ser Cajas Recaudadoras se convierten en puntos de Atención al Cliente.
- Al brindar atención al Cliente en las Agencias la imagen de la Empresa de Agua Potable mejorará pues estará demostrando su interés por la colectividad y ésta a su vez podrá acudir a cualquier agencia por trámites que sólo los podía realizar en la Matriz lo que reducirá el tiempo que el cliente espera por ser atendido.

4.5 GENERACIÓN DEL DOCUMENTO PROPUESTA TÉCNICA ECONÓMICA

Una vez que se ha determinado la mejor propuesta para la Implementación de una Infraestructura de Interred Segura soporte de aplicaciones E-Business se genera el documento Propuesta Técnica Económica.

En esta propuesta se considera:

- Objetivos
- Alcance

- Beneficios
- Infraestructura Técnica Requerida
- Esquema de Diseño de la Interred
- Factores de Éxito
- Plazo de Implantación
- Costo de la Inversión
- Soporte Técnico

4.5.1 OBJETIVOS

4.5.1.1 Objetivo General

Diseñar e Implementar una Infraestructura de Interred segura para soporte de la aplicación E-Business en la Empresa de Agua Potable de la ciudad de Ambato.

4.5.1.2 Objetivos Específicos

- Integrar las redes LAN de las Agencias con la Matriz mediante enlaces wireless.
- Establecer políticas de seguridad para la operación de la Interred segura con el fin evitar ataques internos o externos.
- Establecer políticas de seguridad de VPN para la comunicación con la Compañía proveedora de la aplicación E-Business a fin de obtener soporte de la misma.

4.5.2 ALCANCE

El presente servicio profesional cubrirá el análisis e implantación de la Infraestructura de Interred Segura, la misma que integrará a la Matriz las Agencias de la Empresa de Agua Potable de la ciudad de Ambato.

Adicionalmente, con las tecnologías VPN se implantará una conexión directa al proveedor de la aplicación E-Business con el fin de que ésta pueda brindar soporte técnico, básicamente al administrador de la aplicación. Por otro lado,

dicha conexión será utilizada para realizar mantenimiento a la aplicación que no requiera la presencia de los técnicos del proveedor de la aplicación en la ciudad de Ambato y que pueda ser resuelto en forma remota desde sus oficinas en Quito.

4.5.3 BENEFICIOS

- Integración total de las redes LAN de las Agencias con la red LAN de la Matriz.
- Actualización inmediata de los datos generados en las Agencias hacia la Base de Datos centralizada en la Matriz.
- Contar con información en línea, actualizada y oportuna en la Matriz y Agencias.
- Cada Agencia al contar con información actualizada y en línea a más de ser una Caja Recaudadora se convierte en un punto de Atención al Cliente.
- Con las políticas de seguridad se evitarán el alto grado los ataques internos y externos a la red salvaguardando el activo intangible más valioso: La información de los proceso del negocio.
- Con una comunicación directa a las oficinas del proveedor de la aplicación E-Business, la Empresa de Agua Potable obtiene soporte inmediato ante cualquier eventualidad respecto de la aplicación.

4.5.4 INFRAESTRUCTURA TÉCNICA REQUERIDA

- Se requiere que cada red LAN de las Agencias se conecte a la red LAN de la Matriz a través de enlaces Wireless.

Para la interconexión de la Infraestructura de Interred se requiere lo siguiente:

1 Access Point 2.4 Ghz para la Matriz

1 Radio 2.4 Ghz en cada Agencia y 2 Radios en la Repetidora

1 Antena de 15 dbi 2.4 Ghz Omnidireccional

3 Antenas de 15 dbi 2.4 Ghz Direccional, una para la Agencia Izamba y dos para la Repetidora

1 Torre de Tensores de 18 metros para la Repetidora

30 Licencias de uso del Antivirus para proteger a las estaciones de trabajo y la red en sí de los ataques provenientes de la red interna o externa.

- Se requiere un enlace directo con el proveedor de la aplicación E-Business, para lo cual se necesita:

1 Firewall / Gateway con funciones para la configuración de VPN´s

4.5.5 DISEÑO DE LA INTERRED

Se adjunta los diseños de Interred y VPN que serían implantados en caso de ser contratados.

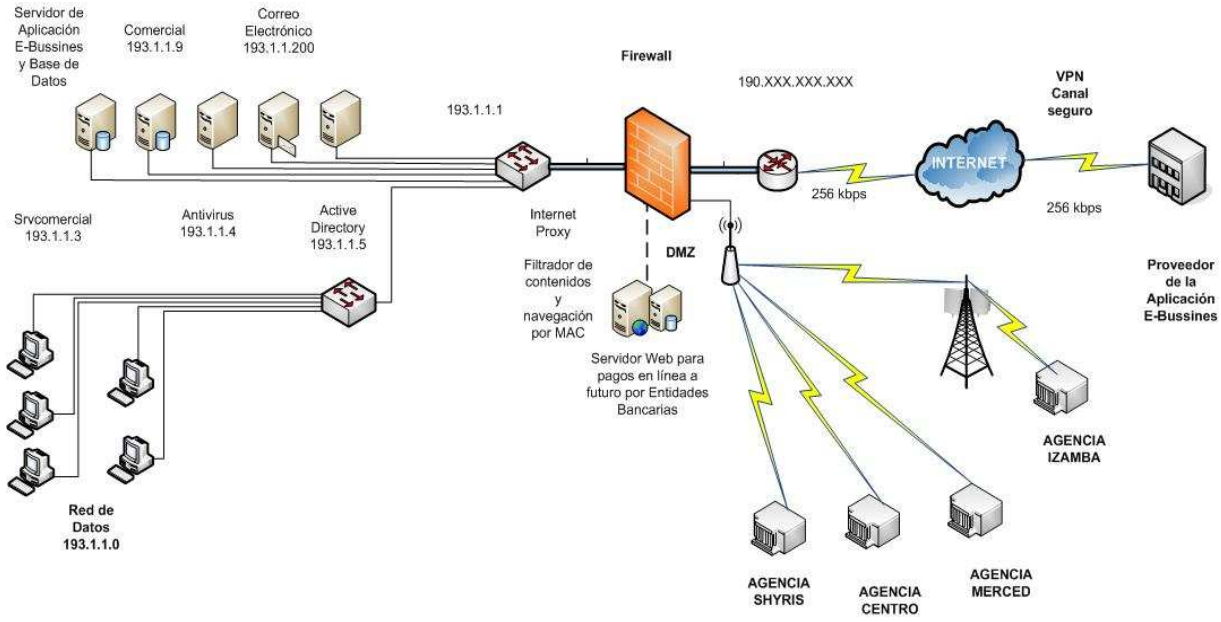


Figura 4.1 Diseño de la Interred para la Empresa de Agua Potable

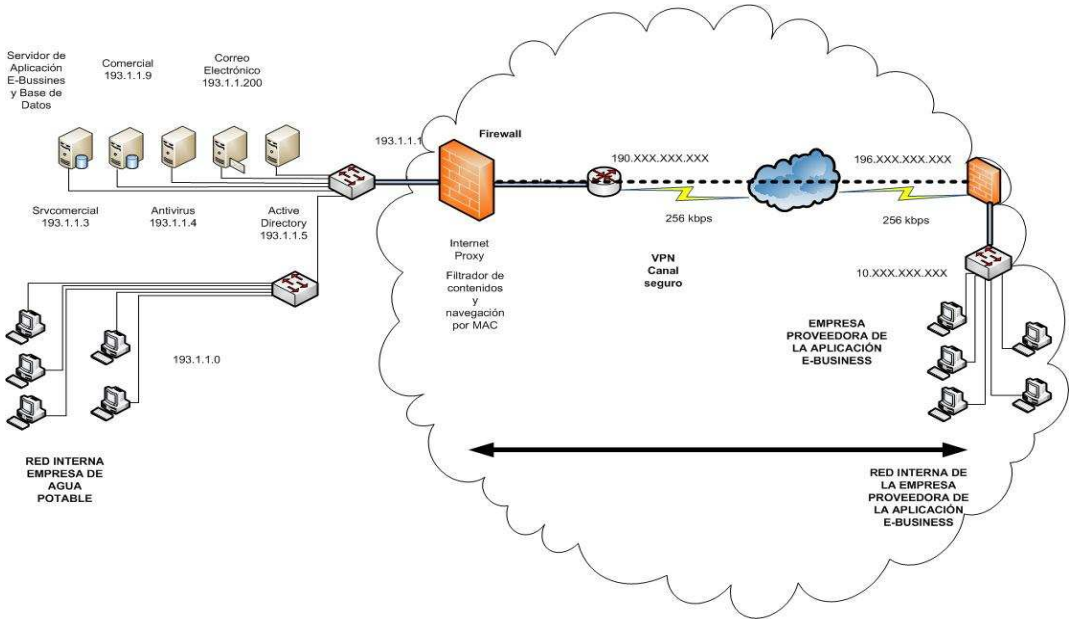


Figura 4.2 Diseño de la VPN con comunicación al Proveedor de la aplicación E-Business

4.5.6 FACTORES DE ÉXITO

- Designar un coordinador del proyecto, el mismo que realizará las gestiones necesarias para conseguir citas y el apoyo oportuno de las diferentes instancias y unidades ejecutivas y administrativas para el normal desenvolvimiento del mismo.

- Proporcionar la información y documentación necesarias para el análisis de la Implementación de una Infraestructura de Interred segura soporte de aplicaciones E-Business de la Empresa de Agua Potable.

- Los plazos y resultados de este proyecto dependerán en alto grado de la oportunidad, participación y apoyo que brinden los funcionarios de la Empresa de Agua Potable de Ambato.

4.5.7 PLAZO DE IMPLANTACIÓN

Se estima que el plazo del proyecto demandará de CUATRO SEMANAS de trabajo (Un mes). Sin embargo, dependiendo de las facilidades proporcionadas, procuraremos reducir este tiempo al máximo y tratar de implementar el proyecto lo más antes del plazo estipulado.

Aspiramos no enfrentar ninguna dificultad que pueda ocasionar retrasos al proyecto, en todo caso, de presentarse tal situación, lo comunicaremos oportunamente para obtener su aprobación.

4.5.8 COSTO DE LA INVERSIÓN

Hemos estimado en 4 semanas la duración del proyecto total.

De acuerdo al tiempo estimado, gastos operacionales que se incurrirían en el Proyecto para el diseño, pruebas e implantación de la Infraestructura de Interred con enlaces Wireless y considerando la formación del equipo de profesionales que se asignará, nuestros honorarios profesionales por el total del proyecto será de **VEINTE Y UN MIL SEICIENTOS TREINTA Y CUATRO DÓLARES AMERICANOS (USD $ 21,634=) MAS EL IVA** correspondiente. Incluye el costo por Licencia del Antivirus para 30 estaciones de trabajo por un año.

Las actividades a realizar se coordinarán con el personal responsable de este Proyecto por parte de la Empresa de Agua Potable de Ambato.

Esta propuesta tiene validez de 30 días.

4.5.9 SOPORTE TÉCNICO

Luego de la implantación y puesta en funcionamiento de la nueva infraestructura de Interred ofrecemos un año de Garantía Técnica sin costo para la Empresa de Agua Potable ante cualquier falla de los equipos producida después del arranque en funcionamiento de la Infraestructura de Interred.

Ponemos a su disposición una etapa de Mantenimiento para servicios especializados que pudiera requerir la Empresa de Agua Potable en un futuro cercano previa negociación del alcance del trabajo a realizar.

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Con la integración de la redes LAN de las Agencias a la red LAN de la Matriz de la Empresa de Agua Potable, a través de la implementación de una Infraestructura de Interred segura soporte de aplicaciones E-Business, la Empresa mejora la calidad del servicio de “Atención al Cliente” al mantener la información en línea, actualizada y oportuna, al mismo tiempo que su imagen crece al ofrecer varios puntos de Atención a la comunidad en lugares estratégicos de la ciudad.

- La principal brecha de seguridad, aunque no lo parezca, es el propio recurso humano de la Empresa, no solamente por una falta de conciencia en cuanto a seguridad informática sino también por falta de capacitación para la ejecución de sus tareas laborales.

- La idea detrás de la implantación de cualquier esquema de seguridad consiste en alcanzar el mayor nivel de seguridad posible y evitar afectar o alterar los procesos de negocio; debe emplearse el adecuado equilibrio entre estos dos aspectos.

- La nueva aplicación E-Business se maneja mediante perfiles de usuarios, por lo que el área directiva de la Empresa y funcionarios de la Empresa pueden acceder a la información en cualquier momento con la certeza de que la información está actualizada.

- Considerando que la nueva aplicación E-Business es accesible vía web, no se requieren de estaciones de trabajo nuevas para su uso, permitiendo de este modo la utilización de las estaciones de trabajo anteriormente usadas en la Matriz (**ver Tabla 2.1**) y en las diferentes Agencias, concretándose de esta manera un ahorro para la Empresa de Agua Potable.

- Es importante destacar que la Empresa de Agua Potable con el fin de mejorar su infraestructura tecnológica ha venido adquiriendo nuevas estaciones de trabajo las mismas que están siendo instaladas en reemplazo de aquellas que han cumplido su vida útil. También se incluyen la adquisición de un nuevo servidor para la aplicación E-Business, una estación que funcionará como servidor de Dominio, una estación que servirá como servidor de antivirus y un servidor para correo electrónico. Todos estos elementos fueron recomendados por el proveedor de la aplicación E-Business como servicios de valor agregado sin costo para la Empresa de Agua Potable como parte de la Propuesta de Servicios en Asesoría de Seguridades en la Infraestructura.

- La implantación del enlace VPN permanente con el Proveedor de la aplicación E-Business constituye una inversión clave cuyo beneficio representa el soporte técnico inmediato al administrador de la aplicación E-Business, disminuyendo el tiempo de inactividad del o los responsables del proceso afectado. Esta herramienta le faculta al proveedor de la aplicación monitorear el desempeño de la misma a fin de mejorar el rendimiento y calidad de la aplicación.

- La comunicación vía VPN a través de un enlace de Internet entre la Empresa de Agua Potable y la Empresa Proveedora, garantizará un soporte adecuado y oportuno a la aplicación E-Business

5.2 RECOMENDACIONES

- Formalizar un plan de capacitación, concientización y difusión a todos los funcionarios de la Empresa de Agua Potable respecto a la responsabilidad que implica el uso de la Identificación y Claves de acceso a la aplicación E-Business y las consecuencias del mal uso ya sea por negligencia o desconocimiento de las políticas de seguridad.

- Asignar un funcionario de la sección de Procesamiento de Datos para el soporte de sistemas a fin de colaborar con la administración de la aplicación E-Business y demás servicios adicionados como son configuración de Firewall, VPN, IDS que son funcionalidades integradas en el Symantec SGS 360.

- Definir las políticas de seguridad en el Firewall a fin de evitar los ataques provenientes de la red interna como externa.

- Elaborar manuales de configuración del Firewall, Proxy, aplicaciones en general y que contenga las políticas de seguridad, políticas de actualización de hardware, software, antivirus, etc. que fueron definidas en la sección 2.3.

- Definir los procedimientos para la comunicación vía VPN con el proveedor de la aplicación E-Business para establecer normas de ingreso a la red para tareas de soporte y mantenimiento de la aplicación.

- Es importante que todo funcionario de la Empresa de Agua Potable tome conciencia sobre el manejo seguro de la información, ya que resulta inútil cualquier sistema de seguridad por complejo y completo que este sea, si los funcionarios, por ejemplo, facilitan su nombre de usuario y contraseña a otras personas y con esto dejan abierta la posibilidad de ataques o robo de información crítica de la Empresa.

- GLOSARIO DE TÉRMINOS

ADSL (Asymetric Digital Suscriber Line)	Tecnología de acceso a Internet asimétrico que utiliza la infraestructura telefónica.
AES (Advanced Encryption Standar)	Es el predecesor de TDES, es un algoritmo de cifrado de bloques, el tamaño del bloque es de 128 bits y la clave es de 128, 192 o 256 bits.
Cable Módem	Enlace de Banda Ancha que utiliza la infraestructura de televisión por cable. Módem que conecta una computadora con Internet a alta velocidad, por medio de una línea de TV por cable.
DES (Data Encryption Estándar)	Algoritmo estándar de encriptación de datos por bloque de 64 bits de longitud. Usa claves de 56 bits. DES es lo suficientemente seguro como para dejar fuera a hakers casuales, sin embargo puede ser quebrado con hardware especial
DMZ (Delimitarized Zone)	Constituye la primera barrera contra la intrusión, creando un foso entre Internet y la red de servicios.
DNS (Domain Name System),	Sistema de nombres de Dominio, permite traducir las direcciones IP de las máquinas en nombres fácilmente entendibles para los humanos y viceversa.

E-Business	Negocio electrónico, entendido como la mejora de las relaciones entre empresas gracias a la conectividad.
E-Commerce	Comercio electrónico, referido a aplicaciones que permiten transacciones e interacciones entre la compañía y el consumidor sobre Internet. También llamadas aplicaciones Business-To-Consumer.
Encriptación	Procedimiento mediante el cual se hace ilegible un mensaje para evitar que lo lean personas no autorizadas.
Firewall	Sistema de seguridad, encargado de proteger una red de área local de accesos no autorizados desde una WAN a la que esté conectada.
FTP	(File Transfer Protocol), protocolo de transferencia de archivos.
Gateway	Dispositivo que se encarga de conectar dos redes de distinto tipo capaz de transformar la información, adaptando el formato de paquetes de la primera red al que necesita la segunda. Trabajan a nivel de transporte (nivel 4 del estándar OSI) o superior.

Hash	Método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash.
HTTP	Protocolo de transferencia de Hipertexto, usado en cada transacción web, y sigue el esquema petición-respuesta entre un cliente y un servidor.
HTTPS	Protocolo seguro de transferencia de hipertexto, es un protocolo de red basado en HTTP, destinado a la transferencia segura de datos de hipertexto. Crea un canal seguro sobre una red insegura.
Intranet	Red de computadores conectadas por medio de un protocolo de comunicación TCP/IP, dentro de una empresa u organización, que enlaza a empleados y miembros, facilitando el acceso a la información y convirtiendo el uso de recursos y aplicaciones en un proceso más amigable, funcional y productivo.
IPSec (Internet Protocol Security)	Protocolo que sirve para establecer una sesión segura entre dos hosts que se comuniquen a través de IP, proporcionando encriptación a nivel de la capa de red, definiendo nuevos formatos de paquete: la cabecera de autentificación (AH), que permite asegurar la integridad de los datos y el ESP (Encapsulating

	Security Payload), que permite asegurar la privacidad e integridad de los datos. AH protege la integridad y autenticidad de los datos, incluyendo los campos invariantes de la cabecera IP. Esta cabecera no proporciona confidencialidad, mientras que ESP protege tanto la confidencialidad como la integridad y la autenticidad de los datos. Cuando se usa para comprobar la integridad de los datos no incluye los variantes de la cabecera IP.
ISP (Internet Service Provider)	empresa que brinda acceso a los servicios a Internet como: navegación en la web, correo electrónico, FTP, DNS, etc.
L2TP (Layer 2 Tunneling Protocol)	protocolo que permite separar el servidor de conexión de nivel 2 OSI (el que “escucha” en el final de la línea telefónica en un módem por ejemplo) del servidor de PPP. De esta manera el cliente accede a un servidor de conexión (ej. banco de módems) y éste -usando L2TP- se comunica con la red (host) con el que el cliente quiere tener acceso. Esto consigue `juntar' dos segmentos de red (uno de ellos es point-to-point) virtualmente.
PLC (Power Line Communication)	Tecnología de acceso a Internet que utiliza la infraestructura eléctrica.
PPTP (Point-to-Point Tunneling Protocol)	Protocolo de encapsulado de PPP sobre IP. Es una especificación desarrollada por un consorcio de fabricantes, entre los que estaban gente como

	Microsoft, 3Com o U.S. Robotics. El protocolo se diseñó originalmente como una forma de encapsular protocolos no TCP/IP (como IPX) para poder ser transmitidos por Internet usando GRE (Generic Routing Encapsulation). Es una especificación genérica, que permite la adición de diversos mecanismos de autentificación y algoritmos de encriptación. Nótese que estas técnicas de seguridad no están dentro del protocolo, sino que se añaden a posteriori.
SSL (Secure Socket Layer)	Protocolo que permite establecer comunicación encriptada entre un navegador Web y un servidor, para mayor seguridad.
TDES (Triple Data Encryption Estándar)	Algoritmo encriptador de datos por bloque que realiza el cifrado DES tres veces utilizando un clave de 192 bits.
VPN (Virtual Private Network)	Red privada que se extiende, mediante un proceso de encapsulación y encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte (Internet).
Xdsl (Digital Sucriber Line)	Tecnología de Acceso a Internet por medio de la infraestructura telefónica.

BIBLIOGRAFÍA

LIBROS

[1] TANNENBAUM, Andrew, “REDES DE COMPUTADORAS”, Pearson Educación, Cuarta Edición, México 2003.

[2] EVANS, Tim. CONSTRUYA SU PROPIA INTRANET: GUÍA PRÁCTICA PARA CONFIGURAR UNA WEB INTERNA. 1era. Edición, México. Prentice-Hall Hispanoamericana. 1997.

[3] MERIKE, Kaeo, DESIGNING NETWORK SECURITY, Cisco Press, Segunda Edición, 2004.

[4] MAIWALD, Eric, NETWORK SECURITY, A BEGINNERS GUIDE, Segunda Edición, McGraw-Hill, 2003.

[5] SNADER, Jon, VPN’S ILLUSTRATED : TUNNELS, VPN AND IPSEC, Adison Wesley Professional , 2005.

[6] CCNA Ver. 3.1 Cisco Networks.

[7] COMER, Douglas. REDES DE COMPUTADORES, INTERNET E INTERREDES. 1era. Edición, México. Prentice-Hall, 1997.

REFERENCIA ELECTRÓNICA

[8] Microsoft, Requisitos del Sistema, http://www.microsoft.com/spain/windows/downloads/ie/sysreq.mspx, Agosto 2009.

[9] Cómo funciona una VPN, http://ipref.wordpress.com/2009/04/28/vpn/, Agosto 2009.

[10] Microsoft, Información general sobre criptografía, http://msdn.microsoft.com/es-es/library/92f9ye3s.aspx, noviembre 2007.

[11] Symantec Gateway Security, http://eval.symantec.com/mktginfo/enterprise/fact_sheets/25657-DS00147-SL_SGS400_fs.pdf, Agosto 2009.

[12] OLIVEIRA, Angel, Criterios para construir una Intranet Corporativa, http://www.aerearh.com/software/intranet.htm, Noviembre 2008.

ARTÍCULOS

[13] HERRERA, Juan, ¿Cómo fortalecer tecnológicamente a las empresas de Agua Potable y Alcantarillado?, ANDESAPA, No.1, Julio 2008.

[14] SYMANTEC, Symantec Client VPN v 8.0.0 – Release Notes, Marzo 2006

REVISTAS

[15] Andesapa, revista del agua #3 Diciembre 2008.

[16] Andesapa, revista del agua #1 Julio 2008

[17] Anemapa, Revista Informativa #36 julio- septiembre 2006

ANEXO 1

ANEXO 1: PROVEEDORES DE SERVICIOS DE INTERNET AUTORIZADOS EN EL ECUADOR

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	AMOGHI S.A.	Latacunga	03-2810-552	Calle Félix Valencia 743 y 2 de Mayo.
	ANDINATEL	Quito	02-2561-005	Jorge Drom S/N y Gaspar de Villarroel. Edif. Andinanet
	ARTIANEXOS	Guayaquil	04-2264-673	Urbanización San Felipe, Manzana 165, villa 18 (frente al Colegio Americano)
	ASAPTEL S.A.	Guayaquil	04- 2291-676	Av. De las Américas 920 C y Av. Carlos Luis Plaza Dañín.
	AT&T GLOBAL NETWORK SERVICES ECUADOR CIA. LTDA.	Quito	02-2433-667	Av. República del Salvador N34-211 y Moscú, Edfi. Aseguradora del Sur, piso 2
	BRIGHTCELL S.A.	Quito	02-2232-619 2232-329	Hernando de la Cruz N31-120 y

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
				Mariana de Jesús
	COMDIGITRONIK S.A.	Quito	02-2255-195	Paris N41-43 y Av. De los Granados
	COMPAÑÍA DE SERVICIOS ELECTROMECÁNICOS PARA LE DESARROLLO CSED	Santo Domingo	02-2768-544.	Km 5 1h, via Quito Baypass Quevedo, de la ciudad de Santo Domingo de Los Colorados
	COMPIM S.A	Guayaquil	04-2884-505 04-2884-506	Bálsamo Norte No. 414 y la quinta (Urdesa Central) 2do. Piso Oficina 5. Guayaquil
	COMPUATEL MANTENIMIENTO INSTALACIONES Y ASESORÍA EN TELECOMUNICACIONES CIA. LTDA.	Quito	02-2260-664	Pasaje La Tierra E10-84 y Avda. Shyris
	CONECEL S.A.	Guayaquil	04-2693-693	
	CORPORACION INTERINSTITUCIONAL DE COMUNICACION ELECTRONICA INTERCOM	Quito	02-2234-447	Av. Amazonas 258 y Jorge Washington

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	CORPORACIÓN XPRESA DEL ECUADOR DATAEXPRESS S.A.	Loja	07-2587-795	Av. Universitaria y Jose Felix de Valdivieso, cuarto piso, de la ciudad de Loja
	COSINET S.A.	Quito	02-2229-818 2559-759	Av. 6 de Diciembre N31-89 y Wimpher
	DINOLAN	Santo Domingo	02-2763-454.	Av. Quito y Cuenca
	EASYNET S.A.	Guayaquil	1800327963 - 04-2682-305 04-2680-435	Guayaquil Calle Víctor Hugo Sicuret y Luis Orrantia (esquina) Central Kennedy Norte de Pacifitel S.A.
	ECUADORTELECOM S.A.	Guayaquil	04-2515-555	Pedro Carbo 555 y Luque , sexto piso. Ed. Ecutel
	ECUAENLACE SATELITAL S.A.	Guayaquil	04-2886-585 04-2883-585	Ciudadela Urdesa, Calle Guayacanes No. 203 y Víctor Emilio Estrada
	ECUAONLINE S.A	Quito	02-2440-831 02-2452-537	Av. República de El Salvador N35-82 y Portugal Edf.

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
				Twintowers
	EFICENSA S.A.	Guayaquil	04-2369-819	Ciudadela Kennedy Norte, Av. José Assaf Bucaram y Secundino Sáenz - Edificio "Linkotel", Primer piso.
	ENTREPRENEURINC	Quito	02-2453-299 02-2434-305	Av República E546 y Alemania, 2do piso.
	ESPOLTEL	Guayaquil	04-2515-010 04-2514-477	Malecon y Loja esq.
	ETAPATELECOM S.A.	Cuenca	07-2866-000	Calle Larga 113 Huanacacap Edif. Banco Central piso 1
	FIX WIRELES INTERNET	Quito	02-2559-064 02-2901-448	Av. Mariana de Jesús 1740 y Antonio de Ulloa OE3-42
	FLATEL COMUNICACIONES CIA. LTDA	Quito	02-2460-880	Nuñez de Vela 903 y Naciones Unidas Edificio Carolina

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
				2000.
	FREDDY GUSTAVO CALVA CALVA	Loja	07-2573-719	Miguel Riofrío 0918, entre 24 de Mayo y Macará
	GPF Corporación Cía. Ltda.	Quito	02-2256-266 02-2920-436	Avenida República # 1331 y Alemanía, edificio Álvares García Piso 1.
	BARAINVER S.A.	Quito	02-255-2372	Versalles 24-52 y Cuero y Caicedo
	GIGOWIRELESS CIA.LTDA	Quito	02-2804-962	Juan Barrezueta N 74-15
	GRUPO BRAVCO CIA.LTDA	Quito	02-2255-566	Avda. Amazonas N39-61 y Pereira, Ed. Centro Financiero P9
	GRUPO MICROSISTEMAS JOVICHSA S.A	Quito	02-2923-500 02-2251-869	Av. Amazonas No. 62-88 y Tomás de Berlanga
	IMBANET S.A.	Ibarra	06-2644-070	Sucre No. 10-51 y Av. Pérez Guerrero

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	IMPSATEL	Quito	02-2264-101 02-2465-066	Urb. IñaQuito Alto, Juan Díaz N37-111
	INFONET ECUADOR	Quito	02-2444-965 02-2456-222 02-2255-4020	Avda. Amazonas N39-169 y Gaspar de Villarroel Ed. Reinoso P1, Of. 103
	INFRATEL CIA. LTDA.	Quito	02-2254-608	Av. De los Shyris N39-281 y Gaspar de Villarroel C.C. Galería local 18
	INTELLICOM INFORMATICA (ECUAENLACE)	Guayaquil	04-2888-565 04-2881-606 04-2881-682	Guayacanes 203 y Av. Víctor Emilio Estrada, Cdla. Urdesa
	INTERTEL CIA. LTDA.	Quito	02-2436-606	Av. Amazonas N39-169* y Gaspar de Villarroel
	JAIME BEJAR FEIJOO	Guayaquil	04-2888-990	Calle Primera No. 1237 y Costanera (Urdesa Central)
	JHONI JOEL JACOME GALARZA	Gualaquiza	07-2780-477.	La Calle Luis Casiraghi y Francisco de

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
				Orellana. Cantón Gualaquiza
	LATINMEDIA S.A.	Quito	02-2435-666 02-2247-301	General Roca 263 y Bosmediano
	LK-TRO-KOM-S.A.	Guayaquil	02-2202-249 02-2200-650 02-2200-164	Guayaquil Calle 28 de Mayo Intersección Tercera Peatonal ciudadela El Paraiso y callejón 1
	LOJASYSTEM C.A.	LOJA	07-2572-480 07-2589-118	Jose A. Eguiguren y Bernardo Valdivieso
	LUDEÑA SPEED TELECOM Y CIA	LOJA	07-2560-380	Avda. Orillas del Zamora 0358 y Clodoveo Carrion
	LUTROL S.A. INTERACTIVE	Quito	02 - 298-6440 02-2986-442 02-2986-645	Av. 12 de Octubre Torre 1492 y A. Lincoln, Edificio Torre 1492, oficinas 606/ 703
	MEGADATOS	Quito	02-2265-050	Nuñez de Vela E3-13 y Av. Atahualpa, Edif. Torre del Puente,

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
				piso 6
	MILLTEC S.A.	Quito	02-2457-022 02-2458-597	Av. Amazonas E3-131 y Río Guayas Edif. Rumiñahui, tercer piso, Of. 301.
	NEMETCOMPANY S.A.	Quito	02-2559-918	Av. Colón 1468 y 9 de Octubre Edito Solamar piso 5 oficina 505
	NETSPEED S.A.	Quito	02-2352-926	lote 13ª, calleB los Sauces en la Midad del Mundo
	NEW ACCESS S.A.	Quito	02-2444-701	Avenida Naciones Unidas E6-99 entre Shyris y Japón, edificio Banco Bolivariano piso 3 oficina 302
	OCITEL S.A.	Machala	07-2933-239 07-2935-465	9 de Octubre 1010 entre Juan Montalvo y 9 de mayo
	ONNET S.A.	Guayaquil	02-2849-950	

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	ORGANIZACION DE SISTEMAS E INFORMATICA OS S.A.	PORTOVIEJO	05-2933-347	Av. del Ejercito y calle Espana esquina de la ciudad de
	OTECEL S.A.	Quito	02-2227-700	Av. República y La Pradera esq.
	PACIFICTEL S.A.	Guayaquil	02-2560-200	Rocafuerte 732 y Roca. Edificio ROCASA
	PANCHONET	Quito	02-2549-800 02-2551-267 02-2229-569	Ruiz de Castilla 763 y Andagoya
	PARADYNE (Ecuador On Line)	Quito	02-2841-409	Av. Gran Colombia 23-116 y Unidad Nacional
	PLUSNET (PUNTONET)	Quito	02-2978-700 02-2759-060	
	Pontificia Universidad Católica de Ecuador	Quito	02-2565-627	Avenida 12 de Octubre 1076 y Rica de la ciudad de Quito
	PORTALDATA S.A	Ambato	03-2422-173 03-2422-172	Juan Benigno Vela 08-23 y Montalvo

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	PRODATA (HOY NET)	Quito	02-2261-431 02-2261-437	Av Atahualpa 955 y Republica Edif Digicom 7 piso
	RDH ASESORIA Y SISTEMAS S.A.	MANTA	05-2628-143	Av. 2 da. Entre calle 11 y 12
	READYNET CIA. LTDA.	Quito	02-2521-345 02-2525-044	Obispo Díaz de la Madrid 445 y La Isla
	RED GLOBAL DE INFORMACIÓN CIA.LTDA.	Cuenca	07-2850-190 07-2822-160	Av. Gran Colombia 20-122 y Unidad Nacional parroquia San Sebastián
	SATNET	Quito	2992444 2440829 2440827 2240228	Av. Eloy Alfaro N-44-406 y de las Higueras
	Servicios de Telecomunicaciones SETEL S.A.	Quito	2252798 2461181	Quito: Av. Eloy Alfaro N-44-406 y de las Higueras
	SITA	Quito	02-2567-221	Robles No. 653 y Amazonas Edif. Proinco Calisto Piso 3 Ofic. 309

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	SPEEDNET S.A.	Guayaquil	04-268-3083	Cdla. Kennedy Norte Av. Luis Orrantia Cornejo No. 24 y Dr. Victor Hugo Sicouret, Edif. Rafermart Piso1
	STEALTH TELECOM DEL ECUADOR S.A.	Quito	2248233	Vicente Fierro E15-13 y calle A, Urb. Analuisa, Batan Alto
	SURAMERICANA DE TELECOMUNIOCACIONES	Quito	2992444 2440829 2440827 2240228	Quito: Av. Eloy Alfaro N-44-406 y de las Higueras
	SYSTELECOM	Quito	223-2846 2227081	Selva Alegre Oe 5-301B y la Isla
	SYSTRAY S.A.	MANTA	05-2628861	Calle 11 y Av. 4 Edificio Cooperativa 15 de Abril piso 3 oficina 301
	TECHSOFTNET S.A.	Guayaquil	04-2566255	Calle P. Icaza # 437 y Baquerizo Moreno, Ed. Atahualpa 7mo.piso

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	TELCONET	Guayaquil	04-2680-555	Avenida de las Américas 1610 y Avenida Héroes de Verdeloma
	TELECOMUNICACIONES NETWORKING TELYNETWORKING C.A.,	Quito	02-2436-491 02-2435-870	Av. Atahualpa E3-49 y Juan Gonzalez (Edificio Perez Pallares) piso 8b
	TELYDATA TELECOMUNICACIONES Y DATOS CIA.	Quito	02-263-956 02-2263-857	Av: Amazonas N39-169 edificio Reinoso 5to. Piso, oficina 502
	TESAT S.A.	Guayaquil	04-2295-904	Guayaquil Centro Comercial Plaza Quil Local # 19 Quito: Isla Floreana 153 y Av. Los Shyris
	TRANSTELCO S.A.	Quito	02-2450-241	Av. 10 de agosto N37-288 y Villalengua
	UNISOLUTIONS INFORMATICA S.A.(Quik Internet)	Quito	02-2253-020 02-2460-364	AV. Gaspar de Villaroel E 10-292 y Av. 6 de Diciembre

LOGO	OPERADOR	DOMICILIO	TELÉFONO	DIRECCION
	UNIVERSIDAD TÉCNICA DE AMBATO	Ambato	03-2420-461 03-2849-164	Av. Los Chasquis s/n, Ciudadela Universitaria-Nueva Ambato, Sector Huachi
	UNIVERSIDAD TECNICA PARTICULAR DE LOJA	LOJA	07-2586-921 07-2570-275 ext.: 2651	San Cayetano s/n

ANEXO 2

ANEXO 2: DATOS DE CUENTAS DE USUARIO POR PERMISIONARIO (ISP)

DATOS DE CUENTAS Y USUARIOS DE INTERNET POR PERMISIONARIO	
MES	MARZO
AÑO	2009

No.	OPERADOR	COBERTURA	ACTUALIZADO	Cuentas Conmutadas	Cuentas Dedicadas	Cuentas Totales	Usuarios Conmutados	Usuarios Dedicados	Usuarios Totales
1	ACANUMAN	Esmeraldas, Portoviejo	31/03/2009	0	155	155	0	0	0
2	ADEATEL	La Troncal	***	***	***	***	***	***	***
3	ALEJANDRO DARIO PULECIO VILLALVA	Gquil, Quito, Cuenca, Babahoyo, Quevedo, Montalvo, Vinces, Baba, San Juan, Valencia, Ventanas	30/11/2005	0	62	62	0	62	62
4	ALIANZA NET	Quito	30/09/2007	0	138	138	0	410	410
5	AMOGHI S.A.	Latacunga	31/12/2005	13	21	34	52	97	149
6	ARTIANEXOS	Babahoyo	31/12/2005	0	37	37	0	37	37
7	ASAPTEL S.A.	Machala, Guayaquil y Puerto Baquerizo (Galápagos), Ambato.	30/06/2007	0	38	38	0	384	384
8	ASETECSA S.A.	Manta, Portoviejo, Gquil, Quito, Cuenca	31/03/2009	0	9	9	0	9	9
9	AT&T GLOBAL SERVICES	Quito y Guayaquil	30/09/2005	28	1	29	112	25	137
10	BARAINVER (TELFONET)	Esmeraldas, Quito, Ambato y Santo Domingo	31/12/2005	15	0	15	60	0	60
11	BARBERAN ARBOLEDA LINDBERGH STEVE	Portoviejo	***	***	***	***	***	***	***
12	BASTIDAS TONATO HARISOL CLEOPATRA	Prov. del Napo	***	***	***	***	***	***	***
13	BRAINSERVICES S.A.	Quito y Guayaquil	***	***	***	***	***	***	***
14	BRIGHTCELL	Quito y Guayaquil	30/06/2005	0	51	51	0	1830	1830
15	CARPIO ALEMAN MARCO ALEXANDER	Camión Sigsig	31/03/2009	0	7	7	0	48	48
16	CAVNET	Milagro	***	***	***	***	***	***	***
17	CENTER COMPUTER NET S.A.	Manta	***	***	***	***	***	***	***
18	COMDIGITRONIK S.A.	Quito	***	***	***	***	***	***	***
19	COMM&NET	Machala, Santa Rosa, Pasaje y Huaquillas	31/03/2009	0	102	102	0	259	259
20	COMPAÑIA DE SERVICIOS ELECTROMECANICOS PARA EL DESARROLLO CSED S.A.	Santo Domingo	30/09/2007	50	1	51	200	3	203
21	COMPIM S.A.	Guayaquil	30/09/2005	4	0	4	16	0	16
22	COMPSANET (FREDDY CALVA)	Yanuncay	30/09/2005	15	0	15	60	0	60
23	COMPUATEL	Quito	31/12/2005	0	135	135	0	249	249
24	CONECEL S.A.	Quito y Guayaquil	31/03/2007	1549	209	1758	6196	6270	12466
25	COSINET S.A.	Quito	30/09/2005	0	73	73	0	206	206
26	DENNYS ENRIQUE SAN LUCAS GARCIA	Portoviejo, Manta, Gquil, Quito, Cuenca, B. de Carsquez	31/12/2005	0	1	1	0	1	1
27	DINOLAN	Santo Domingo	30/06/2006	0	10	10	0	113	113
28	EASYNET S.A.	De acuerdo al contrato de concesión.	31/12/2005	2415	9273	11688	9660	9273	18933
29	ECUADOR TELECOM S.A.	Guayaquil y Quito	31/12/2005	0	15554	15554	0	52125	52125
30	ECUAENLACESATELITAL S.A.	Quito, Guayaquil y Cuenca	31/03/2007	65	39	104	260	124	384
31	ECUAONLINE	Quito, Guayaquil, Cayambe, Otavalo, Latacunga, Cuenca	31/12/2005	0	168	168	0	1011	1011
32	EFICENSA S.A.	Guayaquil y Manta	31/12/2005	34	0	34	136	0	136
33	ELECTROCOM (LA-TRO-KOM S.A.)	Ambato, Quito	31/03/2009	0	80	80	0	557	557
34	EMPRESA ELECTRICA REGIONAL CENTRO SUR C.A.	Cuenca	31/12/2005	0	3	3	0	125	125
35	EMPSETEL CIA. LTDA.	Prov. Del Oro	31/12/2005	8	6	14	32	118	150
36	ENTREPRENEURINC	Quito	31/12/2005	1	1	2	4	100	104
37	ESPOLTEL S.A.	Gquil, Salinas, Prosperina, Las Peñas, Manglar Alto, Santa Elena, Quito	31/03/2009	65	561	626	65	561	626
38	ETAPA TELECOM	Cuenca, Azoguez, Quito, Guayaquil	31/01/2009	15823	589	16412	63292	1557	64849
39	CNT (EX-ANDINATEL S.A.)	De acuerdo al contrato de concesión	31/03/2009	33003	58780	91873	132372	234148	366520
40	CNT (EX-PACIFICTEL S.A.)	Guayaquil, Quito y Cuenca	31/03/2005	2743	5757	8530	10972	110211	121183
41	FASTNET	Prov. Chimborazo	***	***	***	***	***	***	***
42	FIX WIRELESS (MARTHA PATRICIA AULESTIA)	Quito, Ambato, Ibarra y Esmeraldas	31/12/2005	24	28	52	96	160	256
43	FLATEL COMUNICACIONES CIA. LTDA.	Quito	31/03/2009	1	3	4	4	9	13
44	GIGOWIRELESS	Quito	31/12/2005	0	144	144	0	456	456
45	GLOBAL CROSSING ECUADOR	Quito	28/02/2009	7	623	630	28	39831	39859
46	GPF CORPORACION CIA LTDA.	Quito, Gquil, Cuenca, Ambato y Loja	31/12/2005	79	191	270	316	2072	2388
47	GRUPO BRAVCO	Quito, Cuenca, Gquil, Loja, Ambato e Ibarra	28/02/2009	78	91	169	312	2837	3149
48	GRUPO MICROSISTEMAS JOVICHSA S.A.	Quito	31/03/2009	0	221	221	0	4508	4508
49	GUEVARA PINEDA ALBERTO SIGIFREDO	Baños	30/09/2005	0	124	124	0	352	352
50	HARLEY DAVIDSON BARRIONUEVO COX	Prov. de Orellana	***	***	***	***	***	***	***
51	HERNAN MAURICIO DOMINGUEZ LIMAICO	Prov. De Imbabura	31/03/2009	0	2	2	0	2	2
52	IMBANET S.A.	Ibarra	31/12/2005	72	107	179	288	380	668
53	INDUSTRIA MARMOLERA ECUATORIANA S.A. IMESA	***	***	***	***	***	***	***	***
54	INFONET	Quito	31/12/2005	0	13	13	0	659	659
55	INFRATEL	Quito	31/12/2005	0	11	11	0	18	18
56	INTERCOM	Portoviejo	31/12/2005	195	0	195	792	0	792
57	INTERTEL	Quito	31/12/2005	13	161	174	52	429	481
58	INTRIAGO ROSADO FRANCISCO PATRICIO	Machala	***	***	***	***	***	***	***
59	JAIME PATRICIO PESANTEZ NIETO	El Triunfo	31/03/2009	19	6	25	76	72	148
60	JHONI JOEL JACOME GALARZA	Loja	30/09/2005	30	0	30	120	0	120
61	JOSE LUIS COX	Portoviejo, Gquil, B. de Carsquez	31/12/2005	0	17	17	0	68	68
62	KEIMBROOKS	Loja	31/12/2005	0	10	10	0	10	10
63	KOLVECH S.A.	Esmeraldas	***	***	***	***	***	***	***
64	LATINMEDIA	Guayaquil, Quito, Cuenca, Machala, Ambato, Manta.	31/03/2009	0	23	23	0	117	117
65	LOJASISTEM	Loja y Zamora	30/09/2005	0	23	23	0	139	139
66	LUCEÑA SPEED TELECOM Y CIA	Loja y Zamora Chinchipe	30/09/2005	0	5	5	0	305	305
67	LUTROL S.A.	Quito, Guayaquil, Santo Domingo, Manta y Ambato	31/03/2009	2102	6330	8432	8408	22779	31187
68	MACHALA NET S.A. MACHALANETSA	Machala	30/09/2005	0	72	72	0	288	288
69	MARTINEZ REVELO JORGE ISAAC	San Gabriel	31/03/2009	0	17	17	0	51	51
70	MEDIOS INTERACTIVOS MIWEBWORKS CIA. LTDA.	Quito Guayaquil y Cuenca	30/09/2005	0	158	158	0	8785	8788
71	MEGADATOS	Quito, Gquil, Cuenca, Ibarra, Latac, Ambato, Sto Domingo, Mach, Manta, Portoviejo, Salinas, Macas, Riobamba y Pto Ayora	28/02/2009	2961	904	3865	11844	18080	29924
72	MILLTEC	Quito	31/03/2009	123	181	304	492	474	966
73	MOINAVERY S.A.	Guayaquil y Quevedo	***	***	***	***	***	***	***
74	MUNDODIGITAL S.A.	Portoviejo, Manta , Quito y Guayaquil	***	***	***	***	***	***	***
75	NECUSOFT CIA. LTDA.	Prov. De Loja	30/09/2005	6	6	12	24	48	72
76	NEGOCIOS Y TELEFONIA (NEDETEL) S.A.	Guayaquil	31/03/2009	0	4	4	0	4	4
77	NEMETCOMPANY	Quito	30/09/2005	88	0	88	352	0	352
78	NETSPEED	Quito, Guayaquil, Cuenca, Manta, Esmeraldas, Machala, Libertad, Bahía de Carásquez	31/07/2006	0	2	2	0	2	2
79	NEW ACCESS	Quito	31/03/2009	66	57	123	264	570	834
80	OCEANTEL S.A.	Guayaquil	***	***	***	***	***	***	***

81	OCITEL S.A.	Machala, Santa Rosa, Pasaje, Huaquillas, Manta, Sto Domingo, Chone, Guayaquil.	***	***	***	***	***	***	***
82	ONNET	Gquil, Quito, Mach, Cuenca, Esmeraldas, Libertad, B. de Caraquez y Manta	31/03/2009	199	43	242	796	43	839
83	ORGANIZACIÓN DE SISTEMAS E INFORMATICA OS S.A.	Portoviejo, Manta, Guayaquil y Quito	31/03/2009	0	29	29	0	30	30
84	OSCAR ALDO TAPIA FLORES	Prov. De Zamora Chinchipe	31/12/2005	0	5	5	0	5	5
85	OTECEL S.A. (MOVISTAR)	Quito, Guayaquil, Cuenca, Ambato, Machala, Manta, Portoviejo	31/12/2005	275	266	541	1100	2996	4096
86	PACIFICBUSINESS S.A.	Guayaquil	***	***	***	***	***	***	***
87	PANCHONET S.A.	Quito, Cumbayá	31/03/2009	1901	2061	3962	7604	2061	9665
88	PARADYNE	Quito, Guayaquil y Cuenca	31/03/2009	3	40	43	12	181	193
89	PEREZ MENDIA RUTH EUGENIA	Ciudad de Azogues	30/09/2005	0	38	38	0	38	38
90	PEROBELI S.A.	Guayaquil	31/12/2005	0	18	18	0	18	18
91	PORTALDATA	Quito	31/03/2009	13	68	81	52	396	448
92	PRODATA [HOY NET]	Quito, Guayaquil, Ambato, Riobamba, Santo Domingo, Machala, Manta, Cuenca	31/12/2005	5	0	5	20	0	20
93	PUCENET	Quito	31/03/2009	98	0	98	392	0	392
94	PUNTO NET S.A.	Quito, Gquil, Sto Domingo y Cuenca	31/12/2005	3324	7223	10547	13296	42640	55936
95	RDH Asesoría y Sistemas S.A.	Quito, Guayaquil, Cuenca, Ambato, Machala, Manta	30/06/2006	53	0	53	212	0	212
96	READYNET	Quito y Guayaquil	31/12/2005	245	222	470	992	1133	2125
97	REGLOBIN RED GLOBAL DE LA INFORMACION CIA. LTDA.	Cuenca	31/03/2009	85	0	85	340	0	340
98	ROMULO PATRICIO MONTENEGRO TAMAYO	Prov. Imbabura	31/03/2009	0	3	3	0	6	6
99	SALAS TORRES CARLOS FERNANDO	Quito	30/06/2007	0	138	138	0	202	202
100	SANCHEZ GUTIERREZ CARLOS ENRIQUE	Cotacamanga	30/09/2005	0	1	1	0	4	4
101	SATNET	Quito, Guayaquil, Cuenca, Manta, Machala, Ambato, Santo Domingo, Latacunga, Riobamba, Ibarra, Otavalo, Loja ,Milagro, Salcedo, Azoguez, Santa Rosa, Huaquillas, Cayambe, Portoviejo.	31/12/2005	914	0	914	3656	0	3656
102	SERVICIOS DE INTERNET S.A. SERVINET	Quito y Guayaquil	***	***	***	***	***	***	***
103	SERVICIOS DE TRANSMISION INFORMATICA INTEGRALDATA	Prov de Pichincha y Guayas	31/12/2005	0	1	1	0	70	70
104	SETEL	Guayaquil	31/12/2005	0	42	42	0	272	272
105	SITA	Quito, Gquil, Cuenca, Portoviejo, Mach, Milagro, Ibarra, Sto Domingo, Latac, Riobamba y Azoguez	31/03/2009	12	92	104	48	92	140
106	SKYWEB S.A.	Guayaquil	***	***	***	***	***	***	***
107	SOCIEDAD CIVIL STARNET	Quito	30/06/2005	0	67	67	0	362	362
108	SPEEDNET S.A	Quito	30/06/2005	396	0	396	1584	0	1584
109	SPEEDYCOM CIA. LTDA.	Tungurahua, Pichincha y Cotopaxi	***	***	***	***	***	***	***
110	STEALTH TELECOM DEL ECUADOR S.A.	Quito y Guayaquil	31/03/2005	0	129	129	0	458	458
111	SURATEL	Gquil, Quito, Manta, Mach, Cuenca, Amb, Sto Domingo	31/12/2005	0	91000	91000	0	606912	606912
112	SYSTELECOM	Quito y Guayaquil	31/03/2009	0	35	35	0	133	133
113	SYSTRAY S.A.	Manta	31/05/2007	284	2	286	1136	2	1138
114	TECHSOFTNET S.A.	Manta, Gquil, Quito, Portoviejo, Mach, Esmer Cuenca	31/12/2006	0	46	46	0	309	309
115	TELCONET	Quito, Gquil, Loja, Cuenca, Manta, Sto Domingo, Cayambe, Mach, Portoviejo, Chone, B. de Caraquez, Otavalo, Latacunga, Riobamba, Esmer, Cuev, Ambato, Ibarra y Salinas	31/12/2005	1032	106	1138	4128	608	4736
116	TELECOMUNICACIONES NETWORKING TELYNETWORKING C.A.	Territorio nacional (Dial Up por terminales móviles)	31/12/2006	41	40	81	164	84	248
117	TELECSA S.A. [Alegro PCS]	Quito, Riobamba, Ambato	31/03/2007	40833	3094	43927	163332	3094	166426
118	TELEHOLDING S.A.	Quito	30/09/2005	0	1	1	0	40	40
119	TELYDATA CIA. LTDA.	Quito y Guayaquil	31/12/2005	26	297	323	104	927	1031
120	TESAT S.A.	Quito y Guayaquil	31/12/2007	0	1	1	0	30	30
121	TRANSELECTRIC S.A.	Pichincha, Los Rios, Guayas, Azuay, Tungurahua, Chimborazo y El Oro	31/03/2009	0	3	3	0	1051	1051
122	TRANSFERDATOS S.A.	Quito y Guayaquil	31/01/2009	0	2	2	0	2	2
123	TRANS-TELCO	Quito y Guayaquil	30/09/2005	0	474	474	0	539	539
124	UNISOLUTIONS INFORMÁTICA S.A.	Loja, Zamora, Chinchipe, El Oro	31/03/2009	104	2	106	416	4	420
125	UNIVERSIDAD DE CUENCA	Cuenca	***	***	***	***	***	***	***
126	UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	Loja, Zamora, Chinchipe, El Oro y Quito	31/12/2005	0	89	89	0	89	89
127	UNIVISA S.A.	Loja, Zamora, Chinchipe, El Oro	30/09/2005	33	0	33	132	0	132
128	VELASTEGUI RAMIREZ HOLGER KENNEDY	Ciudad de Santo Domingo	***	***	***	***	***	***	***
129	VILLACIS RODRIGUEZ HOLMER JAVIER	Montalvo	***	***	***	***	***	***	***
130	VIRTUALTEL	Prov Pichincha y Guayas	***	***	***	***	***	***	***
131	WICOMECUADOR	Prov Pichincha	***	***	***	***	***	***	***
132	WORKECUADOR INTERNET SERVICES	Quito	31/03/2005	0	11	11	0	94	94
133	ZAMBRANO ALCIVAR BECKER ERNESTO	Portoviejo	30/09/2005	0	9	9	0	9	9
	Total general			111.667	207.122	318.789	446.473	1.188.355	1.634.828

(***) No han remitido información

DESCRIPCIÓN DE LA INFORMACIÓN		
ACTUALIZADO		Es la fecha en que el operador remitió información de cuentas de Internet por última vez
Cuentas Conmutadas	*111.667*	Dentro de esta categoría se han incluido todas las cuentas de Internet que para hacer uso del servicio el usuario debe realizar la acción de marcar a un número determinado ya sea a través de las redes de telefonía fija o móvil.
Usuarios Conmutados	446.473	Ver Nota 2
Cuentas Dedicadas	*207.122*	Son todas aquellas cuentas que utilizan otros medios, que no sea Dial Up, para acceder a Internet, como puede ser ADSL, Cable Modem, Radio, etc.
Usuarios Dedicados	*1.188.355*	Son el número total de usuarios que los Proveedores de Servicios de Internet estiman que disponen por sus cuentas dedicadas
Cuentas Totales	*318.789*	Es la suma de las cuentas conmutadas más las cuentas dedicadas totales
Usuarios Totales	*1.634.828*	Ver Nota 3

Nota 1	La información publicada es recopilada directamente de los proveedores de Servicios de Internet.
Nota 2	Esta Superintendencia estima que por cada cuenta conmutada existe 4 usuarios, sin embargo anualmente se revisará este factor con el propósito de disponer estimaciones lo más aproximadas a la realidad.
Nota 3	El número de usuarios totales de Internet está dado por la suma de los usuarios Conmutados y Dedicados Totales.

ANEXO 3

ANEXO 3: DECRETO 1014

Nº 1014

RAFAEL CORREA DELGADO

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

CONSIDERANDO:

Que en el apartado g) del numeral 6 de la Carta Iberoamericana de Gobierno Electrónico, aprobada por el IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, realizada en Chile el 1 de Junio de 2007, se recomienda el uso de estándares abiertos y software libre, como herramientas informáticas;

Que es el interés del Gobierno alcanzar soberanía y autonomía tecnológica, así como un significativo ahorro de recursos públicos y que el Software Libre es en muchas instancias un instrumento para alcanzar estos objetivos;

Que el 18 de Julio del 2007 se creó e incorporó a la estructura orgánica de la Presidencia de la República la Subsecretaría de Informática, dependiente de la Secretaría General de la Administración, mediante Acuerdo Nº119 publicado en el Registro Oficial No. 139 de 1 de Agosto del 2007;

Que el numeral 1 del artículo 6 del Acuerdo Nº 119, faculta a la Subsecretaría de Informática a elaborar y ejecutar planes, programas, proyectos, estrategias, políticas, proyectos de leyes y reglamentos para el uso de Software Libre en las dependencias del gobierno central; y,

En ejercicio de la atribución que le confiere el numeral 9 del artículo 171 de la Constitución Política de la República;

DECRETA:

Artículo 1.- Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos.

Artículo 2.- Se entiende por Software Libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones puedan ser mejoradas.

Estos programas de computación tienen las siguientes libertades:

a) Utilización del programa con cualquier propósito de uso común
b) Distribución de copias sin restricción alguna.
c) Estudio y modificación del programa (Requisito: código fuente disponible)
d) Publicación del programa mejorado (Requisito: código fuente disponible).

Artículo 3.- Las entidades de la Administración Pública Central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software.

Artículo 4.- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de Software Libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

Para efectos de este decreto se comprende como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa del patrimonio nacional.

Nº 1014

RAFAEL CORREA DELGADO

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

a) Sistema en producción funcionando satisfactoriamente y que un análisis de costo beneficio muestre que no es razonable ni conveniente una migración a Software Libre.

b) Proyecto en estado de desarrollo y que un análisis de costo - beneficio muestre que no es conveniente modificar el proyecto y utilizar Software Libre.

Periódicamente se evaluarán los sistemas informáticos que utilizan software propietario con la finalidad de migrarlos a Software Libre.

Artículo 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica.
b) Regionales con componente nacional.
c) Regionales con proveedores nacionales.
d) Internacionales con componente nacional.
e) Internacionales con proveedores nacionales.
f) Internacionales.

Artículo 6.- La Subsecretaría de Informática como órgano regulador y ejecutor de las políticas y proyectos informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de este Decreto.

Para todas las evaluaciones constantes en este decreto la Subsecretaría de Informática establecerá los parámetros y metodología obligatorias.

Artículo 7.- Encárguese de la ejecución de este decreto los señores Ministros Coordinadores y el señor Secretario General de la Administración Pública y Comunicación.

Dado en el Palacio Nacional en la ciudad de San Francisco de Quito, Distrito Metropolitano, el día de hoy 10 de abril de 2008

f) Rafael Correa Delgado
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

ANEXO 4

ANEXO 4: ESPECIFICACIONES TÉCNICAS DE EQUIPOS

ZyXEL

Unified Security Gateway for Small and Medium-Sized Businesses

- Hybrid VPN
- Comprehensive Threat Protection
- IM/P2P Management
- User-Aware Policy Engine
- Bandwidth Management
- VoIP Security
- High Availability

Internet Security Appliance

ZyWALL USG 300

Benefits

Provides IPSec VPN and SSL VPN in a Single Box

ZyWALL USG 300 is a Unified Security Gateway that integrates comprehensive enterprise-class security features tailored for SMB (Small and Medium-sized Businesses).

With streamlined integration of both IPSec VPN and SSL VPN technologies, the ZyWALL USG 300 is an ideal solution for organizations requiring intensive VPN applications across distributed networks.

No matter you are in a remote branch office or at an unreliable hotel hotspot, the ZyWALL USG 300 can establish secure communication tunnels with IPSec and/or SSL protection. Another benefit of the integration is that the user-aware access control, scheduling, bandwidth usage and anti-threat security features can be enforced against inbound and outbound traffics of the protected network resources.

Real-time Protection against Ever-Evolving Threats

By integrating cutting-edge technologies on a robust platform, the ZyWALL USG 300 is competent to provide multi-layered security for security-aware businesses.

Powered by Kaspersky Labs, the gateway anti-virus security service on ZyWALL USG 300 has the world's shortest response time against emerging viruses; as a result, it helps stopping threats on the network edge and keeps viruses/malwares out of corporate networks. With dual SecuASIC (security co-processor) built-in, the ZyWALL USG 300 can still deliver robust and reliable performance even under heavy networking loads.

In addition, the IDP feature can detect harmful attacks and take necessary actions against the malicious or suspicious activities. The signature-based IDP engine can effectively detect protocol or traffic anomalies, support behavior pattern matching and prevent malicious attacks on the application layer.

Application Patrol to Manage the Use of IM/P2P Applications

The ZyWALL USG 300 is specially crafted to manage the use of IM/P2P applications in modern networking environments without hassle. Armed with AppPatrol, a central dashboard for managing various types of IM/P2P applications, security staff can easily create fine-grained access policies based on ever-changing security needs: identifying and restricting different access levels of prevailing IM/P2P protocols, restricting time of access for different groups of users, enforcing bandwidth quota against certain types of P2P application and prioritizing VoIP traffics to ensure best call quality over slow WAN ISP links. Altogether, the ZyWALL USG 300 is an ideal solution to solve the dilemma in terms of productivity and security.

User-Aware Policy Engine Enables Access Granularity

In addition to basic access control capabilities, the intelligent user-aware policy engine on the ZyWALL USG 300 is designed to make packet-forwarding decisions based on multiple criteria (such as user ID, user group, time of access and network quota, etc.). Furthermore, security staff can apply access policies against a variety of security features such as VPN, Content Filter and Application Patrol.

In conjunction with VLAN and custom security zones, corporate security policies can be effectively enforced to prevent unauthorized access to the network resources.

Bandwidth Management Ensures Quality of Service

The ZyWALL USG 300 provides bandwidth management features for traffic prioritization to guarantee or restrict bandwidth usage per interface/protocol. Security staff can allocate bandwidth for a variety of applications or computer hosts on the corporate network, regardless of the direction of the connection. For example, it's possible to assign higher priority and larger bandwidth to time-critical applications such as VoIP and video conferencing for quality transmission services. In addition, the ZyWALL USG 300 allows you to keep track of bandwidth usage with comprehensive statistical reports.

VoIP Security: Protecting the Converged Networks

Attracted by the benefits, more and more businesses are deploying VoIP applications on their networks. Along with the transition to VoIP also comes with security risks and voice quality issues.

As a VoIP-friendly firewall, the ZyWALL USG 300 reduces the security risks associated with the adoption of VoIP by offering the SIP/H.323 ALG feature to dynamically open only the required ports during VoIP calls; once the call is complete, the opened ports are automatically closed to prevent port sniffing. The IDP feature can detect and prevent attacks usually associated with VoIP deployments. Ultimately, by establishing VoIP traffics over VPNs with traffic prioritization, security staff can minimize security breaches while optimizing call quality over the existing ISP links.

High Availability Features Guarantee Non-Stop Operations for Mission-Critical Applications

With the High Availability features, the ZyWALL USG 300 helps the security staff to easily set up a highly reliable and secure network infrastructure for your business. To minimize the impact of single-point failures, the ZyWALL USG 300 supports device HA (High Availability) to assure network availability should any device failure happen.

On the WAN side, the ZyWALL USG 300 can connect multiple ISP links to ensure Internet availability in case a single ISP link becomes unreliable. The multiple-WAN load-balancing feature can also optimize the bandwidth usage over each ISP link.

Specifications

Performance and Capacity
- SPI Firewall Throughput: 200 Mbps
- IPSec VPN (AES) Throughput: 100 Mbps
- Maximum Concurrent NAT Sessions: 60,000
- Maximum IPSec VPN Tunnels: 200
- Maximum SSL VPN Tunnels: 10
- New Session Rate: 2,000 (sessions/sec)

Gateway Anti-Virus
- Stream-Based Gateway Anti-Virus Powered by Kaspersky Labs
- Covers Top Active Viruses In the Wild List
- Scans HTTP/FTP/SMTP/POP3/IMAP4
- Automatic Signature Update
- No File Size Limitation
- Blacklist/Whitelist

Application Patrol
- IM/P2P Granular Access Control
- Integrated with Scheduling/Rate-Limit/ User-Aware
- IM/P2P Up-To-Date Support*
- Real-Time Statistical Reports

*: Requiring valid IDP subscription

Intrusion Detection and Prevention
- In-line Mode (Routing/Bridge)
- Zone-Based IDP Inspection
- Customizable Protection Profile
- Signature-Based Deep Packet Inspection
- Automatic Signature Update
- Custom Signatures
- Traffic Anomaly: Scanning Detection and Flood Protection
- Protocol Anomaly: HTTP/ICMP/TCP/UDP

Content Filter
- URL Blocking, Keyword Blocking
- Exempt List (Blacklist and Whitelist)
- Blocks Java Applet, Cookies and Active X
- Dynamic URL Filtering Database (BlueCoat)

VPN
IPSec VPN
- Encryptions (AES/3DES/DES)
- Authentication (SHA-1/MD5)
- Key Management (Manual Key/IKE)
- Perfect Forward Secrecy (DH Group 1/2/5)
- NAT over IPSec
- Dead Peer Detection/Replay Detection
- PKI (X.509)
- Certificate Enrollment (CMP/SCEP)
- Xauth Authentication
- L2TP over IPSec Support

SSL VPN
- Clientless Secure Remote Access (Reverse Proxy Mode)
- SecuExtender (Full Tunnel Mode)
- Unified Policy Enforcement
- Supports Two Factor Authentication
- Customizable User Portal

Networking
- Routing Mode/Bridge Mode/Mixed Mode
- Layer 2 Port Grouping
- Ethernet/PPPoE/PPTP
- Tagged VLAN (802.1Q)
- Virtual Interface (Alias Interface)
- Policy-Based Routing (User-Aware)
- Policy-Based NAT (SNAT/DNAT)
- RIP v1/v2
- OSPF
- IP Multicasting (IGMP v1/v2)
- DHCP Client/Server/Relay
- Built-In DNS Server
- Dynamic DNS

Bandwidth Management
- Bandwidth Priority
- Policy-Based Traffic Shaping
- Maximum/Guaranteed Bandwidth
- Bandwidth Borrowing

SPI Firewall
- Zone-Based Access Control List
- Customizable Security Zone
- Stateful Packet Inspection
- DoS/DDoS Protection
- User-Aware Policy Enforcement
- ALG Supports Custom Ports

Authentication
- Internal User Database
- Microsoft Windows Active Directory
- External LDAP/RADIUS User Database
- ZyWALL OTP (One Time Password)
- Force User Authentication (Transparent Authentication)

High Availability
- Device HA (Active-Passive Mode)
- Device Failure Detection
- Link Monitoring
- Auto-Sync Configurations
- Multiple WAN Load Balancing
- VPN HA (Redundant Remote VPN Gateways)

System Management
- Role-Based Administration
- Simultaneous Administrative Logins
- Multi-Lingual Web GUI (HTTPS/HTTP)
- Object-Based Configuration
- Command Line Interface (Console/WebConsole/ SSH/TELNET)
- Comprehensive Local Logging
- Syslog (4 Servers)
- E-mail Alert (2 Servers)
- SNMP v2c (MIB-II)
- Real-Time Traffic Monitoring
- System Configuration Rollback
- Text-Based Configuration File
- Firmware upgrade via FTP/FTP-TLS/WebGUI
- Advanced Reporting (Vantage Report 3.1*)
- Centralized Network Management (Vantage CNM 3.0*)

*: Future release

Certifications
- ICSA Firewall Certified*
- ICSA IPSec VPN Certified*

*: Certificate pending

Hardware Specifications
- Memory: 256 MB RAM/256 MB Flash
- Interface: GbE x 7 (RJ-45, with LED)
- Auto-Negotiation and Auto MDI/MDI-X
- Console: RS-232 (DB9F)
- AUX: RS-232 (DB9M)
- LED Indicator: PWR, SYS, AUX, CARD1, CARD2
- Power Switch: Yes
- Reset Pinhole: Yes
- Extension Card Slot: Yes* (2)
- USB: Yes* (2)

*: These hardware accessories will be supported in future firmware release

Physical Specifications
- Rack Mountable: Yes (19-inch, rack-mount kit included)
- Dimensions: 430.0 (W) x 201.2 (D) x 42.0 (H) mm
- Weight: 2,800 g

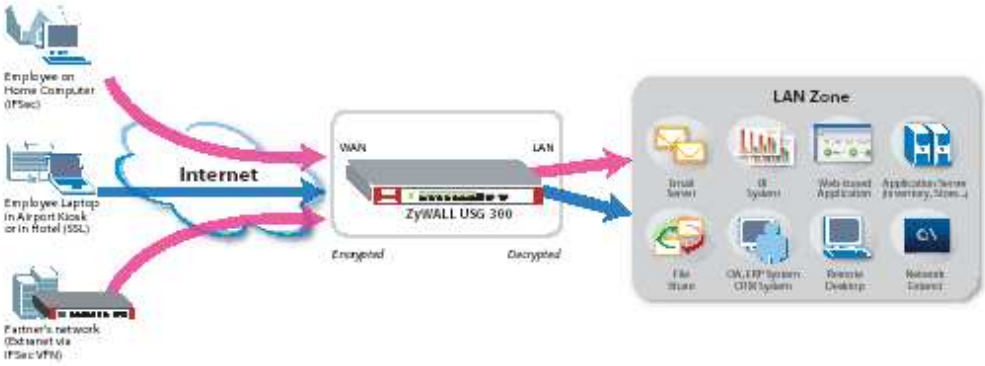
Power Requirement
- Input Voltage: 100-240 VAC, 50/60 Hz, 0.5-0.3 A
- Power Rating: 35 W Max

Environmental Specifications
- Operating Temperature: 0°C ~ 50°C
- Storage Temperature: -30°C ~ 60°C
- Humidity: 20% ~ 95% (non-condensing)

Standard Compliance
- HSF (Hazardous Substance Free): RoHS and WEEE
- EMC: FCC Part 15 Class A, CE-EMC Class A, C-Tick Class A, VCCI Class A
- Safety: CSA International (ANS/UL60950-1, CSA60950-1, EN60950-1, IEC60950-1)

Application Diagram

Incorporates both IPSec VPN & SSL VPN into a single box



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN

Content Control from BlueCoat

For more product information, visit us on the web www.ZyXEL.com

Copyright © 2007 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyXEL logo are registered trademark of ZyXEL Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.

605-100-0300026 07/07

ZyXEL

Unified Security Gateway for SMB/Mid-Large Organizations

- High-Performance VPN Concentrator
- Proactive Network Protection
- IM/P2P Management
- User-Aware Policy Engine
- Bandwidth Management
- VoIP Security
- High Availability

Internet Security Appliance

ZyWALL USG 1000

Benefits

High-Performance VPN Concentrator Integrating Both IPSec VPN and SSL VPN

ZyWALL USG 1000 is a Unified Security Gateway engineered to provide a variety of security services on top of a robust, hardware-accelerated platform.

By integrating both IPSec VPN and SSL VPN technologies, the ZyWALL USG 1000 allows organizations to establish Virtual Private Network (VPN) connections amongst multiple locations such as remote branch offices, business partner sites and even a remote teleworker getting connected in a potentially unsafe hotel hotspot.

Communication channels are securely encrypted so that information leakage/data theft can be mitigated when transmitting confidential information over insecure networks, such as the Internet.

The Hub and Spoke VPN feature is capable of reducing policy management overhead dramatically in a complex, multi-site corporate network infrastructure.

Proactive Network Protection against Blended Threats

By integrating cutting-edge technologies on a robust platform, the ZyWALL USG 1000 is competent to provide multi-layered protection for security-aware businesses.

The gateway anti-virus security service of the ZyWALL USG 1000 is powered by Kaspersky Labs, whose technology boasts the world's shortest response time against emerging viruses and spyware. As a result, it helps stopping blended threats at the network edge while keeping viruses/spyware out of corporate networks. With a SecuASIC co-processor built-in, the ZyWALL USG 1000 can deliver robust and reliable performance under real-world networking loads.

With the embedded signature-based IDP (Intrusion Detection and Prevention) engine, the ZyWALL USG 1000 performs L7 packet inspection for protocol/traffic anomaly or matched patterns. Thus, the ZyWALL USG 1000 provides comprehensive Intrusion Detection and Prevention capability to proactively detect and block potential worms, viruses, Trojans and VoIP threats, etc.

In response to the ever-evolving threats, up-to-date signatures/patterns are automatically downloaded from rock-solid ZSDN infrastructure and installed on your ZyWALL USG 1000.

Application Patrol to Manage the Use of IM/P2P Applications

The ZyWALL USG 1000 is specially crafted to manage the use of IM/P2P applications in modern networking environment without hassles. Armed with AppPatrol, a central dashboard for managing various types of IM/P2P applications, security staff can easily create fine-grained access policy based on ever-changing security needs: identifying and restricting different access levels of prevailing IM/P2P protocols, restricting time of access for different groups of users, enforcing bandwidth quota against certain types of P2P application and prioritizing VoIP traffics to ensure best call quality over slow WAN ISP links. Altogether, the ZyWALL USG 1000 is an ideal solution to solve the dilemma in terms of productivity and security.

User-Aware Policy Engine Enables Access Granularity

In addition to basic access control capabilities, the intelligent user-aware policy engine on the ZyWALL USG 1000 is designed to make packet-forwarding decisions based on multiple criteria (such as user ID, user group, time of access and network quota, etc.). Furthermore, security staff can apply access policies against a variety of security features such as VPN, Content Filter and Application Patrol.

In conjunction with VLAN and custom security zones, corporate security policies can be effectively enforced to prevent unauthorized access to network resources.

Bandwidth Management Ensures Quality of Service

The ZyWALL USG 1000 provides bandwidth management features for traffic prioritization to guarantee or restrict the bandwidth usage per interface/protocol. Security staff can allocate bandwidth for a variety of applications or computer hosts on the corporate network, regardless of the direction of the connection. For example, it's possible to assign higher priority and larger bandwidth to time-critical applications such as VoIP and video conferencing for quality transmission services. In addition, ZyWALL USG 1000 allows you to keep track of bandwidth usage with comprehensive statistical reports.

VoIP Security: Protecting the Converged Networks

Attracted the benefits, more and more businesses are deploying VoIP applications on their networks. Along with the transition to VoIP also comes with security risks and voice quality issues.

As a VoIP-friendly firewall, the ZyWALL USG 1000 reduces the security risks associated with the adoption of VoIP by offering the SIP/H.323 ALG feature to dynamically open only the required ports during the VoIP calls; once the call is complete, the opened ports are automatically closed to prevent port sniffing. The IDP feature can detect and prevent attacks usually associated VoIP deployment. Ultimately, by constructing VoIP traffic over VPNs with traffic prioritization, security staff could mitigate security breaches while optimizing call quality over existing ISP links.

High Availability Features Guarantee Non-Stop Operations for Mission-Critical Applications

With high availability features, the ZyWALL USG 1000 helps the security staff to easily set up a highly reliable and secure network infrastructure for your business. To minimize the impact of single-point of failures, the ZyWALL USG 1000 supports device HA (High Availability) to assure network availability should any device failure happen.

On the WAN side, the ZyWALL USG 1000 can connect multiple ISP links to ensure Internet availability while a single ISP link may be unreliable. The multiple WAN load balancing features optimizes bandwidth usage over each ISP link.

Specifications

Performance and Capacity
- SPI Firewall Throughput: 350 Mbps
- IPSec VPN (AES) Throughput: 150 Mbps
- Maximum Concurrent NAT Sessions: 200,000
- Maximum IPSec VPN Tunnels: 1,000
- Maximum SSL VPN Tunnels: 50
- New Session Rate: 13,000 (sessions/sec)

Gateway Anti-Virus
- Stream-Based Gateway Anti-Virus Powered by Kaspersky Labs
- Covers Top Active Viruses in the Wild List
- Scans HTTP/FTP/SMTP/POP3/IMAP4
- Automatic Signature Update*
- No File Size Limitation
- Blacklist/Whitelist

*: Requiring valid Anti-Virus subscription

Application Patrol (AppPatrol)
- IM/P2P Granular Access Control
- Integrated with Scheduling/Rate-Limit/User-Aware
- IM/P2P Up-To-Date Support*
- Real-Time Statistical Reports

*: Requiring valid IDP subscription

Intrusion Detection and Prevention
- In-line Mode (Routing/Bridge)
- Zone-Based IDP Inspection
- Customizable Protection Profile
- Signature-Based Deep Packet Inspection
- Automatic Signature Update*
- Custom Signatures
- Traffic Anomaly: Scanning Detection and Flood Protection
- Protocol Anomaly: HTTP/ICMP/TCP/UDP

*: Requiring valid IDP subscription

Content Filter
- URL Blocking, Keyword Blocking
- Exempt List (Blacklist and Whitelist)
- Blocks Java Applet, Cookies and Active X
- Content Filter Category Service* (Dynamic URL Filtering Database Powered by BlueCoat)

*: Requiring valid Content Filter subscription

VPN
IPSec VPN
- Encryptions (AES/3DES/DES)
- Authentication (SHA-1/MD5)
- Key Management (Manual Key/IKE)
- Perfect Forward Secrecy (DH Group 1/2/5)
- NAT over IPSec
- Dead Peer Detection/Replay Detection
- PKI (X.509)
- Certificate Enrollment (CMP/SCEP)
- Xauth Authentication
- VPN Concentrator (Hub and Spoke VPN)
- L2TP over IPSec Support

SSL VPN
- Clientless Secure Remote Access (Reverse Proxy Mode)
- SecuExtender (Full Tunnel Mode)
- Unified Policy Enforcement
- Supports Two Factor Authentication
- Customizable User Portal

Networking
- Routing Mode/Bridge Mode/Mixed Mode
- Layer 2 Port Grouping
- Ethernet/PPPoE/PPTP
- Tagged VLAN (802.1Q)
- Virtual Interface (Alias Interface)
- Policy-Based Routing (User-Aware)
- Policy-Based NAT (SNAT/DNAT)
- RIP v1/v2
- OSPF
- IP Multicasting (IGMP v1/v2)
- DHCP Client/Server/Relay
- Built-in DNS Server
- Dynamic DNS

Bandwidth Management
- Bandwidth Priority
- Policy-Based Traffic Shaping
- Maximum/Guaranteed Bandwidth
- Bandwidth Borrowing

SPI Firewall
- Zone-Based Access Control List
- Customizable Security Zone
- Stateful Packet Inspection
- DoS/DDoS Protection
- User-Aware Policy Enforcement
- ALG Supports Custom Ports

Authentication
- Internal User Database
- Microsoft Windows Active Directory
- External LDAP/RADIUS User Database
- ZyWALL OTP (One Time Password)
- Force User Authentication (Transparent Authentication)

High Availability
- Device HA (Active-Passive Mode)
- Device Failure Detection
- Link Monitoring
- Auto-Sync Configurations
- Multiple WAN Load Balancing
- VPN HA (Redundant Remote VPN Gateways)

System Management
- Role-Based Administration
- Simultaneous Administrative Logins
- Multi-Lingual Web GUI (HTTPS/HTTP)
- Object-Based Configuration
- Command Line Interface (Console/WebConsole/SSH/TELNET)
- Comprehensive Local Logging
- Syslog (4 Servers)
- E-mail Alert (2 Servers)
- SNMP v2c (MIB-II)
- Real-Time Traffic Monitoring
- System Configuration Rollback
- Text-Based Configuration File
- Firmware upgrade via FTP/FTP-TLS/WebGUI
- Advanced Reporting (Vantage Report 3.1 Patch 1*)
- Centralized Network Management (Vantage CNM 3.0*)

*: Future release

Certifications
- ICSA Firewall Certified*
- ICSA IPSec VPN Certified*

*: Certificate pending

Hardware Specifications
- Memory: 1 GB RMB RAM/256 MB Flash
- Interface: GbE x 5 (RJ-45, with LED)
- Auto-Negotiation and Auto MDI/MDI-X
- Console: RS-232 (DB9F)
- AUX: RS-232 (DB9M)
- LED Indicator: PWR, SYS, AUX, HDD
- Power Switch: Yes
- Reset Pinhole: Yes
- Extension Card Slot: Yes* (1)
- USB: Yes* (2)
- Optional HDD: Yes* (IDE, 2.5")

*: These hardware accessories will be supported in future firmware release

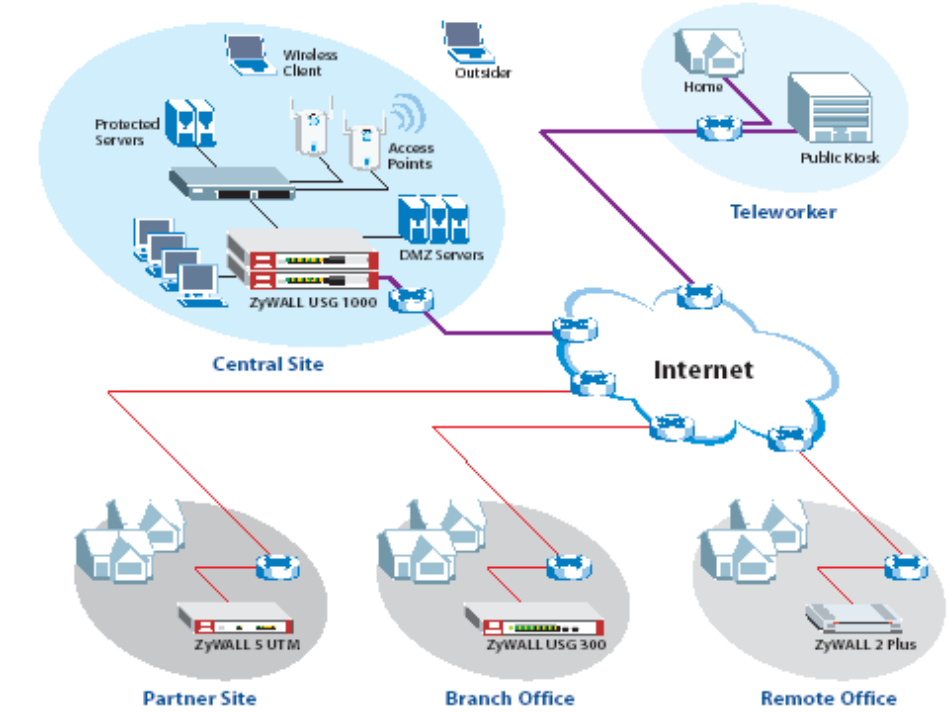
Physical Specifications
- Rack Mountable: Yes (19-Inch, rack-mount kit included)
- Dimensions: 430.7 (W) x 292.0 (D) x 43.5 (H) mm
- Weight: 4,700 g

Power Requirements
- Input Voltage: 100-240 VAC, 50/60 Hz, 1 A Max
- Power Rating: 80 W Max

Environmental Specifications
- Operating Temperature: 0°C ~ 40°C
- Storage Temperature: -30°C ~ 60°C
- Humidity: 5% ~ 90% (non-condensing)

Standard Compliance
- HSF (Hazardous Substance Free): RoHS and WEEE
- EMC: FCC Part 15 Class A, CE-EMC Class A, C-Tick Class A, VCCI Class A
- Safety: CSA International (ANS/UL60950-1, CSA60950-1, EN60950-1, IEC60950-1)

Application Diagram



Powered by Kaspersky, BlueCoat, ICSA Firewall, ICSA VPN

Content Control from BlueCoat

For more product information, visit us on the web www.ZyXEL.com

Copyright © 2007 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyXEL logo are registered trademarks of ZyXEL Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.

65-100-010208 09/07

RB411

The heart of RB411 is the new Atheros CPU which makes this tiny device a quick one. Tests show that it is up to three times more powerful than our previous model.

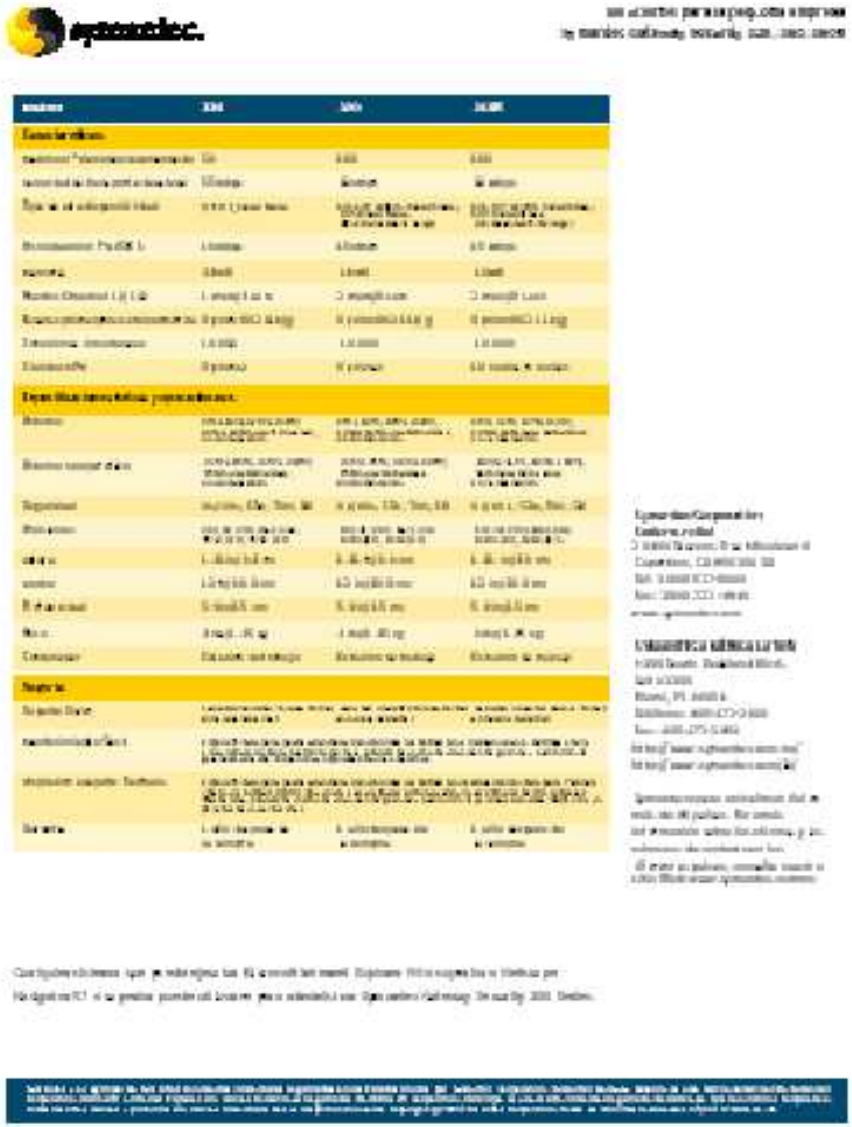
Comparing to RB411, the RB411A adds more memory and a Level4 license, and the RB411AH adds the high performance AR7161 680MHz CPU.

The RB411 includes RouterOS - the operating system, which will turn this powerful system into a highly sophisticated router, firewall or bandwidth manager.

One small device - with all the power of RouterOS, and our most affordable one.

CPU	Atheros AR7130 300MHz (AR7161 680MHz for the AH model)
Memory	32MB DDR SDRAM onboard memory (64MB for the A and AH models)
Boot loader	RouterBOOT
Data storage	64MB onboard NAND memory chip
Ethernet	One 10/100 Mbit/s Fast Ethernet port with Auto-MDI/X
miniPCI	One MiniPCI Type IIIA/IIIB slot
Extras	Reset switch, Beeper
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power, NAND activity, 5 user LEDs
Power options	Power over Ethernet: 10..28V DC (except power over datalines). Power jack: 10..28V DC
Dimensions	10.5 cm x 10.5 cm (4.13 in x 4.13 in) Weight: 82 g (2.9 oz)
Power consumption	~3W without extension cards, maximum ~ 12 W
Operating System	MikroTik RouterOS v3, Level3 license (RB411A and AH: Level4)

Symantec Gateway Security 220, 260, 2000
Poderosa protección de firewall para redes de pequeñas empresas



ANEXO 5

ANEXO 5: PROFORMAS

ALDEBERAN
...su socio tecnológico

Quito, 28 de Agosto de 2008

GNO08-00103

Señor Ingeniero
DIEGO PADILLA
Gerente Técnico
TELYDATA
Ciudad.

De nuestras consideraciones:

Por medio de la presente ponemos a su disposición los recursos y soporte de Aldeberan Cía. Ltda. representante en el Ecuador de equipos MultiTech, Alvarion, Solomon y Zyxel. Nuestra línea de productos cumple con estándares y normas internacionales de calidad y especificaciones técnicas así como de compatibilidad de operación en sistemas abiertos. Los equipos son diseñados para ofrecer soluciones prácticas de excelente calidad y bajo costo.

A continuación se proporciona una breve descripción, así también las principales características de la familia de equipo **Zywall** el cual consideramos podrían ser de gran utilidad y de inmediata aplicación en cubrir las necesidades de comunicación de forma rápida, confiable y económica

INTERNET SECURITY APPLIANCE/ROUTER ZYWALL

El dispositivo de seguridad de Internet, está diseñado para maximizar la seguridad en la red sin tener que comprometer el rendimiento de la misma.

Este dispositivo utiliza encriptación de datos, Autentificación de Usuarios, y el Internet para conectar de manera segura usuarios, oficinas remotas, clientes o proveedores con la oficina corporativa mientras se evita el costo de líneas privadas dedicadas.

La funcionalidad del VPN, está basada en protocolos IPSec, con encriptación de 168 bits para asegurar que la información permanezca privada.

Para proporcionar seguridad el Firewall utiliza Inspección de Paquetes por Estado (Stateful Packet Inspection) entre otros y Filtrado de Contenido de paginas WEB

CARACTERÍSTICAS

- Actualizaciones del Sistema para proteger su red contra las últimas amenazas.
- Navegación concurrente de varios usuarios.
- Acceso a Internet dedicado con ancho de banda compartido usando una sola dirección IP
- Monitoreo y reporte de tráfico.
- Control de acceso a Internet para clientes o filtros de sitios para prevenir el uso no autorizado de Internet.
- Protección de contra denegación de servicio (DoS y DDoS).
- Administración de Ancho de Banda (depende del modelo).

La presente oferta es propiedad de Aldeberan Cía. Ltda., para uso interno exclusivo del cliente, y no podrá ser utilizada total ni parcialmente para conocimiento de otras empresas.

Guayaquil: Cdla. Urdenor I Mz.1030 (131) V.19 +593 4 600 5893 e-Mail: mercadeo@aldeberan.com.ec
Quito: Manuel Valdiviezo Oe6-142 y Thomas Chariove +593 2 227 0315

- Capacidad Inalámbrica (depende del modelo).
- Una o mas zonas desmilitarizada –DMZ- (depende del modelo).
- Balanceo de carga y respaldo a través de dos interfaces WAN-dual WAN- (depende del modelo).
- Priorización del uso del acceso a Internet contratado, basado en políticas (depende del modelo).
- ICSA certificado.

REDES PRIVADAS VIRTUALES (VPN)

Las redes privadas virtuales son ideales para usuarios de negocios que viajan frecuentemente.

- Permite comunicar oficinas remotas a través de enlaces seguros para aplicaciones como: acceso a la red corporativa, transferencias de archivos, e-mail, navegación en la Web, envío o recepción de mensajes o telefonía IP.
- Asegura sus comunicaciones en el Internet en cualquier momento y en cualquier lugar.
- Formación de las VPNs LAN to LAN.
- ICSA certificado.

Propuesta Económica:

Cant.	Descripción	Valor Unitario	Valor Total +IVA
		US$	US$
1	ZyWALL 35 - 35 VPN Tunnels, Dual WAN	503,00	563,36

*** Los precios no incluyen instalación, configuración e inducción de los equipos.**

Consideraciones Comerciales

Forma de Pago
100% para los equipos en inventario, de no estar en inventario considere 50% a la orden y el 50% contra entrega.

Plazo de Entrega Inmediata, salvo venta previa. Y para los productos que no están en inventario considere Veinte(20) días aproximadamente.

Garantía
El producto posee una garantía de 24 meses contra desperfectos de fábrica.

Atentamente,

Geovanna Narváez O.

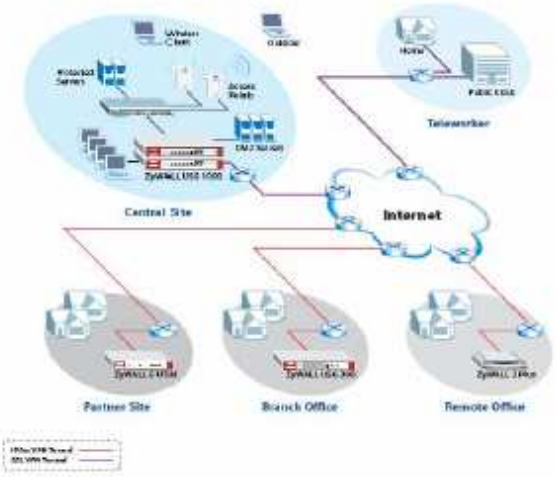
La presente oferta es propiedad de Aldeberan Cia. Ltda., para uso interno exclusivo del cliente, y no podrá ser utilizada total ni parcialmente para conocimiento de otras empresas.

ALDEBERAN
...su socio tecnológico

Propuesta Económica Firewall/Router Zywall USG1000

Cant.	Descripcion	Precio US$	Total US$
1	Firewall ZyWALL USG1000 - 1000VPN, 200.000 Sesiones 5x10/100/1000 Ethernet, 200 Usuarios.	3.533,00	3.533,00
1	Instalación/inducción Firewall ZyXEL USG 1000	425,00	425,00
1	ICARD 1 año Cont Filter ZYL	992,00	992,00
1	ICARD 1 año IDP ZYwall	340,00	340,00
1	ICARD 1 año AV Kaspersky	446,00	446,00
		Total	5.736,00
		Total+IVA	6.424,32

Características técnicas de la solución



La presente oferta es propiedad de Aldeberan Cía. Ltda., para uso interno exclusivo del cliente, y no podrá ser utilizada total ni parcialmente para conocimiento de otras empresas.

ALDEBERAN
...su socio tecnológico

Propuesta: 355 Fecha: 1/29/2009

Preparado para:
Ingeniero(a) Diego Padilla
TelyData Telecomunicaciones y Datos Cia. Ltda
Av. Amazonas N39-169 y Gaspar de Villarroel. Edif
Quito, Pichincha Ecuador

Prepared by: Geovanna C. Narvaez
Account No.: 294
Phone: 022263956

Qty.	Item ID	Description	UOM	Sell	Total
1	Zywall USG1000	Internet Security Appliance USG1000	EA	$3,676.00	$3,676.00
1	Zywall USG300	Internet Security Appliance	EA	$1,395.00	$1,395.00
				Item Total:	$5,071.00
				Sales Tax at 12.000%:	$608.52
				GS Tax:	$0.00
				Total:	**$5,679.52**

Prices are firm until 2/13/2009 Terms: 50%- 50% 30D

Quoted by: Geovanna C. Narvaez, geovanna.narvaez@aldeberan.com.ec **Date:** 1/29/2009
45 dias..

Accepted by: _____ **Date:** _____

ALDEBERAN
...su socio tecnológico

Propuesta: 356 Fecha: 1/29/2009

Preparado para:
Ingeniero(a) Diego Padilla
TelyData Telecomunicaciones y Datos Cia. Ltda
Av. Amazonas N39-169 y Gaspar de Villarroel. Edif
Quito, Pichincha Ecuador

Prepared by: Geovanna C. Narvaez
Account No.: 294
Phone: 022263956

Qty.	Item ID	Description	UOM	Sell	Total
4	NanoStation5	Nano Station 5 - %Ghz, 14 dBi, AAP, Ext, Ant, AirOS	EA	$128.81	$515.24
1	PS5-EXT	PS5-EXT CPE	EA	$262.86	$262.86
4	NanoStation2	Nano Station 2 - Ghz, 14 dBi, AAP, Ext, Ant, AirOS	EA	$118.95	$475.80
1	PS2	Radio 2.4Ghz con antena integrada	EA	$243.40	$243.40
				Item Total:	$1,497.30
				Sales Tax at 12.000%:	$179.68
				GS Tax:	$0.00
				Total:	**$1,676.98**

Prices are firm until 2/13/2009 Terms: Prepagado

Quoted by: Geovanna C. Narvaez, geovanna.narvaez@aldeberan.com.ec **Date:** 1/29/2009

45 dias..

Accepted by: _____ **Date:** _____