ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA EN SISTEMAS

ANALISIS Y DISEÑO DE LA RED DE DATOS, PARA LA IMPLEMENTACIÓN DEL SISTEMA DE PENSIONES DEL IESS, VÍA WEB

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

CALI NIETO FRANKLIN LEONARDO
Email: fcalinieto@cmm.com.ec
PASQUEL MARTINEZ MARLON JAVIER
Email: mpasquel@gmail.com

DIRECTOR: ING. NELSON ÁVILA JIMÉNEZ
Email: navila@uio.satnet.net

Quito, Julio 2008

DECLARACIÓN

Nosotros, Franklin Cali Nieto y Marlon Pasquel Martínez, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros 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.

Franklin Cali Nieto **Marlon Pasquel Martínez**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Franklin Leonardo Cali Nieto y Marlon Javier Pasquel Martínez, bajo mi supervisión.

ING. NELSON ÁVILA
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios, quien es el ser que me da fortaleza y sabiduría para culminar esta meta, a mi familia, a mis padres y hermanos, gracias por el apoyo incondicional y por haber creído en mi, a mi esposa gracias por su paciencia y compresión.

A mis maestros universitarios, por su compromiso de formar profesionales de gran calidad.

No podía olvidarme de mis amigos dentro y fuera de mi vida universitaria, por su apoyo constante, y su amistad sincera.

A mi padre y amigos que están lejos, a quienes recuerdo gratamente.

Sinceramente,

FRANKLIN LEONARDO CALI NIETO

DEDICATORIA

A mi Padre, quien supo guiarme y darme fuerza de voluntad para seguir adelante y superarme cada día, a mi familia quienes se han convertido en mi motivo y razón de vida para luchar, a mi madre y hermanos quienes siempre confiaron en mí.

FRANKLIN LEONARDO CALI NIETO

CONTENIDO

CONTENIDO I
RESUMEN IX
PRESENTACIÓN X
CAPITULO 1 1
INTRODUCCIÓN. 1
1.1 CONVERGENCIA. 6
1.2 MOVILIDAD. 8
1.3 ESCALABILIDAD 9
1.4 ALTA DISPONIBILIDAD. 12
1.5 INTEROPERABILIDAD. 14
1.6 SEGURIDAD. 16
CAPITULO 2 21
ANÁLISIS Y DEFINICIÓN DE REQUERIMIENTOS. 21
2.1 EL SISTEMA DE PENSIONES DENTRO DE LA SEGURIDAD SOCIAL. 21
2.2 COBERTURA GEOGRÁFICA DEL SEGURO DE PENSIONES. 22
2.3 ANÁLISIS DE LA SITUACIÓN ACTUAL 23
2.3.1 SOBRE LAS APLICACIONES. 25
2.3.2 SOBRE EL HARDWARE 26
2.3.3 REDES DE TELEPROCESO. 28
2.3.4 POLÍTICAS DE MANTENIMIENTO. 29
2.3.5 RECURSO HUMANO INFORMÁTICO. 29
2.4 DEFINICIÓN DE REQUERIMIENTOS. 30
2.4.1 APLICACIONES INFORMÁTICAS. 30
2.4.2 SERVICIOS INFORMÁTICOS. 31
2.4.3 EQUIPO INFORMÁTICO. 32
2.4.4 EQUIPAMIENTO DE RED LAN Y WAN. 33
2.4.5 CABLEADO ESTRUCTURADO. 34
2.4.6 RED DE ENERGÍA ELÉCTRICA Y SISTEMA DE RESPALDO (UPS). 35
CAPITULO 3 38
DISEÑO DE LA SOLUCIÓN 38
3.1 DISEÑO DE LA SOLUCIÓN DE RED DE ÁREA LOCAL (LAN). 38
3.1.1 RED LAN DEL CENTRO DE DATOS PRINCIPAL. 39
3.1.1.1 Requerimientos de red LAN del Centro de Datos Principal. 39
3.1.1.2 Criterios de Diseño. 39
3.1.1.3 Protocolos de red. 40
3.1.1.4 Arquitectura de red. 41
3.1.2 RED LAN DE LAS OFICINAS REMOTAS. 44
3.1.2.1 Requerimientos de red LAN de oficinas remotas. 44
3.1.2.2 Criterios de Diseño. 44
3.1.2.3 Protocolos de red. 45
3.1.2.4 Cableado Estructurado. 46
3.1.2.5 Arquitectura de red. 46
3.1.2.5.1 Red LAN con backbone. 46
3.1.2.5.2 Red LAN sin backbone. 50
3.2 DISEÑO DE LA SOLUCIÓN DE RED DE ÁREA AMPLIA (WAN) 52
3.2.1 REQUERIMIENTOS DE RED WAN. 53

3.2.2 PLANTEAMIENTO DE LA SOLUCIÓN. 53
3.2.3 TOPOLOGÍA DE RED. 54
3.2.4 DIRECCIONAMIENTO DE RED WAN. 55
3.2.5 CAPACIDAD DE CANALES DE TELECOMUNICACIONES. 56
CAPITULO 4 59
ANALISIS DE SERVICIOS DE RED. 59
4.1 SERVICIOS. 59
4.1.1 SERVICIOS A NIVEL DE RED. 59
4.1.1.1 Servidor de Nombres de Dominio. 60
4.1.1.2 Protocolo de configuración de host dinámico. 60
4.1.1.3 Servicio de información de red. 60
4.1.2 SERVICIOS A NIVEL DE USUARIOS. 61
4.1.2.1 Correo Electrónico. 61
4.1.2.2 Protocolo de Transporte de Hipertexto (HTTP). 61
4.1.2.3 Servidor de Archivos. 61
4.1.2.4 Proxy. 62
4.2 PLANTEAMIENTO DE LA SOLUCION. 62
4.2.1 IMPLEMENTACION DE LOS SERVICIOS DE RED. 62
4.2.2 IMPLEMENTACION DE LOS SERVICIOS DE USUARIO. 64
4.2.2.1 Proxy. 64
4.2.2.2 Correo Electrónico. 65
4.2.2.3 Implementación del Servidor de Archivos. 67
4.3 IMPLEMENTACION DE SERVICIOS Y APLICACIONES WEB. 67
4.3.1 CAPA WEB. 68
4.3.2 CAPA DE APLICACIONES. 69
4.3.3 CAPA DE BASE DE DATOS. 70
CAPITULO 5 71
PLANTEAMIENTO DE LA POLITICA DE SEGURIDAD. 71
5.1 ANALISIS DE ACTIVOS DE INFORMACION DE LA ORGANIZACIÓN. . 71
5.1.1 IDENTIFICACION DE LA INFORMACION Y SERVICIOS. 72
5.1.2 IDENTIFICACION DE AMENAZAS. 74
5.1.3 IDENTIFICACION DE VULNERABILIDADES. 75
5.1.4 CONSECUENCIAS DE UN INCIDENTE A LA SEGURIDAD. 76
5.1.5 DETERMINACION DE REQUERIMIENTOS DE SEGURIDAD. 77
5.2 ANALISIS DE RIESGOS PARA LA RED DEL SEGURO DE PENSIONES. 77
5.2.1 INFORMACION INSTITUCIONAL. 78
5.2.2 ANALISIS DE RIESGOS A LA SEGURIDAD. 78
5.2.3 IDENTIFICACION DE INFORMACION Y SERVICIOS. 78
5.2.4 IDENTIFICACION DE AMENAZAS. 81
5.2.5 IDENTIFICACION DE VULNERABILIDADES. 83
5.2.6 VULNERABILIDADES ORGANIZACIONALES. 84
5.2.7 VULNERABILIDADES TECNOLOGICAS. 85
5.2.8 CONCECUENCIAS DE UN INCIDENTE DE SEGURIDAD. 88
5.2.9 DETERMINACION DE REQUERIMIENTOS DE SEGURIDAD. 90
5.2.9.1 Requerimientos Técnicos de Seguridad. 90
5.2.9.2 Requerimientos de Seguridad Administrativa. 92
5.3 POLÍTICAS DE SEGURIDAD INFORMÁTICA. 96
5.3.1 INTRODUCCION. 96
5.3.2 POLITICA INSTITUCIONAL 96

5.3.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 96
5.3.3.1 Conceptos 96
5.3.3.2 Clasificación de la Información. 97
5.3.4 POLÍTICAS DE SEGURIDAD DEL PERSONAL. 98
5.3.4.1 Ética. 98
5.3.4.2 Políticas de Claves. 99
5.3.4.3 Políticas Generales de Software. 101
5.3.4.4 Redes. 102
5.3.4.5 Módems. 102
5.3.4.6 Correo Electrónico. 102
5.3.4.7 Internet. 103
5.3.4.8 Laptops y Computadores Portables. 104
5.3.5 POLITICAS DE SEGURIDAD DE COMPUTADORES Y REDES 105
5.3.5.1 Políticas de Administración del Sistema. 105
5.3.5.2 Seguridad Física. 106
5.3.5.3 Políticas de Ingreso a los Sistemas. 107
5.3.5.4 Auditoria. 108
5.3.5.5 Contabilización y Auditoria 109
5.3.5.6 Confiabilidad del Servicio. 110
5.3.5.7 Políticas de Redes y Sistemas Distribuidos. 111
5.3.5.8 Firewall para Internet 114
5.3.5.9 Interfaces a otras redes. 116
5.3.5.10 Políticas de Desarrollo de Software 117
5.3.6 EJECUCION. 118
CAPÍTULO 6 119
ANALISIS DE COSTOS 119
6.1 ANÁLISIS DE COSTOS. 119
6.2 PRESUPUESTO POR DEPENDENCIA. 119
6.3 PRESUPUESTO CONSOLIDADO DE DEPENDENCIAS. 126
6.4 ANALISIS DE COSTOS DE LOS ENLACES. 127
6.5 COSTOS DE LOS EQUIPOS DEL CENTRO DATOS 128
6.6 CONSOLIDACION DE COSTOS FIJOS DEL PROYECTO. 129
6.7 CONSOLIDACION COSTOS DE TELECOMUNICACIONES. 129
CAPITULO 7 131
CONCLUSIONES Y RECOMENDACIONES. 131
ANEXO I ..... - 1 -
ANEXO II ..... - 3 -
ANEXO III ..... - 29 -
ANEXO IV ..... - 34 -
ANEXO V ..... - 38 -

RESUMEN

El presente Proyecto, se centra en el Análisis y Diseño de la red de datos, para la implementación del sistema de Pensiones del IESS, vía Web. Contiene un análisis del estado actual de las tecnologías de la información. Se describe los conceptos bajo los cuales se diseñan e implementan en la actualidad las redes de información; así como también, se revisa los últimos protocolos y estándares que se han incorporado en el equipamiento tanto de red LAN como WAN.

Con el fin de tener un conocimiento cabal del Seguro de Pensiones del Instituto Ecuatoriano de Seguridad Social, se realiza inicialmente una descripción de la misión, visión y papel que cumple dentro del sistema de Seguridad Social.

La realidad tecnológica del Seguro de Pensiones, es analizada, a la vez que se determina los requerimientos del Seguro para poder tener el marco de referencia sobre el cual se plantean las posibles soluciones.

Elemento central del presente trabajo es lo relacionado a las soluciones de red LAN y red WAN, en la cual se describe las arquitecturas de red, los protocolos y estándares con los cuales se construyen las redes y las especificaciones técnicas de los equipos informáticos y de telecomunicaciones que son parte de la solución.

Los servicios de red, cumplen un papel importante dentro de las redes de datos, estos se describen tanto en lo relacionado a los servicios que las redes utilizan para tener una operación adecuada, así como también los servicios de usuario.

Tratándose de una solución que tiene como uno de los elementos constitutivos el acceso vía Web, se plantea la política de seguridades que demanda una infraestructura informática de este tipo.

Finalmente se presenta un análisis de costos de la solución propuesta.

PRESENTACIÓN

Dentro del proceso de modernización del Instituto Ecuatoriano de Seguridad Social, y con la finalidad de llevar adelante el plan Estratégico Institucional, el Seguro de Pensiones, ha redefinido sus procesos internos con miras a brindar a sus usuarios un servicio eficaz, eficiente, oportuno y de calidez. Es en este contexto, que surge la necesidad, de contar con una infraestructura tecnológica alineada a estos nuevos requerimientos de la Organización, que permita automatizar procesos internos; hacer un manejo moderno de la información, que garantice la integridad, confiabilidad y oportunidad de la misma para la toma de decisiones; hacer eficientes los canales tradicionales de servicio al cliente y poner en operación canales alternativos, utilizando para ello, tecnología de última generación.

Uno de los ejes fundamentales de la modernización, es el mejoramiento del servicio que se brinda a los usuarios, para lo cual se ha visto necesario incorporar al portafolio de servicios, medios electrónicos de servicio al cliente. El Seguro de Pensiones está desarrollando un sistema informático que contempla los procesos de Jubilación y Cesantía, estos permitirán a los afiliados de la Institución, presentar sus solicitudes de jubilación vía Internet, facilitando de esta manera el acceso a los trámites con la Institución y adicionalmente mejorando los tiempos de respuesta en la concesión de las prestaciones.

La infraestructura tecnológica que dará soporte a este sistema informático es motivo del presente trabajo, el cual cubre el análisis y diseño de la red de datos, incluyendo las especificaciones técnicas de los elementos activos y pasivos. El diseño también incluirá la integración de los diferentes subsistemas como solución global para la puesta en operación de la aplicación.

El capítulo 1 tiene una función introductoria, donde se hace una revisión del estado actual de las redes de área local (LAN), redes de área metropolitana

(MAN) y las redes de área amplia (WAN); los nuevos protocolos asociados a ellas y los conceptos modernos bajo los cuales se diseñan las redes, tales como: movilidad, escalabilidad, seguridad y convergencia.

En el capítulo 2 se realiza el análisis y definición de requerimientos. Este se ha subdividido en cuatro subcapítulos, el primero de los cuales versa sobre una descripción del Seguro de Pensiones dentro de la Seguridad Social, ello permitirá posicionar en el lector, el papel fundamental que éste cumple y el impacto que tiene en la sociedad ecuatoriana. El segundo subcapítulo muestra la cobertura geográfica del Seguro de Pensiones con las diferentes dependencias y estructura organizacional en el ámbito nacional, con lo cual se dará una visión del alcance que tendrá la red de datos que se diseña. El tercer subcapítulo realiza un análisis de la situación actual de la infraestructura informática y de telecomunicaciones, a partir de la cual, en el cuarto subcapítulo, se ubicará el conjunto de requerimientos que permitan definir los diferentes subsistemas necesarios para generar el diseño de la red.

En el capítulo 3 se realiza el diseño de la solución tanto a nivel de red LAN como de red WAN, ésta se hace tomando en cuenta las características propias de cada dependencia y los diferentes servicios que se requiere implementar. En la parte referente a red WAN, se describe la tecnología que permite la implementación de enlaces de telecomunicaciones entre las diferentes dependencias, así como también la arquitectura de red.

Las redes de datos, cumplen un papel fundamental como sistema de transporte de información; más sin embargo, estas para poder operar, requieren de un conjunto de servios de red que la automatizan y le brindan niveles de inteligencia. El análisis de servicios como DNS, DHCP, Proxy, NIS constituye el capítulo 4. Adicionalmente, se plantea un conjunto de servios de usuario tales como: correo electrónico, servidores de archivos, WEB que en las organizaciones modernas han contribuido a hacer más eficiente el almacenamiento, administración, transporte y difusión de la información.

Uno de los elementos fundamentales, en los sistemas informáticos y de telecomunicaciones modernos, es lo referente a la seguridad, por lo que en el capítulo 5, se realiza el planteamiento de la política de seguridad, a partir de un análisis de los activos de información de la Organización, y los riesgos asociados a ella, elementos estos que permiten delinear la política de Seguridad de la Organización. En ella se realiza una clasificación de la información en función de su nivel de sensibilidad; se definen las políticas de uso de software, protección de servicios y equipamiento de red, protección de equipamiento informático, políticas de acceso a sistemas, políticas para llevar adelante tareas de auditoria, políticas de respaldo y recuperación de información, administración de cambios y seguridad física de la infraestructura informática.

En el capítulo 6 se presenta un análisis de costos de los diferentes subsistemas que constituyen el proyecto; incorporando un desglose de costos de adquisición de la infraestructura, así como también los costos de operación de la misma.

En el capítulo 7 se presenta un conjunto de conclusiones, así como también se realizan las recomendaciones necesarias, con miras a presentar la mejor solución técnico – económica que de cumplimiento al objetivo planteado en el presente trabajo.

CAPITULO 1

INTRODUCCIÓN.

El desarrollo de nuevas tecnologías, provocadas por una creciente y más madura integración de la industria de la computación y de las telecomunicaciones, ha dado lugar al nacimiento de nuevos servicios que facilitan la interrelación de los seres humanos y potencian las actividades de las Organizaciones, entre los que podemos destacar los siguientes: una nueva forma de entender y dar tratamiento a la información, al surgimiento de nuevas formas de comunicación de persona a persona; al establecimiento de medios para llevar adelante relaciones comerciales y de negocios más eficaces y eficientes, con altos índices de seguridad; al acceso a información ubicada en sitios remotos cada vez a menores costos.

La información de voz, datos y video, era obtenida, procesada y transmitida separada una de otra, con bajos niveles de integración e interacción, utilizando para cada uno de ellos una red dedicada. En la actualidad esta separación se ha diluido y la idea de contar con una única red homogénea y de calidad toma fuerza en el mercado, siendo este el inicio de las comunicaciones convergentes, entorno en el que conviven voz, datos y video sin distinción.

El advenimiento de nuevos servicios de comunicación de persona a persona, basados en software, como los servicios de mensajería instantánea, correo electrónico, servicios de mensajes cortos (SMS), voz sobre IP, han sido posibles gracias a tecnologías como VPN, mecanismos de inteligencia de red, priorización de tráfico y protocolos de comunicación multimedia como el ya estandarizado protocolo de inicio de sesión (SIP), que han aportado para hacer de la convergencia una realidad operativa.

Actualmente la compra de bienes de consumo, tickets aéreos, la revisión de catálogos de productos en línea, acceso a servicios de entidades de Gobierno, etc. han sido viables por el desarrollo de tecnologías de telecomunicaciones cada

vez más confiables, con altos niveles de desempeño y bajos costos, sistemas de seguridad más robustos que han permitido garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información; sistemas informáticos cada vez más eficientes y seguros, capaces de manejar alta carga de trabajo. Todo esto, ha impulsado a la industria, comercio y sector Gobierno a proveer sus servicios a través de Internet, generando de esta manera diferentes formas de comercio electrónico, mismas que son destacadas en el siguiente cuadro:

Cuadro 1.1 Formas de comercio electrónico.

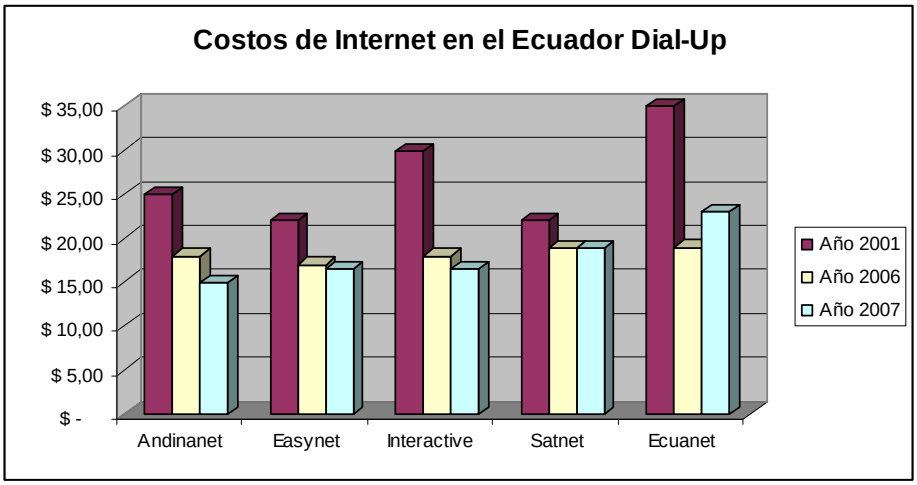
Etiqueta	Nombre completo	Ejemplo
B2C	Negocio a consumidor	Pedido de libros en línea
B2B	Negocio a negocio	La fábrica de automóviles hace un pedido de llantas al proveedor
G2C	Gobierno a consumidor	El gobierno distribuye formas fiscales electrónicamente
C2C	Consumidor a consumidor	Subasta en línea de productos de segunda mano
P2P	Igual a Igual	Compartición de archivos

Fuente: ANDREW TANENBAUM, Redes de Computadores, Cuarta Edición, p.9

En los últimos tiempos se ha experimentado una disminución de los costos de acceso a Internet, así como también un incremento de la capacidad de canal con la cual los usuarios pueden acceder al mismo, esto motivado por la implementación de tecnologías de acceso a red como xDSL y cable módem, factores estos, que han contribuido a incrementar de manera significativa el uso de Internet.

En la figura 1.1 se muestra el comportamiento de los costos de acceso a Internet en el Ecuador, utilizando líneas Dial-Up, para diferentes proveedores de servicio, durante el período comprendido entre los años 2001 al 2007.

Gráfico 1.1. Costos de Internet en el Ecuador Dial-Up.

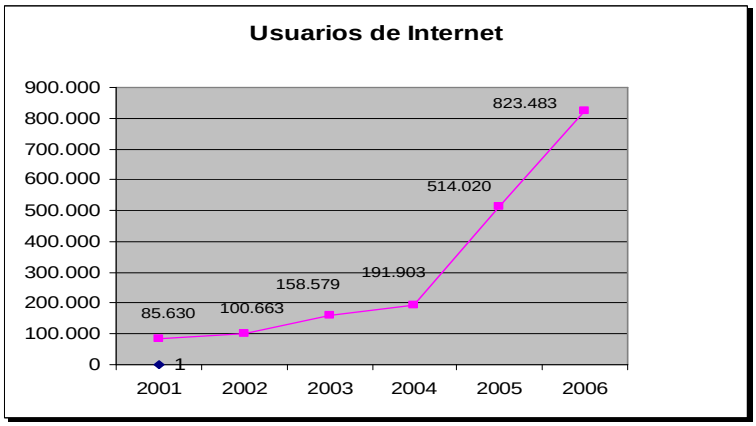


Fuente: Reporte Trimestral de Conectividad N°3 INF ODESARROLLO.EC

Es de esperar que esta tendencia continúe en los próximos años, máxime que el Consejo Nacional de Telecomunicaciones (CONATEL) ha autorizado, durante el mes de junio del año 2007, la implementación y puesta en operación de un nuevo canal de acceso a Internet, mediante el cable submarino; ello apuntando a conseguir una reducción de costos e incrementar el índice de penetración del servicio de Internet en el Ecuador.

La figura 1.2 indica el incremento de usuarios de Internet en el Ecuador, en el período comprendido entre los años 2001 y 2006.

Gráfico 1.2. Incremento de usuarios de Internet en el Ecuador.



Fuente: Reporte Trimestral de Conectividad N°3 INF ODESARROLLO.EC, basado en información Histórica de la Superintendencia de Telecomunicaciones del Ecuador

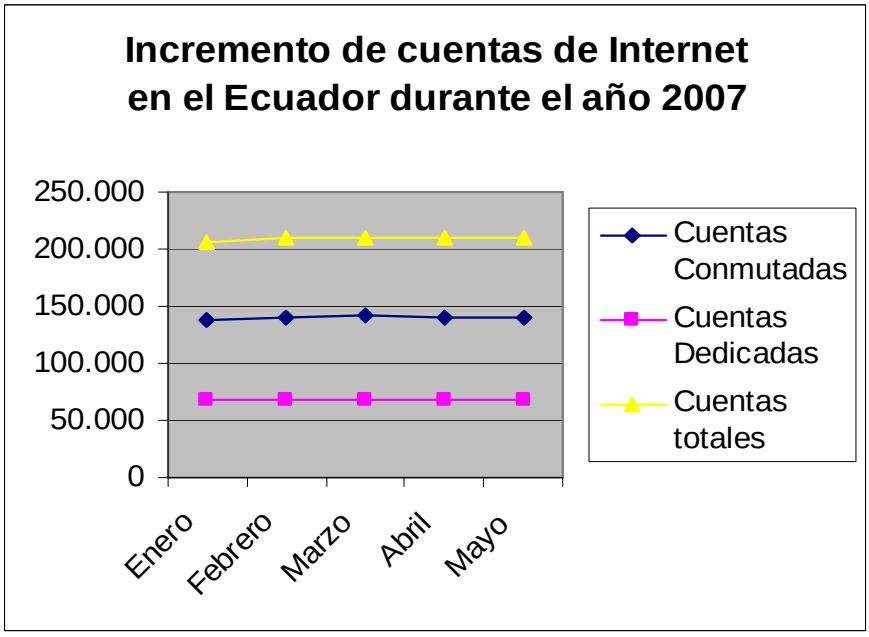
Durante el año 2007, se ha mantenido la tendencia, tanto en lo referente a cuentas como también a usuarios de Internet, estos son destacados en el cuadro 1.2 y las figuras 1.3 y 1.4.

Cuadro 1.2. Incremento de cuentas de Internet en el Ecuador durante el año 2007.

Mes	Cuentas Conmutadas	Cuentas Dedicadas	Cuentas totales	Usuarios Conmutados	Usuarios Dedicados	Usuarios totales
Enero	138.770	67.848	206.618	538.313	269.691	808.004
Febrero	140.974	68.055	209.029	563.208	269.761	832.969
Marzo	141.267	68.606	209.873	539.256	275.613	814.869
Abril	140.938	68.465	209.403	563.752	272.822	836.574
Mayo	140.926	68.866	209.792	563.704	275.470	839.174

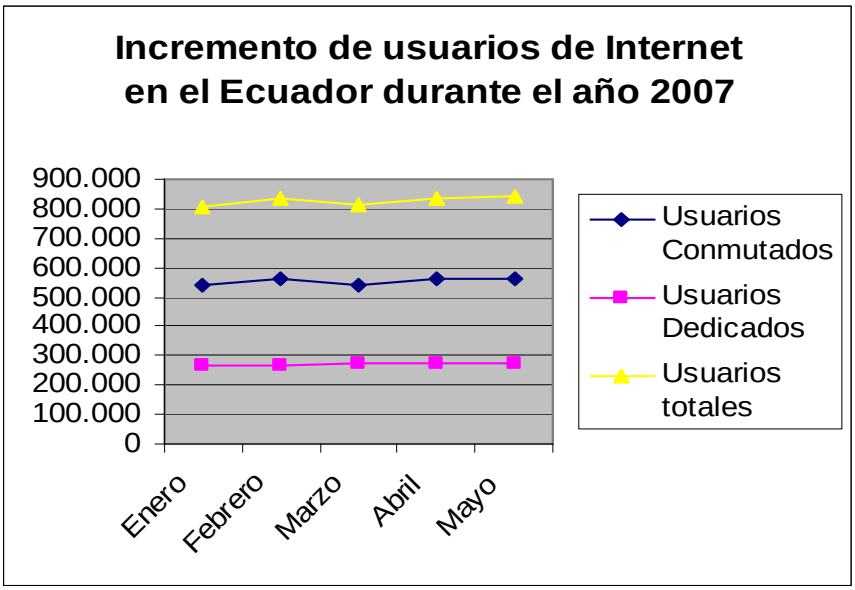
Fuente: Superintendencia de Telecomunicaciones del Ecuador.
http://www.supertel.gov.ec/telecomunicaciones/v_agregado/estadisticas/anual.htm

Gráfico 1.3. Incremento de cuentas de Internet en el Ecuador durante el año 2007.



Fuente: Superintendencia de Telecomunicaciones del Ecuador

Gráfico 1.4. Incremento de usuarios de Internet en el Ecuador durante el año 2007.



Fuente: Superintendencia de Telecomunicaciones del Ecuador

El desarrollo de Internet ha dado lugar a un floreciente sector, el de la *generación de contenidos*, cuya participación dentro del producto interno bruto (PIB) mundial en el año 2005 se estimaba en el 7% (al rededor de USD. 2.5 trillones), mayor que el segmento de telecomunicaciones, cuya participación en el mismo año era del 3.1% del PIB mundial (USD. 1.1 trillones)[1], lo cual muestra que uno de los sectores con mayor expectativa de crecimiento y de manera sostenida, es el de la generación de contenidos, sea estos multimedia, de entretenimiento, educativos, etc.

En lo que respecta a las redes de información, los últimos años han sido ricos en la generación de nuevos conceptos bajo los cuales se diseñan e implementan las redes, siendo los más relevantes los conceptos de *convergencia, movilidad, escalabilidad, alta disponibilidad, interoperabilidad y seguridad*, mismos que han permitido optimizar el uso de la infraestructura de telecomunicaciones al incorporar nuevos protocolos, que se han convertido en estándares de la industria; a la vez que se ha conseguido tener infraestructuras más confiables y robustas con altos índices de rendimiento, tiempos de respuesta y disponibilidad,

[1] Fuente: UNION INTERNACIONAL DE TELECOMUNICACIONES http://www.itu.org

1.1 CONVERGENCIA.

La nueva generación de redes, se diseñan para realizar un manejo de manera integrada de todo tipo de tráfico, voz, datos y video; ya sea de manera cableada e inalámbrica, lo cual ha permitido dar valor a los negocios e incrementar la productividad y niveles de calidad de servicio al cliente.

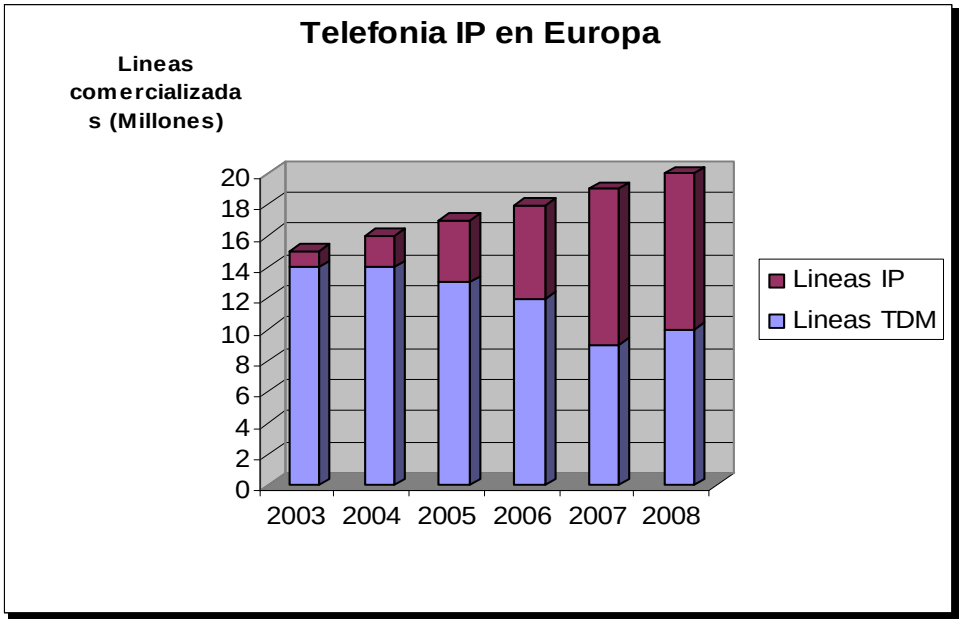
La convergencia de tráfico de distinta naturaleza, impone nuevos requisitos a los servicios ofrecidos por las redes de paquetes; se necesita garantizar una calidad de servicio (QoS) extremo a extremo (E2E). Calidad de servicio es un concepto difícil de interpretar, lo fundamental de una red que ofrece QoS, radica en que los nodos deben de tratar a cada una de las clases de tráfico de manera distinta, esto origina la necesidad de clasificar los datagramas que circulan por la red[2] (CoS).

La incorporación de protocolos de comunicaciones cada vez más avanzados, como los protocolos que permiten manejo de tráfico mediante criterios de priorización (802.1p), QoS, CoS, la llegada del protocolo de inicio de sesión (SIP), sobre el que se asientan aplicaciones avanzadas como mensajería unificada, presencia, conferencia, telefonía IP, han aportado para que la convergencia hoy sea una realidad.

En la actualidad, la telefonía IP crece en aceptación cada día. En la figura 1.5, se muestra el incremento de líneas IP comercializadas en Europa, en el último lustro, y una estimación para el año 2008. Se puede observar adicionalmente un decremento en la comercialización de líneas conmutadas TDM en el mismo período.

[2] Fuente: XVII SIMPOSIUM DE LA UNION INTERNACIONAL DE RADIO, Análisis del Problema de la Escalabilidad en Modelos de Calidad de Servicio en redes IP, Daniel Díaz A, David Fernández C.-2002

Gráfico 1.5. Uso de telefonía IP en Europa.



Fuente: Canalsys estimates, Converged Telephony Análisis, Enero 2005. Documento Perspectivas de Soluciones Convergentes Seguras 3COM Corporation

Los factores que han hecho de esta tecnología una de las de mayor éxito, se pueden puntualizar en los siguientes:

- Ahorro en infraestructura, la implementación de una única red, permite la adopción de economías de escalas, lleva consigo una considerable reducción de costos, ya que la transmisión de la información, se realiza a través de una sola infraestructura de telecomunicaciones.
- Ahorro en la facturación telefónica, obteniéndose en algunos casos ahorro de hasta un 60%, según datos del fabricante 3COM.[3]
- Reducción de los costos en la gestión de la red de voz, ya que los costos de administración de sistemas IP son más económicos que los propietarios de PBX tradicionales.[4]
- Los servicios de comunicación integrados, proporcionados por las soluciones de telefonía IP, incrementan la productividad de los empleados. La convergencia facilita la movilidad y movilidad es sinónimo de productividad.[5]

[3] Fuente: Perspectivas de soluciones seguras convergentes 3COM
[4] Fuente: Perspectivas de soluciones seguras convergentes 3COM
[5] Fuente: Perspectivas de soluciones seguras convergentes 3COM

- La gestión de una red única es más sencilla y por lo tanto menos costosa, existe menos dispositivos que administrar.
- Una red convergente, facilita la creación de entornos de trabajo distribuidos, como por ejemplo Contact Center distribuidos.[6]

Las organizaciones en la actualidad, con el fin de incrementar la productividad de sus empleados, cada vez más están haciendo uso de soluciones que permiten la implementación de presencia, tanto de voz como de datos, así como también de mensajería unificada, ellas permiten el manejo de mensajería de voz, fax mail, servicios de Find Me – Follow Me; conferencias de audio, video y datos; conferencias programadas o ad-hoc, brindando a los usuarios diferentes medios de acceso a la información de voz y datos y/o permitiendo a través de diferentes medios compartir información, la comunicación persona a persona es cada vez más interactiva, en la práctica se potencia la disponibilidad de la información como también la disponibilidad del talento humano, sin miramiento a su ubicación física ó el medio a través del cual está disponible.

1.2 MOVILIDAD.

El incremento de la disponibilidad de la información y de los sistemas, independiente de la ubicación en la que se encuentren sus usuarios y en cualquier momento, han sido posibles mediante el desarrollo de nuevas tecnologías inalámbricas que garantizan una real movilidad en un marco de alta seguridad.

La movilidad no es un servicio; para tener valor, ésta trabaja acompañando a otros servicios, permitiendo mejorar la disponibilidad de los mismos. Es necesario indicar la diferencia que existe entre *Movilidad* y *Portabilidad*, el primer caso es la capacidad de un terminal de cambiar de punto de conexión en la red, sin necesidad de reiniciar ningún tipo de conexión, en tanto que la portabilidad es la capacidad de un terminal de poder operar conectado a diferentes redes de acceso, pero siendo necesario detener y reiniciar las conexiones de red activas en

[6] Fuente: Perspectivas de soluciones seguras convergentes 3COM

el nuevo punto de conexión de la red[7], lo que infiere que la movilidad es más complejo implementar que la portabilidad.

Las ventajas que se logra al implementar movilidad en las redes modernas, pueden resumirse en las siguientes:

- Permite a un usuario acceder a servicios, independientemente del tipo de terminal que se utilice.
- Los usuarios pueden acceder a los servicios, desde cualquier red en cualquier sitio. Para ello cumplen papel importante los dispositivos utilizados por los usuarios.
- Permite utilizar diferentes dispositivos, manteniendo siempre el mismo perfil que el usuario tenga en la red.
- Permite la comunicación con otros nodos que no implementan movilidad, es decir son fijos en la red.
- Permite implementar altos niveles de seguridad, pudiendo intercambiar información de manera protegida.

1.3 ESCALABILIDAD.

Una de las grandes necesidades en las Tecnologías de la Información (TI), es la de contar con infraestructura escalable, que permita garantizar los servicios ante incrementos en la demanda de los mismos, a la vez que facilite una rápida implementación de nuevos servicios sobre infraestructura existente.

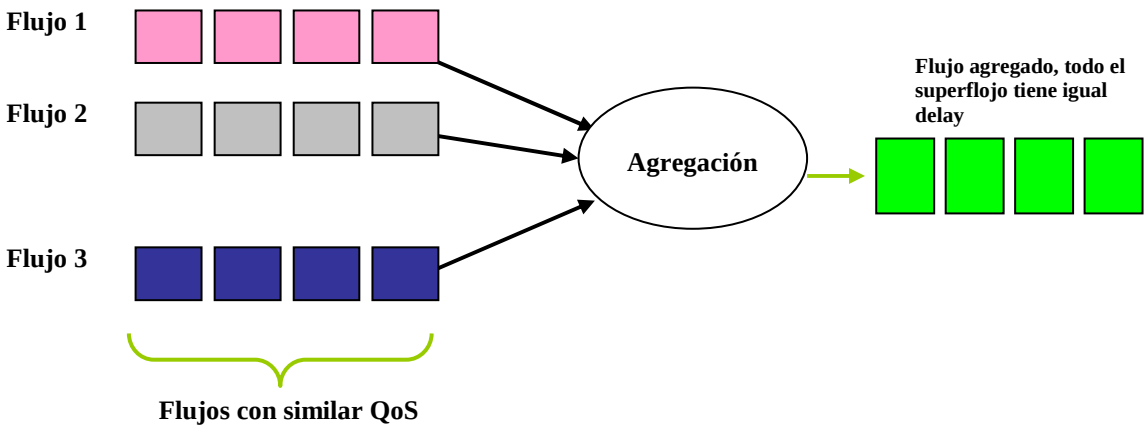
En el caso de las redes de información, esta necesidad de contar con infraestructura fácilmente escalable ha sido complejo y costoso satisfacerla, más aún con la puesta en operación de sistemas convergentes, en los que el incremento de tráfico, producto de la puesta en operación de un nuevo servicio con criterios de calidad de servicio, se traduce en un mayor consumo de recursos

[7] Fuente: Estudio de soluciones de movilidad en redes de Cuarta Generación. CARLOS JESUS BERNARDOS CANO, Marzo del 2004

de memoria y CPU en los equipos de ruteo; ellos necesitan realizar tareas de control de admisión, clasificación de paquetes, gestión de colas, etc. También se requiere hacer un uso óptimo de los enlaces e telecomunicaciones, que posibilite un transporte de información con tiempos de respuesta adecuados y que prevea un incremento de tráfico producto un mayor uso de los servicios por cada vez más usuarios.

Con la finalidad de solucionar este inconveniente se ha dado origen al concepto de *AGREGACIÓN.* Agregar significa tratar varios flujos como si fuera uno solo, los flujos con similares características de calidad de servicio son agregados[8].

Gráfico 1.6. Agregación de diferentes flujos.



Dentro de una zona en la que se ha implementado agregación, se debe cumplir los siguientes requisitos:

- No se debe conocer los flujos individuales.
- Debe mantenerse un aislamiento entre flujos. El tráfico excedente de cualquier flujo, no deberá afectar las prestaciones garantizadas ha cualquier otro flujo.
- Debe asegurarse satisfacer los requerimientos de QoS de cada uno de los flujos individuales.

[8] Fuente: XVII SIMPOSIUM DE LA UNION INTERNACIONAL DE RADIO, Análisis del Problema de la Escalabilidad en Modelos de Calidad de Servicio en redes IP, Daniel Díaz A, David Fernández C.-2002.

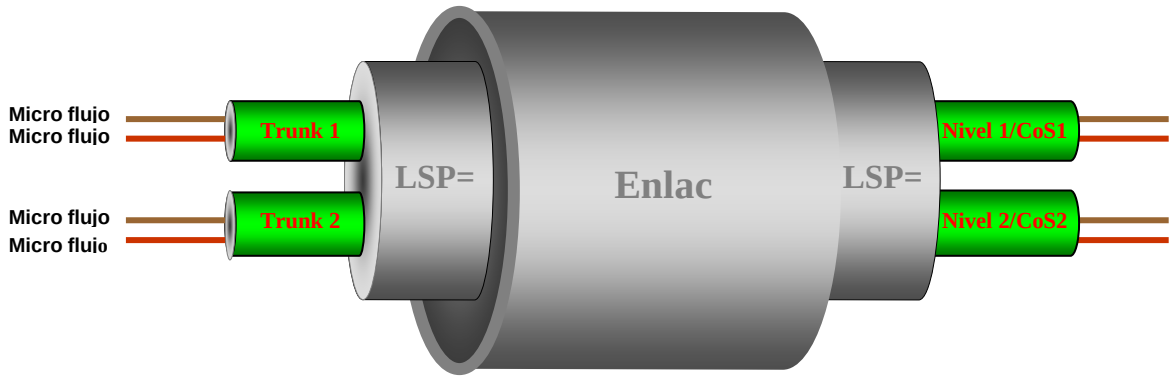
- Debe ser reversible, las reversas en las redes de acceso locales deben ser mantenidas para cada flujo individual después de cruzar la región agregada.

Gráfico 1.7. Elementos que intervienen en una zona de agregación.

Una de las tecnologías emergentes que implementan los conceptos de QoS, CoS y agregación para el transporte de información es la de *conmutación de etiquetas multiprotocolo* (MPLS). MPLS no es parte del paquete de capa de red ni tampoco de la trama de enlace de datos, es independiente de ambas capas. Esta propiedad significa que es posible construir conmutadores MPLS que pueden reenviar paquetes IP así como también celdas ATM, de esta característica proviene la parte multiprotocolo del nombre MPLS[9].

El gráfico siguiente, muestra la característica de agregación de MPLS, en el que varios micro flujos son agregados en varios trunks dentro de un enlace.

Gráfico 1.8. Agregación en un enlace MPLS.



Fuente: XVII SIMPOSIUM DE LA UNION INTERNACIONAL DE RADIO, Análisis del Problema de la Escalabilidad en Modelos de Calidad de Servicio en redes IP, Daniel Díaz A, David Fernández C.

[9] Fuente: ANDREW TANENBAUM, Redes de Computadores, Cuarta Edición, p.416

Con la finalidad de tener éxito en la implementación de agregación, es imprescindible realizar una adecuada *Ingeniería de Tráfico*, ello permitirá garantizar la calidad de servicio que demanda cada tipo de tráfico.

1.4 ALTA DISPONIBILIDAD.

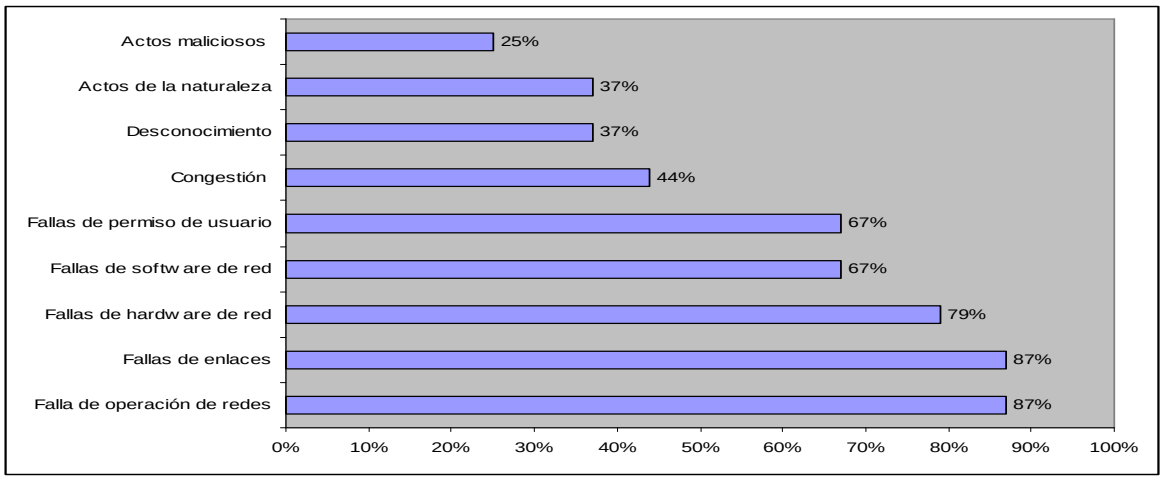
Por disponibilidad se entiende la probabilidad que un ítem (dispositivo, red o servicio) esté operacional y funcional en cualquier momento en el tiempo. Depende en gran medida del tiempo medio que el ítem sea capaz de permanecer operativo sin averías (Mean Time Between Failure MTBF) y del tiempo medio que se tarda en sustituir ó reparar en caso de avería (Mean Time To Repair MTTR)[10].

La disponibilidad de un ítem se puede obtener mediante la siguiente relación:

$$D = (MTFB - MTTR) / MTFB$$[11]

Las causas de no servicio pueden tener diversidad de orígenes, siendo las de mayor recurrencia las de origen fortuito como fallos en el hardware, suministro eléctrico, errores en el software, condiciones ambientales no adecuadas, usuarios ó administradores poco experimentados ó negligentes, etc.

Gráfico 1.9. Causas que afectan la disponibilidad.



Fuente: CISCO NETWORKERS SOLUTIONS FORUM 2006. Routed Fast Converence and High Availability

[10] Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.127

[11] Fuente: CISCO NETWORKERS SOLUTIONS FORUM 2006. Routed Fast Converence and High Availability

Sin embargo de lo anterior, también existen causas de origen deliberado, como los ataques de denegación de servicio (DoS), destrucción de información, siendo los virus la fuente más común de ataques de este tipo, cortes en los canales de telecomunicaciones, etc.

Cuando los niveles de disponibilidad garantizados, tomando como base de medición 24 horas al día durante los 365 días del año, se encuentran en un 99.999%, se dice que los sistemas son de *Alta Disponibilidad*[12], lo que corresponde a un tiempo máximo de no servicio al año de 5 minutos.

Existen algunas estrategias que en suma, permiten garantizar alta disponibilidad de la infraestructura tecnológica y de los servicios, entre las que podemos mencionar:

- Utilizar equipamiento tolerante a fallos, en los que los componentes fundamentales sean redundantes y adicionalmente montados en configuraciones de clúster.
- Los diseños de red deben permitir continuidad en la operación a pesar de fallas en enlaces ó equipos de telecomunicaciones.
- Poner en operación todo el equipamiento bajo condiciones ambientales adecuadas, de temperatura, humedad, etc.
- Implementar sistemas de suministro de energía eléctrica estabilizada redundantes y adecuadamente dimensionados, que contengan los debidos sistemas de protección, como supresores de transientes e implementar sistemas de provisión alternos de energía (generadores eléctricos).
- Las aplicaciones de los ambientes de producción, deben aprobar estrictos procesos de control de calidad, y cuya puesta en operación garantice altos niveles de desempeño y tolerancia a fallas.
- Implementar una adecuada política de seguridad con su respectiva infraestructura de seguridad informática y física.
- Implementar procesos de recuperación de sistemas ante pequeños fallos.

[12] Fuente: CISCO NETWORKERS SOLUTIONS FORUM 2006. Routed Fast Converence and High Availability

- Desarrollar planes de contingencia, que permita reaccionar y recuperarse ante fallos que comprometan la operación total de la infraestructura.
- Elemento fundamental constituye las tareas de prevención, para lo cual se requiere tener operativo un completo sistema de monitoreo, que cubra todos los elementos de la infraestructura, sistemas de generación y distribución eléctrica, equipamiento de telecomunicaciones, equipo informático, sistemas de software, etc., complementado con adecuados procesos de monitoreo llevados adelante por personal calificado. Sobre las tareas de monitoreo se asienta, en gran medida, la disponibilidad de la infraestructura y los servicios.

1.5 INTEROPERABILIDAD.

Garantizar un alto desempeño de una solución, cruza por el hecho de que cada uno de sus componentes, sea de hardware o software, opere eficientemente integrado al conjunto de componentes de la solución. Esta capacidad de los componentes de hardware y software para comunicarse con éxito, se conoce como *interoperabilidad*.

Garantizar la interoperabilidad de la infraestructura, es una tarea compleja. Una de las alternativas que podría garantizarla, es realizar una implementación con componentes que provengan de un solo fabricante; esto tendría sus ventajas, como la posibilidad de utilizar herramientas más avanzadas de administración que los fabricantes incorporan en sus soluciones, dando de esta manera valor agregado a las mismas, potenciando y/o facilitando la administración de la infraestructura, la interoperabilidad de cada uno de los componentes se vería garantizada completamente; al contar con un solo fabricante como responsable del rendimiento de la infraestructura, desaparecería la posibilidad de que un fabricante culpe a otro de los posibles fallos en la infraestructura, se reduciría los costos producto de economías de escala que se podría negociar con los fabricantes.

Sin embargo de lo expresado, en la práctica no es posible contar con un solo fabricante que cubra la gama completa de componentes de una solución. Existe diversidad de fabricantes cada uno de los cuales fabrica de manera especializada componentes en una porción de la solución, existe fabricantes de equipamiento de telecomunicaciones, fabricantes de equipo informático y fabricantes de software para la infinidad de necesidades de automatización, por lo que para garantizar la interoperabilidad del equipamiento de telecomunicaciones, informático y soluciones de software, independientemente del fabricante que lo produzca, la industria a promovido el desarrollo de estándares. Los sistemas que incorporan componentes estándares, se dice que son *sistemas de arquitectura abierta*.

En el caso de los equipos de telecomunicaciones se ha diseñado protocolos de comunicación estándar incorporados a su vez a arquitecturas de red estándar, todos ellos emitidos por Organizaciones avalizadas por la industria y en las que, en la mayoría de casos, participan también los fabricantes como miembros activos de las mismas. En esta área, el nivel de interoperabilidad que se ha conseguido entre los equipos de diferentes fabricantes es muy alto, a tal punto que se han generado certificaciones de cumplimiento de un determinado estándar, como sucede en el caso de los equipos de red inalámbricos con las certificaciones WiFi y WiMAX.

En el área informática, la adopción de estándares ha permitido su integración, de manera eficiente, con los sistemas de telecomunicaciones, dando como resultado un rápido crecimiento de los sistemas computacionales distribuidos y siendo un componente fundamental de los modernos sistemas de comunicación.

Las interfaces de programación de aplicación (API), basadas en estándares, permiten una integración abierta con terceros desarrolladores, lo que ofrece flexibilidad a los usuarios. La comprobación de la interoperabilidad, garantiza que varias soluciones puedan trabajar conjuntamente[13].

[13] Fuente: ACADEMIA DE NETWORKING DE CISCO SYSTEMS, Fundamentos de Redes Inalámbricas, Cisco Press, P.211.

Por todo lo anteriormente mencionado, la implementación de soluciones basadas en estándares, permite minimizar problemas producto de una mala interoperabilidad entre cada uno de sus componentes, garantizando a su vez altos niveles de desempeño de la solución en su conjunto.

1.6 SEGURIDAD.

Las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social. La informática y las redes se están convirtiendo en recursos omnipresentes, tal y como ha ocurrido con el suministro de agua y electricidad. Por consiguiente la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad[14].

La utilización de redes y servicios de comunicación para transportar información, ha sido cada vez más creciente, ya que ha permitido compartir de manera eficiente, efectiva y oportuna la información; sin embargo, esto lleva consigo el riesgo que personas no autorizadas puedan acceder a la misma, con la finalidad de apropiarse, modificar su contenido ó hacer un uso indebido de ella.

El almacenamiento de información corporativa en centros de datos, a fin de poder ser utilizada por sistemas gerenciales ó sistemas que permiten la prestación de servicios a usuarios internos y externos, es una práctica que desde el inicio de los sistemas informáticos se ha realizado, pero que en la actualidad se ha visto afectada al convertirse en objetivo de gente maliciosa.

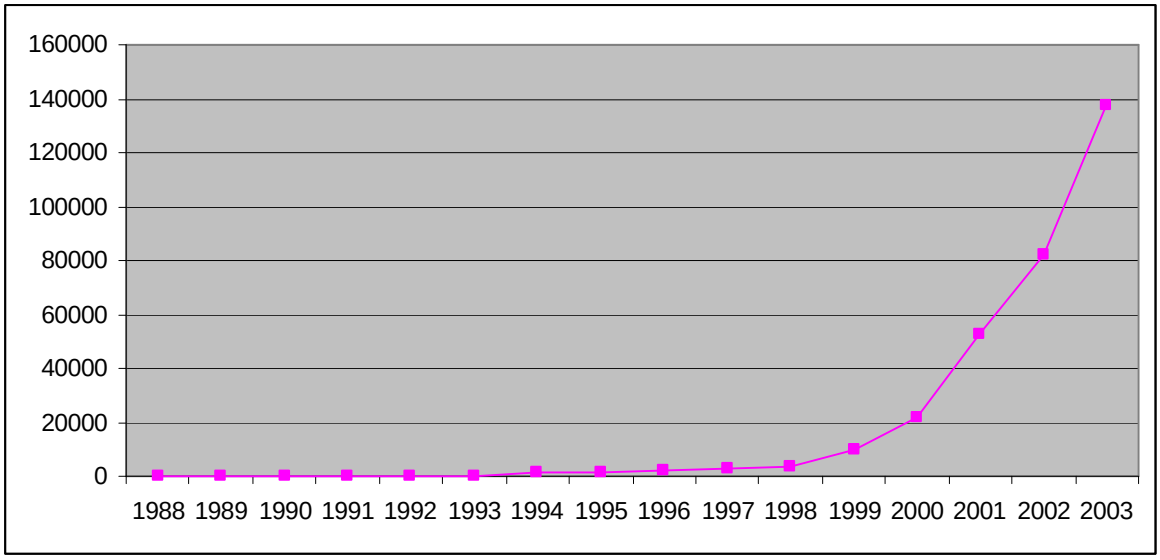
El acceso a sistemas corporativos por parte de usuarios no autorizados, es otro de los tipos de incidentes que se presentan en las Organizaciones, lo que ha llevado a poner mucho énfasis en el desarrollo de aplicaciones atendiendo criterios de seguridad, así como también a la implementación de complejos

[14] Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.2

sistemas de autenticación, autorización y auditoria que permitan mitigar los riesgos potenciales.

Estudios sobre seguridad informática muestran que durante el año 2003 se han producido más de 100.000 incidentes de seguridad y se ha reportado más de 3.000 vulnerabilidades. En el año de 1988 se registraron 6 incidentes y 171 vulnerabilidades[15], lo que muestra que la necesidad de implementar sistemas de seguridad, cada vez es más imprescindible.

Gráfico 1.10. Evolución de los incidentes de seguridad.



Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.21

El estudio sobre seguridad y crimen informático del Computer Security Institute, indica que se estiman pérdidas de los sistemas analizados en más de 141 millones de dólares por problemas de seguridad[16]. Esta cantidad nada despreciable de dinero, muestra que el implementar oportunamente seguridad en las redes y sistemas de información, evitará perdidas cuantiosas a las Organizaciones, siempre será menos costoso invertir en seguridad que las pérdidas producidas por un incidente.

[15] Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.20

[16] Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.20

Las inversiones que se realizan en seguridad, deben también corresponderse con la valoración que se tiene de los activos de información, por lo que, antes de realizar estos procesos de inversión, es necesario realizar un análisis de riesgos y su respectiva valoración, ello permitirá justificar adecuadamente las inversiones en seguridad.

La implementación de seguridad tiene como objetivo garantizar la privacidad, integridad, disponibilidad y autenticidad de la información y de los sistemas, entendiéndose cada uno de éstos términos de acuerdo a las siguientes definiciones:

Privacidad: sólo entidades autorizadas puedan tener acceso a la información. Este tipo de acceso incluye la impresión, visualización y otras formas de revelado de la información[17].

Integridad: Consiste en garantizar que los datos y recursos, no han sido alterados, permanecen completos y son fiables. La modificación no autorizada de los datos, puede ocurrir durante su almacenamiento, transporte o procesamiento[18].

Disponibilidad: Consiste en garantizar que los datos y sistemas permanecen accesibles sin interrupciones cuando y donde se los necesita[19].

Autenticidad: Un computador ó servicio debe ser capaz de verificar la identidad de un usuario[20].

El cumplimiento de estos objetivos, es posible mediante la incorporación de soluciones de seguridad como firewalls, sistemas de prevención de intrusos (IPS), sistemas de autenticación, autorización y auditoría (AAA) de usuarios, algoritmos

[17] Fuente: WILLIAM STALLINGS, Comunicaciones y Redes de Computadores, Séptima Edición, Prentice Hall, p.725.
[18] Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.117.
[19] Fuente: GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, p.122
[20] Fuente: WILLIAM STALLINGS, Comunicaciones y Redes de Computadores, Séptima Edición, Prentice Hall, p.725

de cifrado de la información, listas de acceso (ACL) mismos que actúan para mantener la privacidad de la información; algoritmos de hashing para verificar la integridad de la información (MD5, SHA); sistemas para evitar ataques de denegación de servicio (DoS) y firmas digitales que permiten garantiza la autenticidad de documentos y mensajes.

Todo este conjunto de soluciones, actuando en complemento con una adecuada política de seguridad, permiten proteger los activos de información, así como también garantiza la continuidad de la operación de la infraestructura tecnológica que da soporte a las diferentes aplicaciones, sistemas y servicios de una Organización.

En lo referente al equipamiento requerido para implementar las redes modernas, este también ha tenido grandes desarrollos. En la actualidad este equipamiento está diseñado para garantizar la disponibilidad de las redes, incorporando estándares de la industria que le permiten tolerancia a fallos como por ejemplo:

- Agregación de enlaces, estándar IEEE 802.1ad, LACP.
- Protocolo Rapad Spanning Tree, estándar IEEE 802.1w, RSTP.
- Ruteo redundante, Protocolo de ruteo redundante virtual (VRRP).

Con la finalidad de asegurar que el tráfico prioritario sea quien se transmita en primer lugar, se ha desarrollada nuevos protocolos de priorización de tráfico, como los siguientes:

- Priorización de tráfico estándar 802.1p
- Redirección de puertos de capa 4.
- Limitación de capacidad de canal.
- Bloqueo de aplicaciones y protocolos indebidos.
- Soporte de tráfico multicast (voz, video, colaboración).

Dado que las aplicaciones hacen mayor demanda de la red, también se ha incrementado la capacidad de transmisión a 10Gbps por puerto de comunicación.

En resumen, todo lo expresado en el presente capítulo, nos muestra que los sistemas de información y telecomunicaciones, están marcados por un vertiginoso desarrollo científico tecnológico, que han potenciado la productividad de las organizaciones y que inciden directamente en la sociedad, convirtiéndose en un motor del cambio.

CAPITULO 2

ANÁLISIS Y DEFINICIÓN DE REQUERIMIENTOS.

2.1 EL SISTEMA DE PENSIONES DENTRO DE LA SEGURIDAD SOCIAL.

El Instituto Ecuatoriano de Seguridad Social (IESS) es una entidad, cuya organización y funcionamiento se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia. Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del Sistema Nacional de Seguridad Social.

El IESS tiene la misión de proteger a la población urbana y rural, con relación de dependencia laboral o sin ella, contra las contingencias de enfermedad, maternidad, riesgos del trabajo, discapacidad, cesantía, invalidez, vejez y muerte, en los términos que establece la Ley de Seguridad Social vigente[21].

Para el cumplimiento de su misión, el IESS se encuentra estructurado por cuatro seguros, a saber: Seguro General de Salud Individual Familiar (SGSIF), Seguro General de Riesgos de Trabajo (SGRT), Seguro Social Campesino (SSC), Seguro General de Pensiones (SGP).

En el presente acápite nos referiremos al Seguro General de Pensiones, quien dentro de sus competencias y responsabilidades está la de proteger a la población asegurada contra las contingencias de vejez, invalidez y muerte, así como de la transferencia de la aportación personal correspondiente a la cuenta de ahorro individual obligatorio de cada afiliado, de la aplicación del régimen de

[21] RESOLUCIÓN CD-021, Consejo Directivo IESS, Art. 2.

jubilación por solidaridad intergeneracional y de la administración del subsidio para funerales[22].

De lo anteriormente indicado, se deduce que el Seguro de Pensiones, tiene una función fundamental dentro de la Seguridad Social, cuya labor trasciende al contexto nacional, ya que es el encargado de brindar condiciones de vida dignas al adulto mayor, y a los ecuatorianos que por motivo de alguna incapacidad no pueden insertarse al mercado laboral.

Según estadísticas publicadas por el IESS a diciembre del año 2003[23], se registra 241.018 pensionistas del Seguro General, los jubilados por invalidez ascienden a 15.269, los jubilados por vejez 139. 309 y los beneficiarios de montepío llegan a 86.080.

En complemento a la pensión mensual que reciben los beneficiarios, se otorga también asistencia médica integral, odontológica y farmacéutica a través de las distintas unidades y centros médicos del IESS ó compensación de gastos médicos en caso de atención en centros médicos ajenos al IESS.

Todos los servicios otorgados por el Seguro de Pensiones, son de alto impacto social, por lo que es de importancia superlativa, garantizar la continuidad de su operación a fin de cumplir su misión con altos índices de satisfacción del cliente.

2.2 COBERTURA GEOGRÁFICA DEL SEGURO DE PENSIONES.

Según el artículo 37 de la resolución CD-021 del Consejo Directivo del IESS, el Seguro de Pensiones está constituido por la Dirección del Seguro de Pensiones, la Subdirección de Pensiones, la Subdirección de Contabilidad y Control Presupuestario y las Unidades Provinciales de Pensiones, por lo que de acuerdo a la ley el Seguro de Pensiones debe tener presencia en el ámbito nacional. Sin embargo, en la actualidad el Seguro de Pensiones tiene aperturadas nueve oficinas en las ciudades de Ibarra, Quito, Ambato, Riobamba, Cuenca, Loja,

[22] RESOLUCIÓN CD-021, Consejo Directivo IESS, Art. 35.
[23] IESS, Página web, http://www.iess.gov.ec

Portoviejo, Guayaquil y Machala, correspondientes a los nueve regionales que anteriormente constituían el IESS.

El número de funcionarios que actualmente desempeñan sus funciones, en cada una de las oficinas descritas anteriormente, se indican en el siguiente cuadro:

Cuadro 2.1. Distributivo de funcionarios del Seguro de Pensiones.

Dependencia	Número de Funcionarios	Ubicación
Dirección de Pensiones	8	Edf. Riesgos del Trabajo piso 1
Subdirección de Contabilidad y Control Presupuestario	5	Edf. Riesgos del Trabajo piso 4
Subdirección de Pensiones Azuay	29	Edf. Dirección Provincial piso 5
Subdirección de Pensiones Pichincha	93	Edf. Matriz piso 7 y 5
Subdirección de Pensiones Guayas	65	Edf. Dirección Provincial piso 7 y 3
Unidad Provincial Imbabura	11	Edf. Seguro de Pensiones piso 1
Unidad Provincial Tungurahua	10	Edf. Dirección Provincial piso 2
Unidad Provincial Chimborazo	13	Casa Calero PB, piso 1 y 2
Unidad Provincial Loja	14	Edf. Dirección Provincial piso 3
Unidad Provincial Manabí	19	Edf. Dirección Provincial piso 3
Unidad Provincial el Oro	13	Edf. Dirección Provincial piso 2

Fuente: Dirección de Pensiones IESS.

2.3 ANÁLISIS DE LA SITUACIÓN ACTUAL.

Con la finalidad de obtener información acerca de la situación actual, se utilizó como metodología la *entrevista,* la cual se desarrolló con el Responsable informático del Seguro de Pensiones y el Coordinador de Gestión Tecnológica del IESS, buscando satisfacer las siguientes inquietudes:

Cuadro 2.2. Cuestionario para realizar el levantamiento de información.

LEVANTAMIENTO DE INFORMACIÓN DE SITUACIÓN ACTUAL **INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL** **SEGURO DE PENSIONES**
SECTOR: Gestión Tecnológica (GT) **FUENTE:** Coordinador de GT, Coordinador Informático del Seguro de Pensiones.
1. ¿Qué aplicaciones informáticas tiene en producción el Seguro de Pensiones? **2.** ¿Las aplicaciones informáticas sobre qué tecnología fueron desarrolladas y operan? **3.** ¿El desarrollo de las aplicaciones, responde a alguna metodología de desarrollo de software? **4.** ¿Existe una política de gestión de los datos que permita garantizar la confiabilidad, integridad y disponibilidad de los mismos? **5.** ¿Qué tipo de tecnología de telecomunicaciones se utiliza actualmente y cuál es su cobertura? **6.** ¿Existe una política de gestión de los recursos de telecomunicaciones? **7.** ¿Qué tipo de equipamiento informático posee actualmente el Seguro de Pensiones? **8.** ¿Existe aplicaciones informáticas gerenciales, de manejo documental o de otro tipo, que faciliten los procesos administrativos del Seguro de Pensiones? **9.** ¿Existe políticas y procesos de mantenimiento, tanto para el hardware como para el software? **10.** ¿El personal informático que gestiona la infraestructura en su conjunto, es personal calificado y en número suficiente?

Por la información obtenida en las entrevistas, podemos decir lo siguiente:

En la década de los años 80, el Instituto Ecuatoriano de Seguridad Social, puso en operación su sistema informático basado en dos equipos Mainframe IBM 390,

uno de los cuales opera en la ciudad de Guayaquil y el restante en la ciudad de Quito, cada uno de ellos atendiendo a usuarios de las distintas provincias, de acuerdo a lo que se indica en el siguiente cuadro:

Cuadro 2.3. Zonas de cobertura de los Mainframe IBM 390.

Mainframe IBM 390	Provincias a las que da servicio		
	Región Sierra	**Región Costa**	**Región Oriental**
Mainframe IBM 390 de la ciudad de Quito	Carchi Imbabura Pichincha Cotopaxi Tungurahua Bolívar Cañar Azuay	Esmeraldas	Sucumbíos Napo Orellana Pastaza
Mainframe IBM 390 de la ciudad de Guayaquil	Loja	Guayas Los Ríos El Oro Manabí Galápagos	Morona Santiago Zamora Chinchipe

Los sistemas mainframe, alojan las aplicaciones informáticas de cada uno de los Seguros del IESS, dentro de las que se encuentra las aplicaciones de Jubilación, Cesantía, Supervivencia, Fondo Mortuorio, Reliquidación de jubilación de vejez e invalidez, Mejora Civil, Viudez y Orfandad; propias de la operación del Seguro de Pensiones.

2.3.1 SOBRE LAS APLICACIONES.

El desarrollo de aplicaciones se basa en tecnología informática de la década de los 70 y 80, utilizando lenguaje de programación PL1; sin métodos ni técnicas formales de Ingeniería de Software. No existe una adecuada integración entre

cada uno de sus módulos. Los procesos de mantenimiento son costosos y el software generado por estos procesos, no atraviesa un proceso de control de calidad.

Existe información de derechohabientes repetitiva y poco confiable; ya que no existe un repositorio único de datos, cada módulo mantiene su propia información, por lo que es necesario registrar la información referida en cada módulo.

La información existente no es confiable, la modificación de los datos puede ser realizada por operadores o usuarios del sistema, sin acogerse a una política establecida para el efecto.

Existen registros que no tienen relación con ningún derechohabiente, por lo que no existe certeza de contar con la información completa de cada uno de ellos.

Lo anterior, impacta directamente en la prestación de servicios, ya que al realizar los procesos de jubilación, se requiere acudir a métodos manuales y archivos físicos con el fin de completar la información, lo que hace que este proceso no sea eficaz, eficiente y oportuno.

2.3.2 SOBRE EL HARDWARE

La ausencia de una gestión tecnológica apropiada, ha dado como resultado una marcada obsolescencia tecnológica dentro del Seguro de Pensiones, lo cual dificulta la implementación de nuevos sistemas que potencien adecuados procesos administrativos y de servicio al cliente.

La operación del Seguro de Pensiones, se basa en los sistemas del mainframe 390; para acceso a las aplicaciones informáticas desde cada una de las dependencias, los usuarios cuentan con terminales de host, propios de la tecnología mainframe, cuya distribución se encuentra en el cuadro 2.4.

Como equipos para impresión se utiliza impresoras de host, estas permiten la impresión únicamente desde el sistema host.

Algunas áreas cuentan con computadores personales y sistemas de impresión, pero que no se encuentran integrados a través de una red de datos, sino que prestan servicio únicamente a los funcionarios que las operan.

Los computadores personales e impresoras no son de última generación, teniendo un tiempo de operación en promedio de 4 años. Este equipamiento, no ha sido adquirido ni puesto en operación respondiendo a un plan de equipamiento, es producto de iniciativas aisladas de funcionarios, que por necesidad de sus actividades diarias han solicitado a los niveles de Dirección su adquisición.

En el siguiente cuadro se indica la distribución, cantidad y tipo de equipos que actualmente operan en el Seguro de Pensiones.

Cuadro 2.4. Detalle de equipamiento por Dependencia.

Dependencia	Terminal de Host	Impresora de Host	Computador Personal	Impresora Láser	Impresora Matricial
Dirección de Pensiones	3		2	1	
Subdirección de Contabilidad y Control Presupuestario	2	1	5	1	
Subdirección de Pensiones Azuay	15	3	2	1	
Subdirección de Pensiones Pichincha	54	12	5	1	
Subdirección de Pensiones Guayas	37	7	6	1	

Dependencia	Terminal de Host	Impresora de Host	Computador Personal	Impresora Láser	Impresora Matricial
Unidad Provincial Imbabura	8	2	2		3
Unidad Provincial Tungurahua	7	2	2		3
Unidad Provincial Chimborazo	8	2	4		1
Unidad Provincial Loja	8	2	3	1	2
Unidad Provincial Manabí	11	2	2	1	2
Unidad Provincial el Oro	7	1	2	1	1
TOTAL	**160**	**34**	**35**	**8**	**12**

Fuente: Coordinación de informática del Seguro de Pensiones IESS.

2.3.3 REDES DE TELEPROCESO.

La red de telecomunicaciones, que utiliza el Seguro de Pensiones, pertenece a las redes de conmutación de circuitos, cuyos enlaces se realizan a través de la red telefónica pública conmutada (PSTN) de los proveedores Andinatel SA., Pacifictel SA. y Etapa, cada uno de estos dando servicio en sus zonas de cobertura. Los problemas derivados de un mal funcionamiento de los equipos de telecomunicaciones, tienen al momento tiempos altos de restauración, ya que dentro de la Institución, no se cuenta con un área suficientemente estructurada que permita atender estas contingencias, lo que dificulta la prestación de servicios con altos índices de disponibilidad, incidiendo directamente en una mala atención al público por falta de información oportuna.

2.3.4 POLÍTICAS DE MANTENIMIENTO.

Existe ausencia de políticas de mantenimiento, tanto en lo referente al software, hardware y telecomunicaciones.

En el caso de las aplicaciones, no se tiene una política de control de calidad del producto generado por tareas de mantenimiento, existe una gran dependencia de las aplicaciones con el programador asignado a ella, no existe una política ni los medios para llevar adelante un adecuado manejo de versiones, ni tampoco existe procedimientos para manejo de cambios. Cada programador desarrolla, prueba y pone en producción las modificaciones realizadas a los módulos de su competencia.

Existe un área encargada del mantenimiento del hardware, pero tiene limitaciones de orden técnico, de presupuesto y operativo, por lo que los procesos de mantenimiento tanto preventivo como correctivo de la infraestructura son casi nulos.

El mantenimiento de la infraestructura de telecomunicaciones, se lleva adelante a través de terceros, cuyos servicios son prestados cada ocasión que se presenta un problema.

El equipamiento que constituye el núcleo central, no cuenta con contratos de mantenimiento ni soporte para provisión de partes y asesoría técnica, lo que constituye un grave riesgo para la normal operación del Seguro de Pensiones.

2.3.5 RECURSO HUMANO INFORMÁTICO.

El equipo de trabajo que constituye el área informática del Seguro de Pensiones, no está lo suficientemente capacitado, el nivel de formación en su gran mayoría es de nivel de tecnólogo, quienes adicionalmente no poseen instrucción certificada por el fabricante del sistema mainframe IBM 390, que los faculte a realizar una adecuada gestión tecnológica.

Por lo mencionado en los acápites anteriores, podemos concluir que la inexistencia de una infraestructura tecnológica robusta y fiable, con altos índices de rendimiento y disponibilidad, inexistencia de información confiable que permita una prestación de servicio al cliente adecuada y que coadyuve a una toma de decisiones eficiente, eficaz y oportuna y la ausencia de una gestión tecnológica que oriente la tecnología hacia satisfacer las necesidades de la Organización, ponen en grave riesgo la prestación de los servicios que el Seguro de Pensiones da a sus pensionistas.

2.4 DEFINICIÓN DE REQUERIMIENTOS.

Con la finalidad de llevar adelante un proceso de modernización; que le permita al Seguro de Pensiones constituirse en una aseguradora moderna, con altos índices de satisfacción de los clientes internos y externos, se desarrolló el Plan Estratégico, siendo parte integrante de él, el Plan Estratégico de Informática.

El presente trabajo, recoge las directrices dictadas en el Plan Estratégico de Informática, como uno de los insumos de requerimientos. Es el marco de referencia a partir del cual se diseñará las redes y servicios informáticos del Seguro de Pensiones.

Para la determinación del número de equipos que se requiere por dependencia, se realizó una encuesta al coordinador de informática del Seguro de Pensiones, a partir de la cual se diseñará las redes de área local y dimensionará los equipos de red e informáticos.

2.4.1 APLICACIONES INFORMÁTICAS.

A fin de contar con un sistema que responda a los requerimientos del plan estratégico, el Seguro de Pensiones contrató el desarrollo de la aplicación de Pensiones. Esta está constituida por los módulos de Jubilación de vejez,

Jubilación por invalidez, Mejora Civil, Reliquidación de jubilación de vejez e invalidez, Supervivencia y Fondo Mortuorio.

Se requiere el diseño de la infraestructura necesaria para que la referida aplicación pueda ser puesta en operación, considerando que para el efecto, la aplicación prestará servicio con los siguientes criterios:

1) Todos los módulos de usuario deben tener acceso tanto desde Internet como desde cada una de las dependencias del Seguro de Pensiones en un horario de 24 horas al día, los 7 días a la semana.
2) Los módulos que son de funcionarios liquidadores, deben ser accedidos exclusivamente desde las dependencias del Seguro de Pensiones, en un horario de 16 horas al día los 5 días de la semana.

2.4.2 SERVICIOS INFORMÁTICOS.

Se requiere la implementación de un conjunto de servicios informáticos que apoyen la automatización de los procesos y flujos administrativos, así como la administración de la información a través de herramientas que faciliten y garanticen agilidad y seguridad en su manipulación y acceso.

Los servicios informáticos deben tener una estrategia de operación diaria enmarcada en el servicio al usuario.

Los principales sistemas y servicios informáticos son:

1) Servicio de acceso a Internet
2) Servicio de Intranet Institucional.
3) Servicio de correo electrónico.
4) Servicios de red que permitan una operación inteligente de las redes (DNS, DHCP, PROXY, NFS).

2.4.3 EQUIPO INFORMÁTICO.

Los servidores de aplicaciones y base de datos deben tener las siguientes características:

1) Basados en tecnología RISC, diseñados para operar con alta carga de trabajo y en condiciones de alta disponibilidad.
2) Alta velocidad de respuesta.
3) Capacidad de operación en configuración de cluster.
4) Capacidad Hot Swap en discos duros y fuentes de alimentación.
5) El sistema de almacenamiento será centralizado, utilizando para este efecto sistema de almacenamiento en red (SAN)
6) El sistema operativo será Unix: Solaris, AIX, Linux, etc.

Los servidores Web y de servicios de red deben tener las siguientes características:

1) Basados en tecnología CISC, diseñados para operar con alta carga de trabajo y en condiciones de alta disponibilidad.
2) Alta rendimiento.
3) Capacidad de operación en configuración de cluster.
4) Capacidad Hot Swap en discos duros y fuentes de alimentación.
5) El sistema operativo será Unix: Solaris, AIX, Linux, etc.

El Sistema Operativo que se instalará en las PCs, debe cumplir con las características de ser seguro, estable, amigable al usuario y que esté regido por licencias GPL del Software Libre. Se debe mantener estandarización en todo el parque informático del Seguro de Pensiones.

En lo relacionado al sistema de impresión, éste debe tener impresoras de alto rendimiento tipo láser y diseñadas para trabajo en red, considerando para su dimensionamiento el número de usuarios que soportará y su carga de trabajo.

Para determinar el equipo informático requerido en cada una de las dependencias del Seguro de Pensiones, se procedió a realizar una encuesta, misma que se realizó con el responsable de informática. Los resultados se indican en el siguiente cuadro:

Cuadro 2.5. Requerimiento de equipo informático por dependencia.

LEVANTAMIENTO DE INFORMACIÓN DEL SISTEMA INFORMÁTICO INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL SEGURO DE PENSIONES				
Dependencia	**Computador Personal**	**Impresora Láser Tipo 1**	**Impresora Láser Tipo 2**	**Servidor de Red**
Dirección de Pensiones	8	2		1
Subdirección de Contabilidad y Control Presupuestario	5		1	
Subdirección de Pensiones Azuay	20	2	2	1
Subdirección de Pensiones Pichincha	69	10	3	1
Subdirección de Pensiones Guayas	52	6	3	1
Unidad Provincial Imbabura	13	3		1
Unidad Provincial Tungurahua	12	3		1
Unidad Provincial Chimborazo	13	3		1
Unidad Provincial Loja	13	3		1
Unidad Provincial Manabí	16	4		1
Unidad Provincial el Oro	12	3		1
TOTALES	**233**	**39**	**9**	**10**

Fuente: Coordinación de informática del Seguro de Pensiones IESS.

2.4.4 EQUIPAMIENTO DE RED LAN Y WAN.

1) La institución se guía por el principio de mantener una plataforma estandarizada de hardware y software, que facilite su administración y operación, eliminando costos generados por una diversidad tecnológica
2) Se requiere el diseño de una red de telecomunicaciones con criterios de convergencia, escalabilidad, interoperabilidad y alta disponibilidad a nivel

nacional; por lo que la infraestructura debe soportar voz, datos, video, mediante la incorporación de protocolos de calidad de servicio, priorización y clasificación de paquetes.

3) El núcleo de la plataforma LAN debe estar integrado por equipos diseñados para realizar tareas bajo el principio de alta disponibilidad

2.4.5 CABLEADO ESTRUCTURADO.

Se requiere las especificaciones técnicas del sistema de cableado estructurado, considerando que éste debe permitir tener altas tasas de transferencia de datos, ya que soportará los servicios convergentes que pondrá en operación el Seguro de Pensiones. Las características principales son:

1) Es sistema de cableado estructurado debe ser categoría 6.
2) Debe cumplir con los estándares EIA/TIA 568, EIA/TIA 569, EIA/TIA 606, EIA/TIA 607, TSB-67.
3) El bakbone de datos, en los edificios que se requiera, debe ser de fibra óptica.

El levantamiento de información se realizó mediante una encuesta, cuyos resultados se muestran en el siguiente cuadro:

Cuadro 2.6. Requerimiento de puntos de red por dependencia.

LEVANTAMIENTO DE INFORMACIÓN CABLEADO ESTRUCTURADO INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL SEGURO DE PENSIONES		
Dependencia	**N°. de Puntos de Red**	**Distribución de puntos**
Dirección de Pensiones	11	Edf. Riesgos del Trabajo Piso 1 11 puntos de red Piso 4 7 puntos de red
Subdirección de Contabilidad y Control Presupuestario	7	
Subdirección de Pensiones Azuay	25	Edf. Dirección Provincial Piso 5 25 puntos de red
Subdirección de Pensiones Pichincha	83	Edf. Matriz Piso 7 45 puntos de red Piso 5 18 puntos de red Planta Baja 20 puntos de red

LEVANTAMIENTO DE INFORMACIÓN CABLEADO ESTRUCTURADO INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL SEGURO DE PENSIONES		
Dependencia	**N°. de Puntos de Red**	**Distribución de puntos**
Subdirección de Pensiones Guayas	62	Edf. Dirección Provincial Piso 7 22 puntos de red Piso 3 20 puntos de red Planta Baja 20 puntos de red
Unidad Provincial Imbabura	17	Edf. Seguro de Pensiones Piso 1 17 puntos de red
Unidad Provincial Tungurahua	16	Edf. Dirección Provincial Piso 2 16 puntos de red
Unidad Provincial Chimborazo	17	Casa Calero PB 5 puntos de red Piso 1 7 puntos de red Piso 2 5 puntos de red
Unidad Provincial Loja	17	Edf. Dirección Provincial Piso 3 17 puntos de red
Unidad Provincial Manabí	21	Edf. Dirección Provincial Piso 3 21 puntos de red
Unidad Provincial el Oro	16	Edf. Dirección Provincial Piso 2 16 puntos de red
TOTAL	**292**	

Fuente: Coordinación de informática del Seguro de Pensiones IESS.

Es necesario indicar, que como parte del mejoramiento del servicio al cliente, el Seguro de Pensiones implementará centros de Servicio en cada una de las unidades provinciales, los cuales también demandan infraestructura de cableado estructurado.

En ANEXO 1 se muestra plantilla utilizada para levantamiento de información.

2.4.6 RED DE ENERGÍA ELÉCTRICA Y SISTEMA DE RESPALDO (UPS).

Con la finalidad de contar con un sistema de suministro de energía eléctrica confiable y seguro, se requiere las especificaciones técnicas de las redes de energía eléctrica las cuales deben incorporar los sistemas de protección necesarios que garanticen una adecuada operación de la red.

Adicionalmente se requiere las especificaciones técnicas de los sistemas de respaldo de energía eléctrica UPS, los cuales deben permitir su administración a través de protocolo SNMP.

Para el levantamiento de información se realizó una encuesta, cuyos resultados se muestran en el cuado siguiente:

Cuadro 2.7. Distribución de puntos eléctricos, normales y estabilizados.

Dirección de Pensiones y Subdirección de Contabilidad		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
1	2	9
4	1	6
TOTAL	**3**	**15**

Subdirección de Pensiones Azuay		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
5	4	21
TOTAL	**4**	**21**

Subdirección de Pensiones Pichincha		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
PB	2	18
5	2	16
7	9	36
TOTAL	**13**	**70**

Subdirección de Pensiones Guayas		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
PB	2	18
3	3	17
7	4	18
TOTAL	**9**	**53**

Unidad Provincial de Imbabura

Piso	Ptos Eléctricos Normales	Pto. Eléctrico Estabilizado
1	3	14
TOTAL	**3**	**14**

Unidad Provincial de Tungurahua		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
2	3	13
TOTAL	**3**	**13**

Unidad Provincial de Chimborazo		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
PB	1	4
1	1	6
2	1	4
TOTAL	**3**	**14**

Unidad Provincial de Loja		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
3	3	14
TOTAL	**3**	**14**

Unidad Provincial de Manabí		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
3	4	17
TOTAL	**4**	**17**

Unidad Provincial del Oro		
Piso	**Ptos Eléctricos Normales**	**Pto. Eléctrico Estabilizado**
2	3	13
TOTAL	**3**	**13**

En ANEXO 1 se muestra plantilla utilizada para levantamiento de información.

CAPITULO 3

DISEÑO DE LA SOLUCIÓN

El Seguro de Pensiones, en el marco del proceso de Modernización definió como uno de los ejes fundamentales de éxito, la modernización de la Infraestructura Tecnológica que da soporte a su operación. Es en esta consideración y basados en los avances tecnológicos del momento; que se estableció un *marco conceptual* que define y orienta la nueva tecnología, la que alineada a las necesidades de la organización, potenciará y apoyará los procesos internos para una adecuada toma de decisiones y mejoramiento de los servicios al usuario.

El marco conceptual establece la incorporación de los conceptos de alta disponibilidad, interoperabilidad, escalabilidad, movilidad, convergencia y seguridad como elementos mandatarios que deben ser cumplidos tanto por el equipamiento y tecnología empleados, así como también por los diseños y políticas con los que se implementan y operan los mismos, cobijados todos estos por la necesidad de contar con infraestructura de arquitectura abierta.

En base a lo anteriormente señalado y dando cumplimiento a lo definido como requerimientos en el capítulo 2.4, se plantea la siguiente solución tanto para red LAN como para red WAN.

3.1 DISEÑO DE LA SOLUCIÓN DE RED DE ÁREA LOCAL (LAN).

Se plantea los diseños de red de área local (LAN), tanto para el centro de datos principal, como también para las nueve oficinas remotas.

3.1.1 RED LAN DEL CENTRO DE DATOS PRINCIPAL.

3.1.1.1 Requerimientos de red LAN del Centro de Datos Principal.

- Soporte de convergencia de tráfico de voz, datos y video.
- Diseño de red e incorporación de equipamiento con criterio de alta disponibilidad.
- Diseño escalable, que permita su crecimiento sin necesidad de afectar la operación de la infraestructura.
- Diseño del sistema de seguridad de la red LAN del centro de datos.

3.1.1.2 Criterios de Diseño.

Para el diseño de la red LAN del centro de datos se aplica la metodología de diseño recomendada por el fabricante CISCO[24], en la que se define un modelo de capas, siendo estas las siguientes:

- Capa de acceso
- Capa de Distribución
- Capa de Core.

En la capa de acceso (conocida también como de borde), se ubican las diferentes estaciones de trabajo de usuarios, como también los recursos de impresión de red. El equipamiento que se utilizará son switches.

La capa de distribución marca el límite entre la capa de acceso y la de core. Esta capa provee servicios de filtraje de paquetes, rutea tráfico entre diferentes grupos departamentales, segmenta la red en diferentes dominios de broadcast. Como equipamiento se utilizará ruteadores.

[24] INTERCONNECTING CISCO NETWORK DEVICES, Cisco Press año, 2000, p.8

La capa de core, es donde se concentra el equipamiento principal de los servicios informáticos y de aplicaciones de la organización. Su diseño debe estar previsto para un manejo de alto tráfico.

Con la finalidad de tener alta disponibilidad de los servicios y manejo de altos volúmenes de tráfico, se incorpora al diseño el concepto de balanceo de carga, el cual permitirá balancear carga entre los servidores WEB.

3.1.1.3 Protocolos de red.

802.1ad: Permite contar con canales de comunicación entre switches redundantes y con balanceo de carga, entre switches, haciendo agregación de la capacidad de canal de los puertos.

802.1w: Rapad Spanning Tree, mismo que nos permite tener enlaces redundantes en la red, pero sólo activo un canal, con rápido proceso de recuperación en caso de falla de un enlace.

802.1Q: es necesario contar con diferentes dominios de broadcast en un marco de seguridad, por lo que para implementarlos se requiere hacer uso de VLAN.

802.1p: Priorización del tráfico, ya que se requiere tener una red convergente, el equipamiento debe permitir priorizar entre los diferentes tipos de tráfico que fluyen por la red.

CoS: Para poder realizar priorización de tráfico, inicialmente el equipamiento de poder clasificar el tráfico.

QoS: se debe garantizar calidad de servicio en cada uno de los aplicativos y tipos de tráfico, el equipamiento debe por tanto, permitir un manejo adecuado del tráfico.

Giga Ethernet: La demanda cada vez más exigente en tiempo de respuesta y manejo de alto volumen de tráfico, requiere que la red sea capaz de manejar alto tráfico, por lo que se utilizará transmisiones en el orden de giga bits por segundo.

3.1.1.4 Arquitectura de red.

Se plantea un diseño en varios niveles, cada uno de los cuales es separado por un firewall que permite la implementación de seguridad. Únicamente se debe habilitar acceso a los servidores a usuarios autorizados.

Los niveles que se tendrán son:

- Outside: Correspondiente a la parte de red que interactúa con Internet.

- Zona Semi-militarizada de Servicios públicos: en los que se ubicará los servidores WEB que darán servicio a través de Internet, así como también los servidores de correo electrónico que trabaja con Internet y el servidor de nombres de dominio (DNS). Este último servidor se actualizará con el servidor del proveedor de acceso a Internet, a la vez que replicará los registros DNS hacia los servidores DNS del interior de la red.

- Zona Militarizada: Se ubicará los servidores de aplicaciones, además del equipamiento de administración del equipo informático, servicios y telecomunicaciones.

- Con la finalidad de brindar alto nivel de seguridad a la información, el acceso a la base de datos se realizará a través de otro nivel de firewall, con lo que se limita en mejor medida la exposición de la misma.

En el centro de datos se implementará adicionalmente una red dedicada exclusivamente a las tareas de monitoreo y operación, tales como las tareas de actualización de aplicaciones, aplicación de parches, etc. Esta red servirá exclusivamente a los equipos destinados a esos fines, y no tendrán acceso a ninguna de las redes por las que fluye el tráfico de las aplicaciones.

Una tercera red, constituye la red de conexión al sistema de almacenamiento, storage área network (SAN), será utilizada exclusivamente por los equipos que hacen uso de la información almacenada en el dispositivo de almacenamiento, así como también por los equipos que realizan tareas de respaldo de la información.

En lo que respecta a las seguridades que se debe implementar, esta se realizará utilizando algunas técnicas:

Firewall de filtraje de paquetes: es el primer nivel de firewall se implementará mediante listas de acceso (ACL) en los equipos ruteadores.

Firewall tipo Statefull Inspecction: es el encargado de delimitar los diferentes niveles de la red, se requiere la implementación de equipos destinados a este propósito exclusivo.

Firewall tipo Proxy: destinado a trabajar a nivel de capa de aplicación, en este momento se implementará el firewall de Proxy destinado al servicio http.

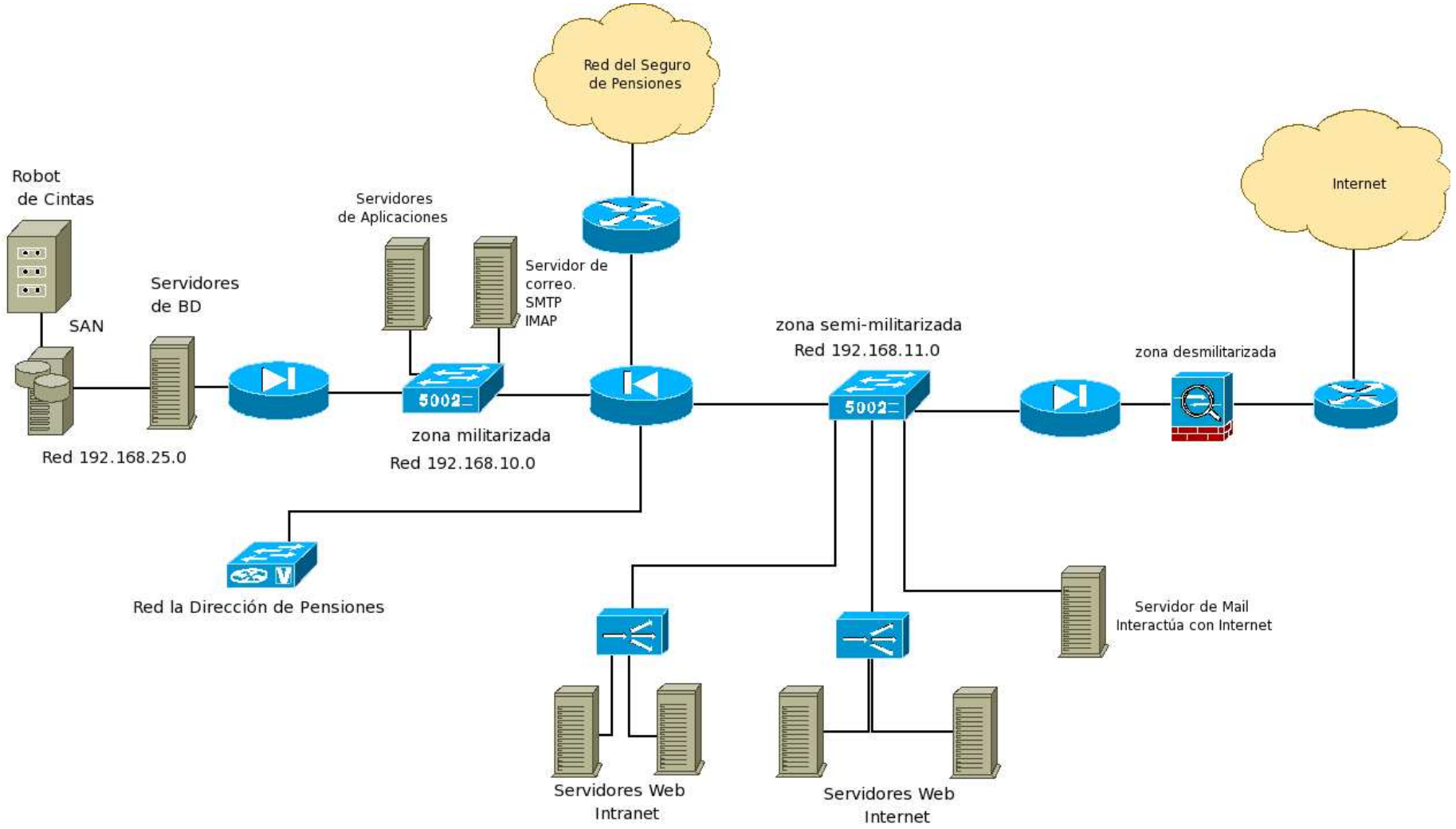
El diagrama de red se muestra en el gráfico 3.1.

El esquema de direccionamiento ha ser utilizado en la red del centro de datos es el que se muestra a continuación.

Cuadro 3.1. Direccionamiento del Centro de Datos.

SUBRED	Direccionamiento
Subred de Servidores WEB	**Dirección de red:** 192.168.11.0 **Máscara:** 255.255.255.0
Subred de Servidores de Aplicaciones	**Dirección de red:** 192.168.10.0 **Máscara:** 255.255.255.0
Subred de Base de Datos	**Dirección de red:** 192.168.25.0 **Máscara:** 255.255.255.0

Gráfico 3.1. Arquitectura de red LAN del centro de datos principal.



Las especificaciones técnicas de los equipos informáticos, seguridades y de telecomunicaciones se adjuntan en el ANEXO II.

3.1.2 RED LAN DE LAS OFICINAS REMOTAS.

Con la finalidad de tener diseños de red LAN que cubran los requerimientos planteados en el capítulo 2.4, así como también considere las características propias de los edificios donde desarrollan sus actividades las diferentes dependencias; se plantea 2 arquitecturas de red.

Para edificios en los que por tener oficinas distribuidas en diferentes pisos de un edificio, se plantea la necesidad de contar con un backbone de edificio y consecuentemente su integración a través de switch de core.

En las locaciones en las que la dependencia utiliza una sola planta de un edificio, se plantea una arquitectura de red que no considera bakbone ni switch de core.

3.1.2.1 Requerimientos de red LAN de oficinas remotas.

- Soporte de convergencia de tráfico de voz, datos y video.
- Diseño de red e incorporación de equipamiento con criterio de alta disponibilidad.
- Diseño escalable, que permita su crecimiento sin necesidad de afectar la operación de la infraestructura.
- Diseño del sistema de seguridad de la red LAN.

3.1.2.2 Criterios de Diseño.

Las redes de área local de las dependencias remotas, deben implementar niveles de seguridad, de tal manera que el acceso a la información local, se realice de acuerdo a políticas de la Organización, adicionalmente, el tráfico de broadcast debe ser controlado, ya que impacta directamente en el rendimiento de la red.

Estos dos elementos enunciados, pueden ser manejados mediante la configuración de VLANS.

La implementación de VLANS debe realizarse por departamentos, a fin de contribuir a incrementar la seguridad interna de la red.

3.1.2.3 Protocolos de red.

802.1ad: Permite contar con canales de comunicación entre switches redundantes y con balanceo de carga, entre switches, haciendo agregación de la capacidad de canal de los puertos.

802.1w: Rapad Spanning Tree, mismo que nos permite tener enlaces redundantes en la red, pero sólo activo un canal, con rápido proceso de recuperación en caso de falla de un enlace.

802.1Q: es necesario contar con diferentes dominios de broadcast en un marco de seguridad, por lo que para implementarlos se requiere hacer uso de VLAN.

802.1p: Priorización del tráfico, ya que se requiere tener una red convergente, el equipamiento debe permitir priorizar entre los diferentes tipos de tráfico que fluyen por la red.

CoS: Para poder realizar priorización de tráfico, inicialmente el equipamiento de poder clasificar el tráfico.

QoS: se debe garantizar calidad de servicio en cada uno de los aplicativos y tipos de tráfico, el equipamiento debe por tanto, permitir un manejo adecuado del tráfico.

Giga Ethernet: La demanda cada vez más exigente en tiempo de respuesta y manejo de alto volumen de tráfico, requiere que la red sea capaz de manejar alto tráfico, por lo que se utilizará transmisiones en el orden de giga bits por segundo.

3.1.2.4 Cableado Estructurado.

El sistema de cableado estructurado que se debe implementar en las oficinas remotas, debe garantizar el transporte de altos volúmenes de información, por lo cual se plantea la necesidad de construir el mismo utilizando componentes de cableado categoría 6. Esta categoría se encuentra vigente en la industria, además de que en el mercado ecuatoriano existe el equipamiento necesario para realizar las pruebas de certificación.

Los estándares que se debe cumplir son los siguientes:

EIA/TIA 569: Diseño y Administración de la Red
EIA/TIA 568: Control de calidad de la instalación.
EIA/TIA 606: Administración
EIA/TIA TSB-67: Pruebas de Cableado Estructurado
EIA/TIA 607: Tierras y aterramientos para sistemas de telecomunicaciones

Los estándares detallados, deben ser de estricto cumplimiento, por lo que es de vital importancia realizar procesos de certificación de los sistemas que se debe implementar.

Uno de los requerimientos, indicado en el capitulo 2.4, es el de tener redes convergentes, por lo que el sistema de cableado estructurado debe tener un solo punto en cada una de las áreas de trabajo, a través del cual, fluirá tráfico de voz, datos y video.

Las especificaciones técnicas del sistema de cableado estructurado se encuentra en ANEXO II.

3.1.2.5 Arquitectura de red.

3.1.2.5.1 Red LAN con backbone.

Las dependencias del Seguro de Pensiones que tienen oficinas distribuidas en algunos pisos de un edificio, requieren para su implementación un backbone de

datos. Este permitirá la comunicación de los diferentes subsistema de cableado horizontal que existe en el edificio.

El backbone de datos estará implementado con fibra óptica (de acuerdo al requerimiento del capítulo 2.4) multimodo de 6 hilos, de los cuales estarán operativos dos pares de hilos y el restante será respaldo en caso de averías en uno de los enlaces principales.

En cada uno de los pisos existirá un switch de acceso, cuyo dimensionamiento y número de puntos está acorde con el número de puntos que se encuentra en el subsistema horizontal del cableado estructurado.
Los switch de cada piso se integran al switch de core, a través de dos canales de fibra óptica, cuyos puertos en los switch deben tener configuración de agregación de enlace (802.1ad), a fin de incrementar la capacidad del canal que enlaza los switch de acceso con el switch de core y manejar balanceo de carga y alta disponibilidad.

El core de la red, se debe implementar con dos switch, esto permitirá mantener la red operativa en caso de falla de uno de los switch.

Cada uno de los switch, debe tener la estructura de VLANS como se indica en el siguiente cuadro:

Cuadro 3.1. Asignación de ID de las diferentes VLANS.

ID VLAN	NOMBRE de VLAN	AREA
1	VL-MONITOREO	Monitoreo
2	VL-GF	Gestión Financiera
3	VL-LIQUIDADORES	Liquidadores
4	VL-CS	Centro de Servicio
5	VL-ROUT	VLAN para conexión con el ruteador
6	VL-DIRECCIÓN	Dirección de Pensiones. Aplica solamente para la red de la mencionada Dirección

Las subredes que se tendrá en cada LAN, corresponde a los diferentes grupos de trabajo que laboran en una dependencia, siendo estos los de Gestión Financiera, Liquidadores y el Centro de Servicio al Cliente. Adicionalmente para tareas de administración y monitoreo, es necesario tener una VLAN para este efecto, la cual será utilizada por personal técnico. La arquitectura de red, requiere tener una VLAN que permita la comunicación entre el ruteador y switch de core, ella no es utilizada por ningún usuario, solamente utilizan los equipos de red.

En los switch de acceso como los switch de core, debe configurarse los protocolos de calidad de servicio, priorización y clasificación de paquetes, en donde la mayor prioridad se debe asignar al tráfico de voz.

Para tener una red automatizada, se debe habilitar en los switch de core el servicio UDP Helper, el mismo que permitirá distribuir en las subredes de las diferentes VLNAS, las direcciones IP de las estaciones de trabajo de manera automatizada.

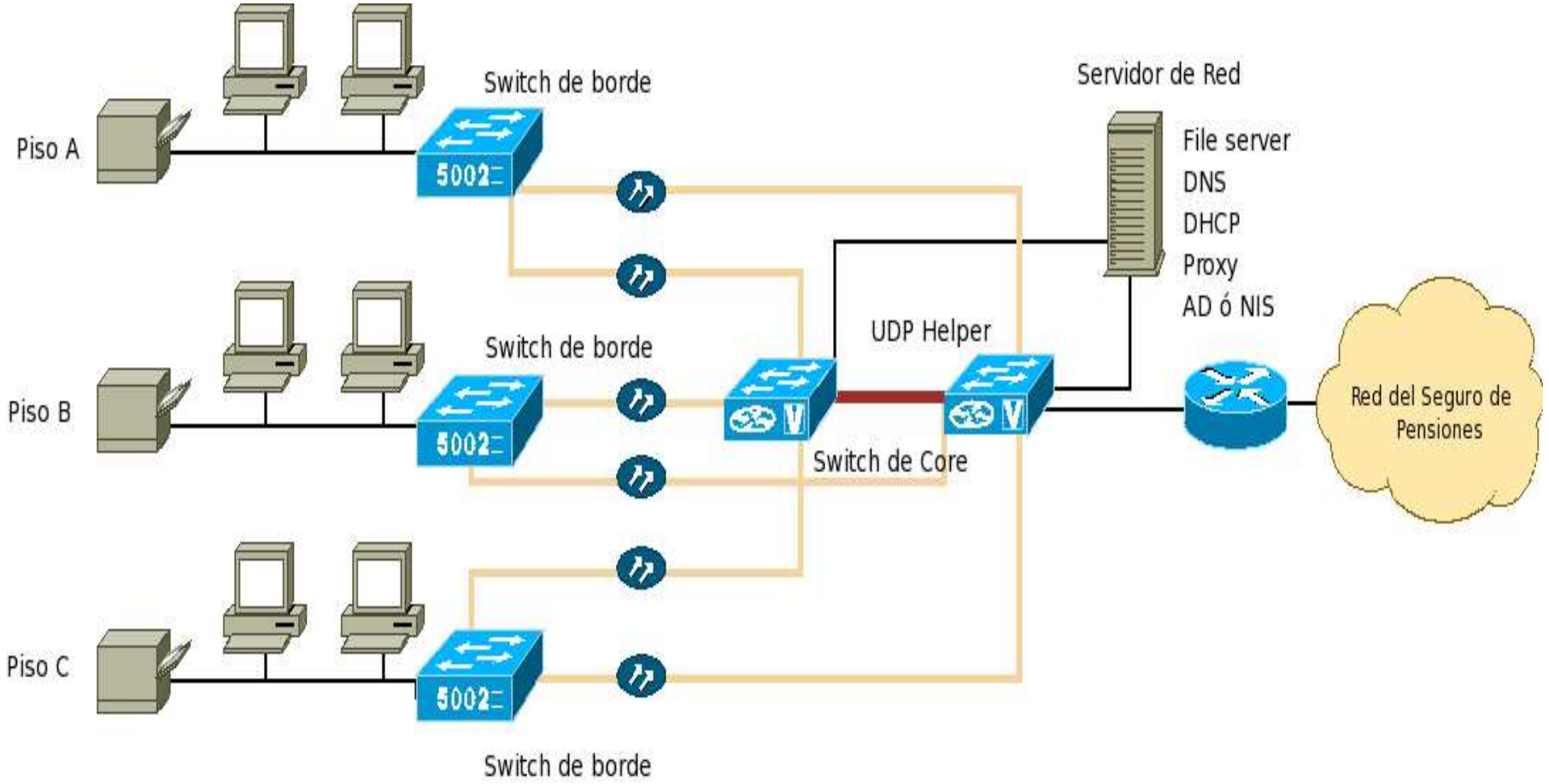
En el gráfico 3.2 se indica la arquitectura de la red.

En lo que respecta al direccionamiento que se utilizará para cada una de las redes, se considera los siguientes criterios para asignación de direcciones:

- La primera dirección válida de red ó subred se asignará al Servidor.
- La última dirección válida se asignará a la interfaz LAN del ruteador.
- Las 5 primeras y últimas direcciones son excluidas del rango de DHCP.

El rango excluido en cada red ó subred, será utilizado por dispositivos que requieren direcciones fijas, como servidores e impresoras.

Gráfico 3.2. Arquitectura de red LAN utilizando backbone de datos.



Cuadro 3.2. Esquema de Direccionamiento redes con backbone.

Dependencia	Esquema de Direccionamiento
Dirección de Pensiones y Subdirección de Contabilidad	**Dirección de red**: 192.168.2.32 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.2.38 a 192.168.2.58 **Default Gateway:** 192.168.2.62 **IP Servidor de Red:** 192.168.2.33
Subdirección de Pichincha	**Dirección de red**: 192.168.3.0 **Máscara:** 255.255.255.0 **Rango DHCP:** 192.168.3.5 a 192.168.3.250 **Default Gateway:** 192.168.3.254 **IP Servidor de Red:** 192.168.3.1
Subdirección del Guayas	**Dirección de red**: 192.168.4.128 **Máscara:** 255.255.255.128 **Rango DHCP:** 192.168.4.134 a 192.168.4.250 **Default Gateway:** 192.168.4.254 **IP Servidor de Red:** 192.168.4.129
Subdirección del Azuay	**Dirección de red**: 192.168.5.64 **Máscara:** 255.255.255.192 **Rango DHCP:** 192.168.5.70 a 192.168.5.122 **Default Gateway:** 192.168.5.126 **IP Servidor de Red:** 192.168.5.65

3.1.2.5.2 Red LAN sin backbone.

Esta arquitectura de red se aplica a las oficinas que desarrollan sus actividades en una sola planta de edificio, ó que el número de usuarios y las distancias existentes entre las áreas de trabajo y el cuarto de telecomunicaciones no amerita la implementación de backbone, ya que esto encarecería innecesariamente la solución.

El switch que establece la conectividad en esta red, debe tener configurado VLAN´S, para realizar un control de tráfico de broadcast, a la vez que se incorpora un elemento de seguridad interno de la red local.

Los criterios utilizados para asignación de direcciones IP, son los mismos que se indicaron en el acápite 3.1.2.5.1.

El siguiente cuadro, muestra los rangos de direcciones asignados a cada una de las redes remotas.

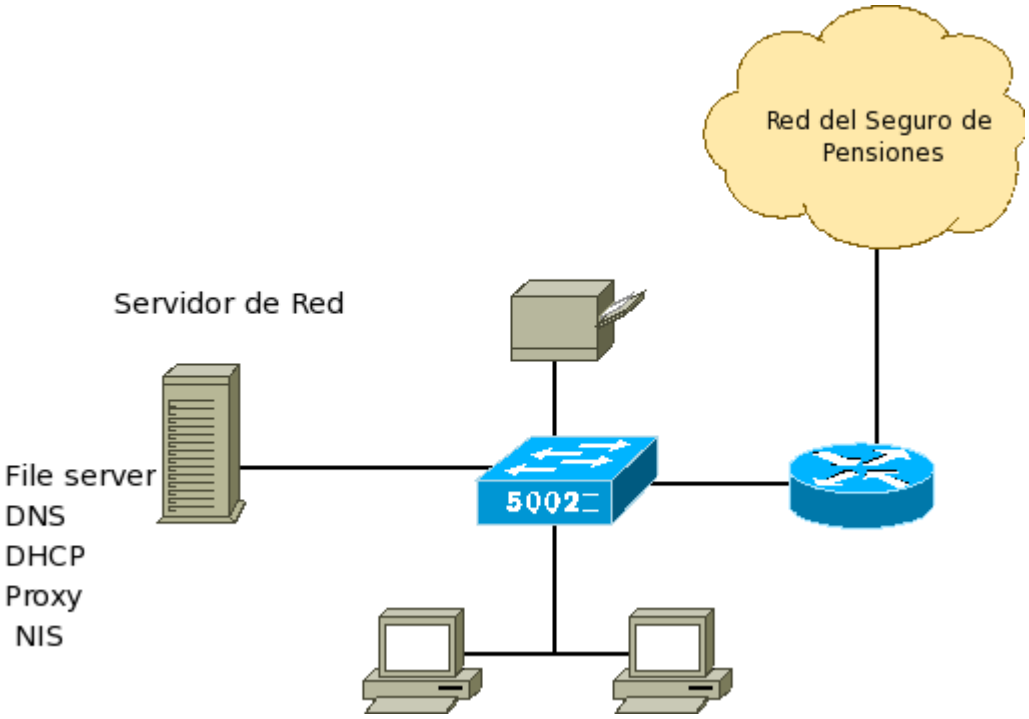
Cuadro 3.3. Esquema de Direccionamiento redes sin backbone.

Dependencia	Esquema de Direccionamiento
Unidad de Pensiones Imbabura	**Dirección de red**: 192.168.6.32 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.6.38 a 192.168.6.58 **Default Gateway:** 192.168.6.62 **IP Servidor de Red:** 192.168.6.33
Unidad de Pensiones Tungurahua	**Dirección de red**: 192.168.6.64 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.6.70 a 192.168.6.90 **Default Gateway:** 192.168.6.94 **IP Servidor de Red:** 192.168.6.65
Unidad de Pensiones Chimborazo	**Dirección de red**: 192.168.6.96 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.6.102 a 192.168.6.122 **Default Gateway:** 192.168.6.126 **IP Servidor de Red:** 192.168.6.97
Unidad de Pensiones Loja	**Dirección de red**: 192.168.6.128 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.6.134 a 192.168.6.154 **Default Gateway:** 192.168.6.158 **IP Servidor de Red:** 192.168.6.129
Unidad de Pensiones Manabí	**Dirección de red**: 192.168.6.160 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.6.166 a 192.168.6.186 **Default Gateway:** 192.168.6.190 **IP Servidor de Red:** 192.168.6.161
Unidad de Pensiones de El Oro	**Dirección de red**: 192.168.6.192 **Máscara:** 255.255.255.224 **Rango DHCP:** 192.168.6.198 a 192.168.6.218 **Default Gateway:** 192.168.6.222

Dependencia	Esquema de Direccionamiento
	IP Servidor de Red: 192.168.6.193

En el siguiente gráfico se muestra la arquitectura de red.

Gráfico 3.3. Arquitectura de red LAN sin backbone de datos.



3.2 DISEÑO DE LA SOLUCIÓN DE RED DE ÁREA AMPLIA (WAN).

La red de área amplia (WAN), representa el conjunto de soluciones de telecomunicaciones que permiten la conectividad remota de las diferentes redes de área local para la transmisión de tráfico de voz, datos y video.

La liberalización del mercado de las telecomunicaciones y el desarrollo de nuevas tecnologías han propiciado una oferta cada vez mayor de soluciones de telecomunicaciones en nuestro país.

3.2.1 REQUERIMIENTOS DE RED WAN.

El diseño de la red de telecomunicaciones se realizará considerando los criterios de convergencia, escalabilidad, interoperabilidad y alta disponibilidad. Ésta infraestructura debe soportar tráfico de voz, datos y video; mediante la incorporación de protocolos de calidad de servicio.

3.2.2 PLANTEAMIENTO DE LA SOLUCIÓN.

Los equipos de red WAN del Seguro de Pensiones, así como también la infraestructura de los proveedores de servicios de telecomunicaciones, debe posibilitar la implementación de calidad de servicio fin a fin; ello permitirá manejar tráfico de distinta naturaleza (voz, datos y video) a través de los enlaces entre las diferentes dependencias.

Siendo la tecnología de conmutación de etiquetas multiprotocolo (MPLS) orientada al manejo de enlaces de telecomunicaciones con criterios de calidad de servicio y agregación, se plantea la incorporación de la misma como solución tecnológica de telecomunicaciones, en las ciudades en las que los proveedores de servicio estén en capacidad de entregar. En la actualidad, existen proveedores en las ciudades de Quito, Guayaquil y Cuenca con esta tecnología.

Los restantes canales, pueden utilizar tecnología Frame-Relay, la cual en el país es ampliamente difundida y tiene cobertura en las principales ciudades.

Con la adopción de MPLS como tecnología de telecomunicaciones, se garantiza escalabilidad en la red WAN, ya que esta mediante las soluciones de agregación, facilita el escalamiento, en capacidades de canal y manejo de diferente tipo de tráfico con criterio de calidad de servicio.

La red WAN del Seguro de Pensiones debe tener un alto índice de disponibilidad y rendimiento, utilizando una conexión dedicada vía microonda ó por medio físico, para la interconexión de todas las oficinas del Seguro de Pensiones.

3.2.3 TOPOLOGÍA DE RED.

Uno de los requerimientos de implementación es la de contar con una solución de alta disponibilidad, por lo que se plantea una arquitectura de red con un backbone central, constituido por los nodos de las ciudades de Quito (Edf, Dirección de Pensiones), Guayaquil (Subdirección de Pensiones Guayas) y Cuenca (Subdirección de Pensiones Azuay), todos estos en una configuración delta.

A cada uno de estos nodos, confluirán las dependencias de acuerdo a una distribución regional, se indica a continuación:

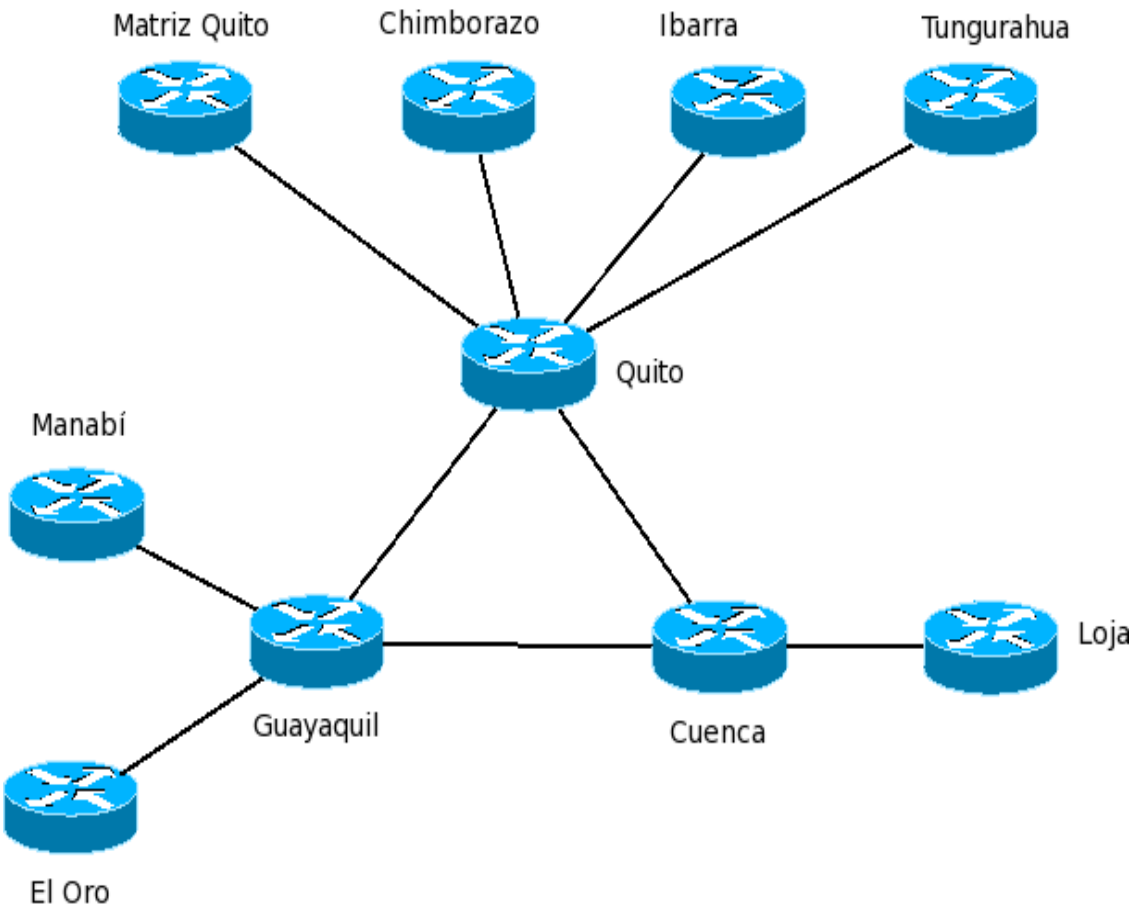
Cuadro 3.4. Distribución regional de los enlaces de Telecomunicaciones.

NODO	SITIOS REMOTOS
Nodo Quito:	Subdirección de Pichincha Subdirección de Imbabura Subdirección de Tungurahua Subdirección de Chimborazo
Nodo Guayaquil	Subdirección de Manabí Subdirección de El Oro
Nodo Cuenca	Subdirección de Loja.

En el gráfico 3.4 se muestra la topología de red

Es necesario indicar que los nodos de las ciudades de Guayaquil y Cuenca, estarán ubicados en los centros de datos de las correspondientes Subdirecciones de Pensiones, en tanto que el de Quito, se encontrará en las instalaciones de la Dirección de Pensiones.

Gráfico 3.4. Topología de red WAN.



3.2.4 DIRECCIONAMIENTO DE RED WAN.

Con la finalidad de incorporar un elemento de seguridad a nivel de red WAN, el direccionamiento debe manejar máscara de 30 bits, esto impedirá la posibilidad de que alguien no autorizado, conecte un dispositivo para lectura de información que fluye por el enlace, ya que este dispositivo no tendrá direcciones IP disponibles para formar parte de la subred entre los ruteadores.

El cuadro siguiente indica el esquema de direcciones IP, para las interfaces WAN de los ruteadores.

Cuadro 3.5. Direccionamiento IP de red WAN.

Origen	Destino	IP Origen	IP Destino	Máscara de red
BACKBONE DE TELECOMUNICACIONES				
Dirección de Pensiones (Quito)	Subdirección de Pensiones Guayas	10.10.1.1	10.10.1.2	255.255.255.252
Dirección de Pensiones (Quito)	Subdirección de Pensiones Azuay	10.10.1.5	10.10.1.6	255.255.255.252
Subdirección de Pensiones Guayas	Subdirección de Pensiones Azuay	10.10.1.9	10.10.1.10	255.255.255.252
ENLACES DESDE NODOS A LAS OFICINAS DE PENSIONES				
Dirección de Pensiones (Quito)	Unidad Pensiones Pichincha	10.10.1.17	10.10.1.18	255.255.255.252
	Unidad Pensiones Imbabura	10.10.1.13	10.10.1.14	255.255.255.252
	Unidad de Pensiones Tungurahua	10.10.1.37	10.10.1.38	255.255.255.252
	Unidad de Pensiones Chimborazo	10.10.1.21	10.10.1.22	255.255.255.252
Subdirección de Pensiones Guayas	Unidad de Pensiones El Oro	10.10.1.29	10.10.1.30	255.255.255.252
	Unidad de Pensiones Manabí	10.10.1.25	10.10.1.26	255.255.255.252
Subdirección de Pensiones Azuay	Unidad de Pensiones Loja	10.10.1.33	10.10.1.34	255.255.255.252

3.2.5 CAPACIDAD DE CANALES DE TELECOMUNICACIONES.

Cuadro 3.6. Capacidad de canal de cada uno de los enlaces.

ORIGEN	DESTINO	CAPACIDAD DE CANAL	TIPO DE CANAL
BACKBONE DE TELECOMUNICACIONES			
QUITO	GUAYAQUIL	1,5 Mbps.	MPLS
QUITO	CUENCA	1,5 Mbps.	MPLS
GUAYAQUIL	CUENCA	1,5 Mbps.	MPLS
ENLACES			
QUITO	SUDIRECCION DE PENSIONES	1,0 Mbps.	Frame Relay
QUITO	IBARRA	256 Kbps.	Frame Relay

ORIGEN	DESTINO	CAPACIDAD DE CANAL	TIPO DE CANAL
QUITO	TUNGURAHUA	256 Kbps.	Frame Relay
QUITO	CHIMBORAZO	256 Kbps.	Frame Relay
CUENCA	LOJA	256 Kbps.	Frame Relay
GUAYAQUIL	MANABI	256 Kbps.	Frame Relay
GUAYAQUIL	EL ORO	256 Kbps.	Frame Relay

El cálculo de los enlaces de telecomunicaciones se realizó tomando como base la cantidad de bytes de las páginas del Sistema de Pensiones, las cuales según pruebas en la aplicación son de 25KB cada página. Con esta información y considerando un nivel de concurrencia de un 5% del número de usuarios de cada oficina, se determinó las capacidades de canal que se muestran en el cuadro 3.6.

Ejemplo:

Para el cálculo del enlace de telecomunicaciones Guayaquil - Quito, siendo este un nodo en el que confluyen las dependencias de Manabí y el Oro, se tiene que el total de usuarios es igual a la sumatoria de los usuarios de las dependencias referidas. Según el cuadro 2.6 se tendría:

A= 25KB x (62+21+16) = 2.475 KB x 1024 x 8 = 20,3Mbits
A: Cantidad de bits de descarga por todos los usuarios.

Si el nivel de concurrencia fuera del 100%, es decir que todos los usuarios descargan una página de la aplicación en 1 seg., la capacidad de canal sería de:

C’ = A / T = 20,3Mbits / 1seg = 20,3Mbps
T: Unidad de tiempo en segundos
C’: Capacidad de canal
C = C' x Concurrencia = 20,3Mbps x 0,05 = 1,015Mbps

Manejando capacidades de canal estandarizadas se tiene un canal de 1.5 Mbps.

Enlace de Telecomunicaciones Manabí – Guayaquil

A = 25KB x 21 x 1024 x 8 = 4,3Mbits
C’ = 4,3Mbits / 1seg = 4,3Mbps
C = 4,3Mbps x 0,05 = 215Kbps
Manejando capacidades de canal estandarizadas se tiene un canal de 256Kbps.

Enlace de Telecomunicaciones El Oro – Guayaquil

A = 25KB x 16 x 1024 x 8 = 3,3Mbits
C’ = 3,3Mbits / 1seg = 3,3Mbps
C = 3,3Mbps x 0,05 = 165Kbps

Manejando capacidades de canal estandarizadas se tiene un canal de 256Kbps.

Para el dimensionamiento del enlace Guayaquil – Cuenca, se considera que este canal soportará máximo tráfico cunado el enlace Quito – Guayaquil esté fuera de servicio, por lo que su capacidad de canal será igual al del enlace Quito – Guayaquil, siendo este de 1,5Mbps.

Las especificaciones técnicas del equipamiento de red LAN y WAN, así como de enlaces de telecomunicaciones se encuentran en el ANEXO II.

CAPITULO 4

ANALISIS DE SERVICIOS DE RED.

4.1 SERVICIOS.

En este capítulo se ofrece un enfoque de todos los servicios que se van a implementar en la infraestructura de red del Seguro de Pensiones del Instituto Ecuatoriano de Seguridad Social.

El funcionamiento de un entorno de computación en red depende de muchos servicios que proporcionan distintos componentes de software. Estos servicios podemos clasificarlos en dos clases: los servicios a nivel de red y los servicios a nivel de usuario.

Algunos de estos servicios son necesarios para que las computadoras participen en el entorno de computación en red, incluso antes de que se ejecuten las aplicaciones a nivel de usuario. Estos servicios a nivel de red permiten que las computadoras en un entorno de computación en red, funcionen como un todo coherente, estos son: servicio de nombres de dominio (DNS), protocolo de configuración dinámica de host (DHCP) y servidor de información de red (NIS).

Otros servicios son necesarios para dar soporte a aplicaciones de usuario: estos servicios son: CORREO ELECTRÓNICO, SERVIDOR DE ARCHIVOS, WEB y PROXY[25].

4.1.1 SERVICIOS A NIVEL DE RED.

Estos servicios no los usan directamente los usuarios. En lugar de esto forman parte integral del entorno de computación en red proporcionando servicio a los

[25] Administración de Sistemas Linux , M Carling, Stephen Degler, James Dennos, Prentice Hall, p.213

sistemas operativos y a las aplicaciones. La prestación de estos servicios a todos los sistemas de una organización sienta las bases de los servicios de nivel superior. La prestación fiable de estos servicios hace que el entorno de computación en red sea estable y predecible.

4.1.1.1 Servidor de Nombres de Dominio.

Servicio de nombres de dominio proporciona traducciones de nombres de host a direcciones IP. También proporciona traducciones inversas de direcciones IP a los nombres de host. DNS delega la responsabilidad de la administración de los nombres de host a los responsables de administración de red, es uno de los servicios fundamentales que un administrador de red debe implementar.

4.1.1.2 Protocolo de configuración de host dinámico.

DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los hosts de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente / servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después.

4.1.1.3 Servicio de información de red.

El servicio de información de Red (NIS) proporciona a todos los host que haya en un dominio NIS, datos unificados concernientes a los usuarios, grupos de usuarios, alias de correo y otra información del sistema.

4.1.2 SERVICIOS A NIVEL DE USUARIOS.

4.1.2.1 Correo Electrónico.

El correo electrónico ha eclipsado a la telefonía, al fax y a la iteración personal directa como vehículo esencial para la comunicación. El funcionamiento de muchos negocios ha llegado a depender del envió fiable de correo.

Es un servicio que permite a los usuarios enviar y recibir mensajes instantáneos mediante sistemas de comunicación electrónicos, principalmente se usa el nombre de correo electrónico para denominar al sistema que provee este servicio en Internet, mediante el protocolo de transporte de mensajes cortos (SMTP). Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de contenido. Su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo normal para muchos usos habituales.

4.1.2.2 Protocolo de Transporte de Hipertexto (HTTP).

Publicación de sitios web alojados en el servidor empresarial, manejando múltiples dominios y acceso dinámico a bases de datos empresariales tales como Informix, Oracle, MySQL. Permite implementar soluciones de comercio electrónico, extranets, publicación de información organizacional ó habilitar acceso a servicios corporativos.

4.1.2.3 Servidor de Archivos.

Compartición segura y configurable de documentos y carpetas para usuarios de la red, mediante Samba para integrare con redes Windows y NFS para integrarse con redes Unix/Linux permitiendo generar respaldos centralizados, distribución de aplicaciones, actualizaciones o simplemente extensión de discos de trabajo,

permitiendo la asignación de carpetas individuales para cada usuario de la red o grupos específicos.

4.1.2.4 Proxy.

Para el acceso compartido a Internet desde la red interna, permitiendo el control de usuarios y equipos que tienen opción de navegación; configuración dinámica de sitios permitidos y/o negados, horarios de navegación, servicios disponibles tales como “free mail”, chat, descarga de archivos, acceso a música, videos, etc.

Configuración de “Proxy caché” para una navegación más rápida y sobre todo mejor aprovechamiento del canal de telecomunicaciones.

4.2 PLANTEAMIENTO DE LA SOLUCION.

El campo de acción del Seguro de Pensiones es a nivel nacional manteniendo 9 oficinas distribuidas en las ciudades de Quito, Guayaquil, Ibarra, Ambato, Riobamba, Cuenca, Loja, Machala, Portoviejo para atención de los usuarios. Para la implementación de los servicios de red del Seguro de Pensiones se debe tomar en cuenta varios parámetros, entre los cuales podemos mencionar, alto trafico en la red, seguridad en los accesos a los servicios y aplicaciones, facilidad de administración de los servicios, minimizar el impacto en caso de falla de los equipos servidores o de los servicios. De esta manera nos permitirá dar a los usuarios un servicio eficaz, seguro y confiable, explotando de mejor forma la plataforma y tecnología instalada.

4.2.1 IMPLEMENTACION DE LOS SERVICIOS DE RED.

Para la implantación de los servicios de red, tomando en cuenta los parámetros antes mencionados, se deberá instalar un servidor que atenderá los servicios de DNS, DHCP y NIS, corriendo bajo la plataforma Linux en cada localidad y en el nodo principal matriz en Quito.

El servicio de DNS se lo implementará y configurará ejecutando named que es el servidor de nombres, distribuido por BIND (Demonio de nombres de Internet de Berkeley)[26]. Para la implementación del servicio de DNS, se manejará un esquema de replicación de los servidores DNS de todas las redes remotas desde el servidor principal del nodo matriz, los archivos de la configuración del servidor de DNS del nodo principal se encuentra en el ANEXO III.

Para el servicio de DHCP vamos a utilizar el demonio DHCP que viene incorporado en el sistema operativo Linux, el cual nos permitirá definir los ámbitos o rangos de direcciones de red dentro de los cuales se asignarán automáticamente a los usuarios que se conecten a la red de datos local. Estos ámbitos o rangos de direcciones de red son asignados en base a un plan de direccionamiento previamente establecido para la configuración de las redes a nivel nacional (ver CAPITULO 3), los archivos de configuración del servidor de DHCP del nodo principal se encuentra en el ANEXO III.

Para la implementación del servicio de NIS se deberá utilizar el demonio de NIS que se encuentra embebido en el sistema operativo. El esquema de trabajo de NIS es similar al de DNS ya que vamos a manejar replicación en donde un servidor maestro, en el nodo matriz, replicará a los servidores esclavos en las redes remotas, con lo cual logramos tener un esquema distribuido para el manejo de usuarios, brindando al usuario la facilidad de conexión desde cualquier red remota a cada uno de los servicios permitidos a él.

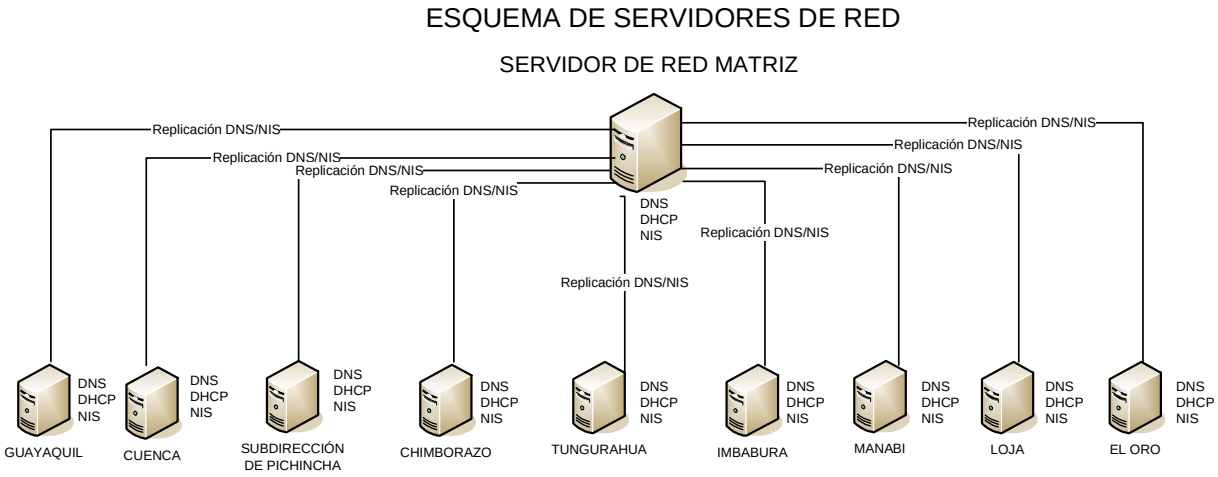
Definición de los sistemas que integran el esquema NIS:

- *Servidor Maestro:* Es el origen de los datos NIS para el dominio. Todas las actualizaciones de los datos NIS se producen en este servidor[27].
- *Servidor Esclavo:* Mantiene una copia de la base de datos maestra. Se actualiza cuando los datos cambian en el servidor maestro[28].

[26] Referencia DNS and BIND, tercera edición, Paul Albitz y Cricket Liu, 1998
[27] Managing NFS and NIS, de Hal Stern, publicado por O'Really & Associates
[28] Managing NFS and NIS, de Hal Stern, publicado por O'Really & Associates

- *Cliente:* El sistema se conecta a un esclavo NIS o servidor maestro para obtener datos NIS[29].

Gráfico 4.1: Esquema de servidores de red.



4.2.2 IMPLEMENTACION DE LOS SERVICIOS DE USUARIO.

De igual forma como se tomó en cuenta los parámetros requeridos para los servicios de red, los tomaremos en cuenta para la implantación de los servicios de usuarios.

4.2.2.1 Proxy.

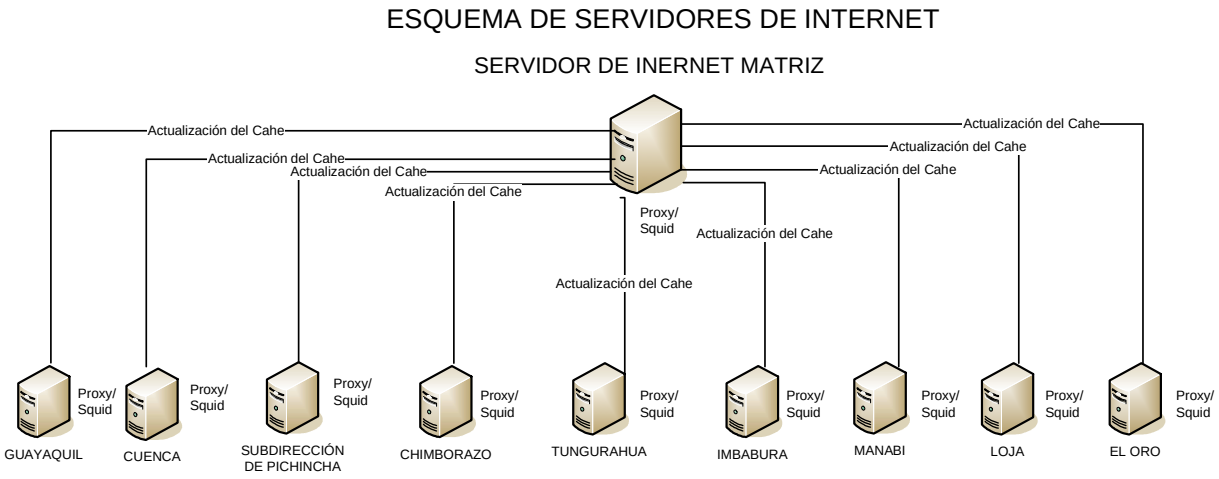
Para proporcionar a los usuarios el servicio de Internet utilizaremos el servicio Squid de Linux, el objetivo de utilizar esta solución es el aprovechamiento de las funciones incorporadas en esta aplicación como es el servidor caché, facilidad en el control de acceso, administración y monitoreo lo cual nos permite dar un mejor uso de los recursos de la infraestructura de red.

El esquema establecido para realizar proxy, es que cada servidor local actualice su caché de páginas en el servidor Squid principal, de tal manera que cada

[29] Managing NFS and NIS, de Hal Stern, publicado por O'Really & Associates

usuario navegue localmente y solo el servidor será el que refresque sus archivos caché, evitando así una saturación en los recursos de la red, que podría darse en caso de no manejar el esquema referido, en el ANEXO III presentamos el archivo de configuración del Squid del nodo matriz.

Gráfico 4.2 Esquema de servidores de Internet.

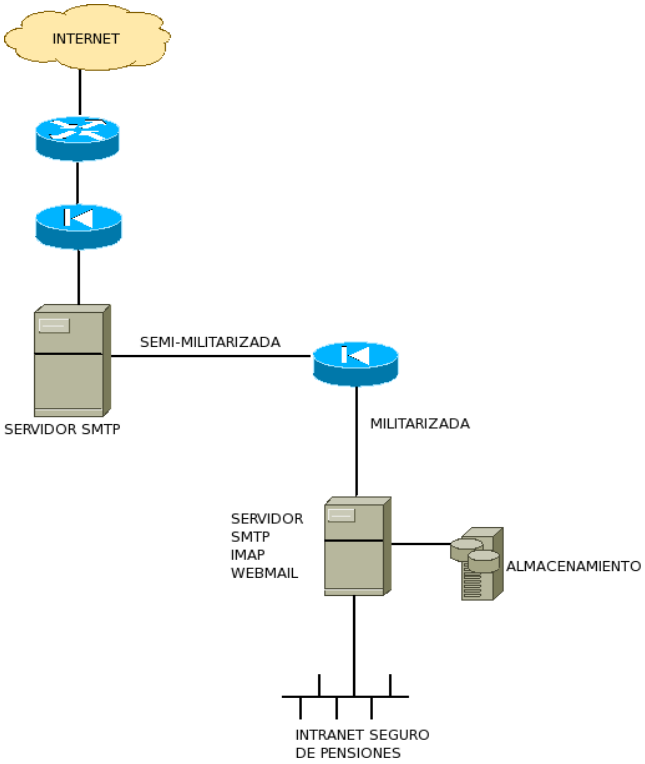


4.2.2.2 Correo Electrónico.

Con la finalidad de proporcionar a los usuarios el servicio de correo electrónico y aprovechar las herramientas que nos facilita el sistema Operativo Linux vamos a utilizar los demonios de Postfix que manejan protocolo SMTP para el envió de correos y el demonio IMAP para la distribución de correo electrónico. Para implementar un esquema de correo electrónico seguro, eficaz y confiable se ha tomado en cuenta las mejores prácticas de implementación de este servicio y se plantea la siguiente arquitectura:

En el grafico 4.3 se muestra el esquema de Correo Electrónico.

Gráfico 4.3: Esquema del Servicio de Correo Electrónico.



Utilizaremos dos equipos servidores de rango medio y un storage (ver especificaciones ANEXO II), los cuales deberán trabajar bajo el esquema de Front end y Back end en donde tendremos un servidor principal MX MTA (Mail Transport Agent) que será quien interactúe con Internet y es encargado del envió y recepción de correo, este equipo se encontrará en la zona semi-militarizada, el otro servidor estará localizado en la zona militarizada y realizará funciones de MTA y de MDA (MAIL Delivery AGENT). Se utilizará el cliente IMAP para la lectura de los correos almacenados en los buzones de los clientes, los datos de correo electrónico estarán alojados en la unidad de almacenamiento.

Este esquema nos permite tener el servicio de correo centralizado para todos los usuarios del Seguro de Pensiones a nivel nacional, los cuales podrán tener acceso mediante un cliente de correo como Evolution, Thunderbird y otros, a cada usuario se le proporcionara un nombre de usuario y clave de acceso para el ingreso a este servicio.

Para agregar seguridad al servicio de correo electrónico vamos a utilizar herramientas robustas completamente compatibles con Linux y que son de tipo Open Source tales como MailScanner combinado con Clanv y Spammassassin, que permitirá agregar protección contra correo masivo no solicitado, fraudes electrónicos, virus, gusanos y troyanos.

Es necesario proveer al usuario la posibilidad de revisar su correo electrónico mediante el uso del ambiente WEB, para lo cual vamos a usar la herramienta Webmail Squirrelmail.

4.2.2.3 Implementación del Servidor de Archivos.

Un usuario de red mediante este servicio puede buscar, conservar o publicar información y tener acceso a través de los recursos de la red[30].

Para realizar el manejo de archivos, se instalará un servidor para cada agencia incluido la matriz y utilizaremos NFS para atender dicho servicio con los clientes Linux. Una de las utilidades principales que nos proporciona y por la cual se pensó en usar la estructura de NFS y NIS es la portabilidad de las cuentas de usuarios con sus directorios locales, es decir nosotros desde cualquier localidad que nos encontremos podemos ingresar a nuestro directorio local simplemente con nuestro usuario y clave.

4.3 IMPLEMENTACION DE SERVICIOS Y APLICACIONES WEB.

En lo que se refiere a servicios y aplicaciones Web, estos se implementarán en el nodo matriz bajo el esquema de 3 capas con la siguiente arquitectura.

[30] Sistemas de comunicación orientadas a la descentralización de las entidades publicas Guevara Julca, José Zulu

4.3.1 CAPA WEB.

El acceso al sistema del Seguro de Pensiones se realizará vía Web, para lo cual se implementará una granja de servidores, compuesto por cuatro equipos (las especificaciones técnicas se encuentran en el ANEXO II), los cuales se conectarán a dos balanceadores de carga. Éstos balanceadores trabajarán atendiendo uno a los usuarios de la Intranet y el otro a los del Internet por separado.

La capa Web de la aplicación del Seguro de Pensiones se debe implementar con la configuración que se detalla a continuación:

Configurar el servidor Apache para obtener balanceo de carga hacia el servidor JBOSS de la aplicación mediante el módulo *mod_jk*[31].

Para habilitar el módulo se debe copiar el archivo *mod_jk-1.2.23-apache-2.2.x-linux-x86.so* al archivo */etc/httpd/modules/mod_jk.so* usar el comando:

```
# cp mod_jk-1.2.23-apache-2.2.x-linux-x86.so /etc/httpd/modules/mod_jk.so
```

Editar los siguientes archivos:
/etc/httpd/conf.d/mod_jk.conf:
/etc/httpd/conf/workers.properties:
/etc/httpd/conf/uriworkermap.properties:

Ver la configuración del mod_jk.conf, workers.properties, uriworkermap.prperties en el ANEXO IV

Dichos archivos configuran el comportamiento del balanceo con mod_jk.
Se debe modificar la configuración del servidor Apache para guardar relación con la opción *maxThreads* del Connector AJP de JBoss, ver ANEXO IV

[31] El módulo *mod_jk* fue obtenido de http://tomcat.apache.org/download-connectors.cgi, versión para Linux.

La configuración por defecto de Red Hat Enterprise Linux 5 utiliza la estrategia *prefork* para ejecutar los procesos de Apache.

4.3.2 CAPA DE APLICACIONES.

En esta capa estarán los servidores que contendrán las reglas de negocio de la aplicación del Seguro de Pensiones que proporcionará servicio a los afiliados, funcionarios y jubilados.

CARACTERISTICAS DE LAS APLICACIONES:

La aplicación del Seguro de Pensiones tienen las siguientes características:

- Desarrollada sobre Arquitectura J2EE, utilizando componentes estándares de la industria.
- Permite ser deployada en diferentes contenedores de aplicaciones como JBOSS, OC4J de Oracle.
- Aplicación construida por módulos que nos permite incorporar módulos adicionales sin afectar su normal funcionamiento.
- Independencia de la arquitectura de los servidores de aplicaciones
- Fácil de administrar y Parametrizar.
- Facilidad para someterse a cambios debido a los avances tecnológicos con el menor costo e impacto posible.

De acuerdo a las características de la aplicación y en cumplimiento a los requerimientos indicados en el capítulo 2.4, se ha determinado trabajar sobre la siguiente plataforma:

- Sistema Operativo Linux REDHAT 5.0
- Aplication Server JBoss 4.2

Para aprovechar al máximo los recursos del equipo e implementar alta disponibilidad y balanceo de carga, se debe explotar las bondades que posee el contenedor de JBOOS. En el servidor se debe configurar varios servidores de JBOSS virtuales, cada uno contendrá el sistema y trabajarán en forma

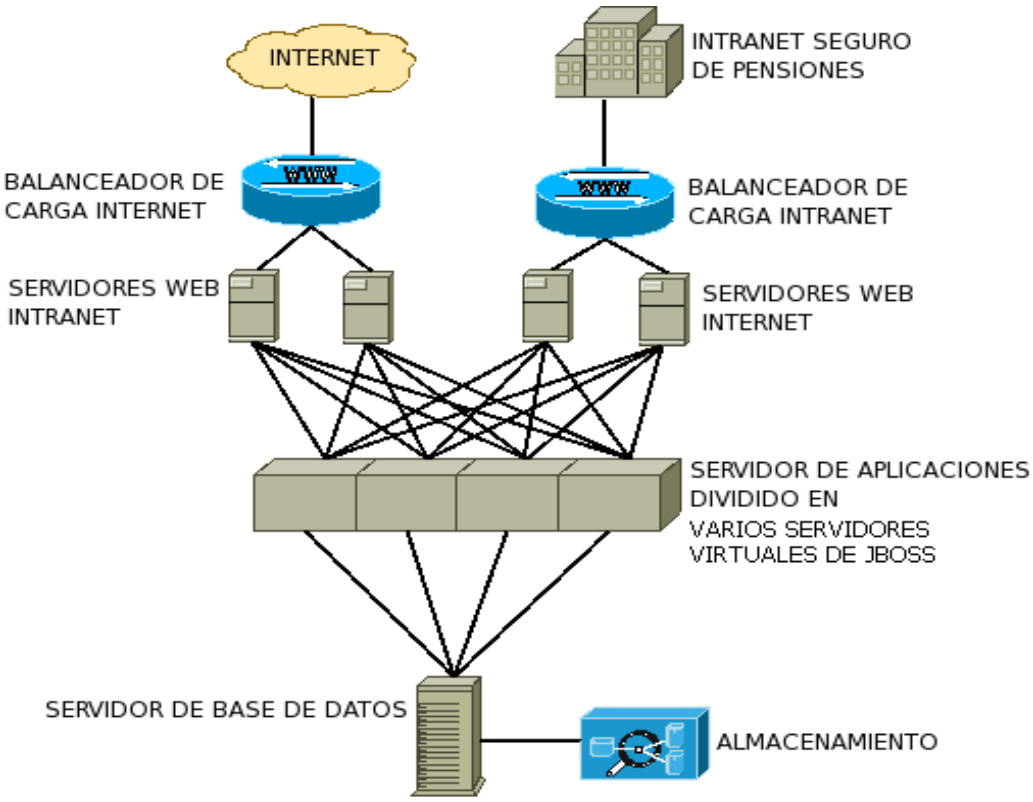
independiente, es decir que si uno tiene problemas o sale fuera de servicio, el modulo mod_jk de los Webs lo detecta y no le entrega peticiones hasta que se restablezca la operación, de esta manera garantizaremos la disponibilidad del servicio.

El módulo mod_jk se encarga de entregar las peticiones a cada servidor JBOSS utilizando el algoritmo de Round Robin para balaceo de carga.

4.3.3 CAPA DE BASE DE DATOS.

En esta capa debe estar la Base de datos de la Institución, para lo cual se establecieron las características de equipos (ver ANEXO II) sobre los cuales operará la Base de Datos.

Gráfico 4.4: Esquema de los Servicios de Aplicaciones Web.



CAPITULO 5

PLANTEAMIENTO DE LA POLITICA DE SEGURIDAD.

5.1 ANALISIS DE ACTIVOS DE INFORMACION DE LA ORGANIZACIÓN.

El aseguramiento de una red de comunicación significa el establecimiento de medidas que permitan cumplir los requisitos de protección respecto a la integridad, disponibilidad, confidencialidad y autenticidad de la información conducida por la red. Para valorar efectivamente los requerimientos de seguridad es necesario realizar un análisis de riesgos a la realidad administrativa, tecnológica y operativa de la red. Posteriormente será posible definir políticas, normas de seguridad y desarrollar procedimientos relacionados con mecanismos de seguridad.

- ¿Qué información y servicios provistos por la red de comunicaciones desea proteger?
- ¿De qué o de quién se desea proteger la información y los servicios?

Para esto se utiliza la metodología fundamentada en un proceso lógico conformado por las siguientes etapas.

- IDENTIFICACION DE LA INFORMACION Y SERVICIOS QUE DEBAN SER PROTEGIDOS: Sobre la base de la misión y funciones del Seguro de Pensiones, identificar la información y servicios críticos para el cumplimiento de funciones.
- IDENTIFICACION DE AMENAZAS: Descubrir las amenazas potenciales que puedan causar incidentes de seguridad.

- IDENTIFICACION DE VULNERABILIDADES: Determinar las vulnerabilidades presentes en los activos definidos para que sean corregidas debidamente.
- CUANTIFICACION DEL COSTO: De las pérdidas y/o calificación del impacto de un incidente a la seguridad. Determinar las prioridades de las necesidades de protección.
- DETERMINACION DE REQUERIMIENTOS DE SEGURIDAD: Establecer las medidas administrativas, técnicas, operativas necesarias para la protección de la información y servicios.

5.1.1 IDENTIFICACION DE LA INFORMACION Y SERVICIOS.

Para esta identificación es necesario enfocar las áreas asociadas al cumplimiento de las funciones fundamentales del Seguro de Pensiones del Instituto Ecuatoriano de Seguridad Social: Dirección del Seguro de Pensiones, Subdirección de Pensiones y las Unidades Provinciales de Pensiones, mediante las cuales conoceremos, por medio de entrevistas, los diferentes procesos de la Institución y los detalles de los mismos, lo que permite identificar y calificar con facilidad la sensibilidad de la información y disponibilidad de los servicios considerando las características de seguridad.

Cuadro 5.1 Fuentes y temas de consulta para la identificación de información y servicios.

LEVANTAMIENTO DE INFORMACIÓN DEL SISTEMA INFORMÁTICO **INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL** **SEGURO DE PENSIONES**
SECTOR: DIRECCION **FUENTE:** Director y Subdirector del Seguro de Pensiones.
1. Propósito de la red de telecomunicaciones dentro de las políticas, estrategias y directrices Institucionales. **2.** La red de telecomunicaciones y la proyección externa del Seguro de Pensiones del IESS: imagen y reputación. **3.** La red de telecomunicaciones como soporte a la prestación de servicios.

Cuadro 5.2 Fuentes y temas de consulta para la identificación de información y servicios Sector Operativo.

LEVANTAMIENTO DE INFORMACIÓN DEL SISTEMA INFORMÁTICO INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL SEGURO DE PENSIONES
SECTOR: OPERATIVO **FUENTE:** Jefes Departamentales, Personal Operativo, Departamento de informática
1. Nuevos procedimientos de servicio con la inclusión de la informática **2.** Programas de capacitación **3.** Comunicación de Unidades Provinciales **4.** Acceso a fuentes de información **5.** Difusión, promoción y publicidad **6.** Medios de vinculación con el sector externo, Empresas, Comunidad y Estado

Cuadro 5.3 Fuentes y temas de consulta para la identificación de información y servicios Sector Administrativo.

LEVANTAMIENTO DE INFORMACIÓN DEL SISTEMA INFORMÁTICO INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL SEGURO DE PENSIONES
SECTOR: ADMINISTRATIVO **FUENTE:** Secretarías, Departamento de informática
1. La red como medio de procesamiento y transmisión de la información. Sistemas de información administrativos institucionales. **2.** La red como soporte de sistemas y métodos administrativos para una optima prestación de servicios a los afiliados. **3.** La red como medio de publicación de resoluciones relacionadas con las políticas, normas y leyes institucionales.

5.1.2 IDENTIFICACION DE AMENAZAS.

Las amenazas siempre han existido, la diferencia es que ahora, el enemigo es mas rápido, más difícil de detectar y mucho más atrevido. Es por eso que toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias no deseadas[32].

El tratamiento que se plantea en esta etapa será aplicado en forma individual a aquella información y servicios identificados en la etapa anterior.

FUENTE AMENAZAS: GENTE

- Administrador
- Operador
- Usuario
  - Interno
  - Externo

FUENTES AMENAZAS: EVENTOS DEL MEDIO AMBIENTE Y NATURALES

- Interrupción suministro eléctrico
- Interrupción de líneas de comunicación de datos
- Riesgos Naturales: Incendio, Terremoto, Inundaciones

CARACTERISTICAS DE SEGURIDAD AMENAZADAS

- Control de acceso
- Confidencialidad
- Integridad
- Disponibilidad
- No Repudio

[32] Referencia Guía de Administración de seguridades en Linux de 2da, Edición

5.1.3 IDENTIFICACION DE VULNERABILIDADES.

Las amenazas se pueden convertir en realidad a través de fallas de seguridad, que conocemos como vulnerabilidades y que deben ser eliminadas al máximo para que el ambiente que se desea proteger este libre de riesgos de incidentes de seguridad[33].

El siguiente es el esquema que se plantea para el cumplimiento de esta etapa.

VULNERABILIDADES ORGANIZACIONALES:

Las vulnerabilidades son debilidades asociadas con cada activo de información, en este caso, tratamos las vulnerabilidades que se desprenden de la administración, operación y uso de los sistemas.

El siguiente listado enumera las actividades básicas de administración, operación y uso de sistemas en los cuales pueden existir vulnerabilidades.

De los Administradores:

- Control acceso lógico y físico
- Identificación / Autentificación
- Integridad de la información y Servicio

De los Operadores:

- Conocimiento de las operaciones de la aplicación
- Tareas de mantenimiento

De los usuarios Internos:

[33] Referencia Guía de Administración de seguridades en Linux de 2da, Edición

- Identificación / Autentificación
- Destrezas computacionales

VULNERABILIDADES TECNOLOGICAS:

Estas vulnerabilidades son las que se derivan del diseño, implementación y configuración de:

- Arquitectura de la Red
- Sistemas Operativos implementados
- Implementación de servicios de red
    - Correo electrónico
    - Publicación Servicios WEB
    - Acceso a Internet

5.1.4 CONSECUENCIAS DE UN INCIDENTE A LA SEGURIDAD.

Una vez evaluado todos los *activos a proteger, amenazas y vulnerabilidades* el siguiente paso es analizar todo en conjunto para determinar las consecuencias en caso se concrete alguna amenaza en la disponibilidad, integridad, confidencialidad de la información y/o la disponibilidad del servicio.

Dependiendo de la gravedad, se establece la prioridad. La potencialidad de la amenaza y la existencia de vulnerabilidades configuran los escenarios en los cuales suceden incidentes a la seguridad de la red de comunicación estos escenarios son los riesgos a los que estaría expuesta la red.

Para medir el impacto se asignará calificaciones cualitativas alto, medio, bajo.

Las consecuencias de una amenaza, en un ambiente transaccional como el del Seguro de Pensiones, pueden ser entre otras las siguientes:

- Disminución de la productividad por la interrupción de actividades operativas.
- Una pérdida de credibilidad y oportunidad.

- Imposibilidad de cumplir con las responsabilidades administrativas

5.1.5 DETERMINACION DE REQUERIMIENTOS DE SEGURIDAD.

Los requerimientos de seguridad pueden darse en 2 áreas:

- Requerimientos Administrativos
- Requerimientos Técnicos

REQUERIMIENTOS ADMINISTRATIVOS: Orientados a corregir vulnerabilidades organizacionales a través de buenas prácticas en la administración de recursos de la red y mecanismos de seguridad.

REQUERIMIENTOS TECNICOS: Orientados a corregir vulnerabilidades tecnológicas.

De acuerdo al criterio del departamento de Defensa de los Estados Unidos[34] los requerimientos de seguridad pertenecen a los siguientes tipos:

- Control de acceso
- Identificación / Autentificación
- Integridad
- Auditoria

5.2 ANALISIS DE RIESGOS PARA LA RED DEL SEGURO DE PENSIONES.

Se aplica la metodología propuesta en el acápite anterior. Antes de aplicar es necesario conocer información importante que dice de los objetivos de la red de

[34] Referencia documento del Departamento de Defensa de EEUU

telecomunicaciones, dentro del cumplimiento de los fines del Seguro de Pensiones del IESS.

5.2.1 INFORMACION INSTITUCIONAL.

El análisis del Seguro de Pensiones se detalla en el capítulo 2.

5.2.2 ANALISIS DE RIESGOS A LA SEGURIDAD.

Actores que intervienen en todos los procesos

- Niveles directivo, operativo, ejecutivo, administrativo
- Personal técnico y administrativo del Centro de Cómputo.
- Proveedores de Internet

5.2.3 IDENTIFICACION DE INFORMACION Y SERVICIOS.

SECTOR: DIRECTOR – EJECUTIVO:

Fuentes de Consulta:

- Director de Pensiones
- Subdirector de Pensiones

Información y servicios identificados:
Sin embargo que las consultas a este sector no identifican explícitamente la información y servicios que requieren protección, la información proporcionada por los consultados permite deducir la importancia en un contexto general que tiene la red de telecomunicaciones.

Consultadas las autoridades de la importancia y el rol que cumple o debe cumplir la red de telecomunicaciones, estas son sus visiones:

- Es un referente importante en el plan estratégico dentro del proceso de modernización del Instituto Ecuatoriano de Seguridad Social especialmente en

el Seguro de Pensiones, considerando sobre todo la gran importancia que está teniendo el Internet.

- Es una infraestructura de comunicación vital e imprescindible en las líneas de comunicación interna y externa a través del correo electrónico.
- Es un elemento de apoyo en la modernización del Seguro de Pensiones, intercomunicando la Dirección y Subdirecciones Provinciales entre sí y con el medio social.
- Es un elemento fundamental de apoyo para los nuevos retos que enfrenta el Seguro Social, principalmente en su plan de modernización y mejoras de servicio al cliente.

SECTOR: OPERATIVO:

Fuentes de Consulta:

- Coordinador de Gestión Tecnológica
- Operadores, Administradores del área Tecnológica
- Coordinadores del proyecto

Información y Servicios Identificados:

- Información confidencial de los afiliados, Base de Datos.
- Información de carácter personal conducida a través de mensajes electrónicos.
- Información confidencial de carácter propietario que se necesite compartir con usuarios internos y externos.
- Información generada para consultas estadísticas del Seguro de Pensiones.
- Información publica del sitio WEB del Seguro de Pensiones.
- Infraestructura de Servidores de Base de Datos y Aplicaciones para el área de producción.
- Infraestructura para los sistemas de Backups de las bases de datos.
- Infraestructura de Servidores de Servicios de Red, Correo, Internet, Archivos, WEB y otros.

- Infraestructura computacional con acceso al Internet y disponibilidad de servicios de red para trabajar en el sistema informático del Seguro de Pensiones.
- Infraestructura computacional que permita el acceso de usuarios externos al sistema informático del Seguro de Pensiones vía WEB.
- Infraestructura computacional para capacitación a los funcionarios y usuarios del sistema informático.
- Infraestructura computacional del grupo de desarrolladores y administradores con acceso al Internet y disponibilidad de servicios de red para cumplir con las funciones designadas.
- Ambiente operativo que incluye las actividades de Seguro de Pensiones, como son áreas de trabajo, áreas de almacenamiento de la información crítica, agencias de atención al cliente, centros de procesamiento de datos.
- Infraestructura de telecomunicaciones equipos de conectividad, conexiones.

SECTOR: ADMINISTRATIVO:

Fuentes de Consulta:

- Secretaria General
- Departamento de Procesamiento de Datos
- Funcionarios del Seguro de Pensiones

Información y servicios Identificados:

En lel cuadro 5.4 se listan los sistemas relacionados con la información que maneja el sector administrativo. Se incluyen la calificación otorgada por los consultados a la sensibilidad de la información.

Cuadro 5.4. Sistema de Información identificados con una calificación de los niveles de las características de seguridad.

Sistema de información	Confidencialidad	Integridad	Disponibilidad
Sistema Pensiones	Alta	Alta	Alta
Modulo de Jubilación	Alta	Alta	Alta
Modulo de Cesantías	Alta	Alta	Alta
Sistema Supervivencia	Alta	Alta	Media

Consolidando los datos colectados, resulta que la información y servicios que requieren seguridad son los siguientes:

- Información Administrativa manejada por los respectivos Sistemas. Información listada en el cuadro 5.1.
- Información de la base datos de los afiliados.
- Información propietaria de los usuarios.
- Información estadística.
- Información de los sistemas Informáticos.
- Servicio de correo electrónico.
- Servicio de Internet.
- Servicio de WEB de la Institución.
- Infraestructura de comunicaciones.
- Infraestructura computacional para los usuarios.
- Infraestructura computacional para capacitación.
- Servidores de Bases de datos y Aplicaciones.
- Servidores de Servicios de Red.
- Ambiente Físico Operativo.

5.2.4 IDENTIFICACION DE AMENAZAS.

- Amenazas a los Sistemas de Información:
  - Errores de código.
  - Código malicioso.
  - Fallos técnicos.

  - Errores de usuarios.
  - Falta de seguridad de acceso a los sistemas de información.

- Amenazas a la información de Base de Datos de los afiliados:
  - Plagio.
  - Falsificación.
  - Alteración.
  - Pérdida de privacidad.

- Amenazas a la información Propietaria, Estadística:
  - Plagio.
  - Falsificación.
  - Alteración.
  - Pérdida de privacidad.

- Amenazas a la información de los desarrolladores:
  - Plagio.
  - Alteración.

- Amenazas servicios de Correo Electrónico:
  - Pérdida de privacidad.
  - Alteración.

- Amenazas al servicio de Internet:
  - Falla Proveedores.
  - Ataque de negación de servicios.
  - Uso Impropio.
  - Falla equipos.

- Amenazas al servicio WEB:
  - Ataques de negación de servicios.
  - Alteración de información.
  - Falla de los componentes.

- Amenazas a la infraestructura de telecomunicaciones:
    - Fallas de funcionamiento.
    - Falta de seguridad en el diseño e implementación de la infraestructura.
    - Falta personal capacitado para el manejo y administración.

- Amenazas a la infraestructura computacional usuarios, administradores, desarrolladores, capacitación:

    - Ataques de virus.
    - Falsificación de identidad.

- Amenazas servidores de Base de Datos, Aplicaciones y servidores de red:

    - Falla en el equipo (Hardware).
    - Problemas de Sistema operativo.
    - Ataques de virus.

- Amenazas al ambiente físico operativo:
    - Desastres naturales.
    - Accesos no autorizados.

5.2.5 IDENTIFICACION DE VULNERABILIDADES.

La cultura de la seguridad de información en el Seguro de Pensiones debe estar en capacidad de regular el comportamiento de las distintas partes relacionadas con los servicios Internet y los sistemas de información, de allí que es necesario un tratamiento formal de la seguridad reflejado en políticas Institucionales.

Tanto la implementación de la red como los sistemas deben tener todos los criterios de seguridad, sin descuidar aspectos como los mencionados en la

sección anterior respecto a las amenazas desde el Internet y la implementación de controles que hagan posible un uso discreto, discriminado y planificado de los recursos.

En lo que sigue se identifican las vulnerabilidades organizacionales y tecnológicas, que podemos tomar en cuenta en el análisis de riesgos del Seguro de Pensiones

5.2.6 VULNERABILIDADES ORGANIZACIONALES.

Identificación y Autentificación:

El mecanismo de autenticación empleado en todos los sistemas y servicios del Seguro de Pensiones es el password, elegidos por el usuario o por el sistema.

Control de acceso lógico:

Exige la identificación y autenticación del usuario o el cifrado de soportes magnéticos intercambiados entre entidades o de respaldo interno, o de información transmitida en línea.

Correo electrónico:
Para el acceso al servicio de correo electrónico debe poseer un usuario y una clave proporcionada por el administrador del sistema de correo, se debe mantener la confidencialidad de la información.

Conexión Internet:

Establecer un control de acceso a los usuarios del servicio de Internet, al igual que listas de acceso a sitios que no sean necesarios para desarrollar normalmente sus obligaciones con la Institución.

Sistema de Información Administrativos:

Los sistemas de información deben tener un control de acceso estricto ya que cualquier mal uso o manipulación de los datos podría ocasionar alteraciones que pueden generar perdidas para la institución, exige un esquema de usuario y password cifrado.

Mantenimiento de Software y Hardware:

Prever un esquema de respaldo completo y consistente de la información y configuraciones de los sistemas antes de realizar un mantenimiento de hardware y software sobre los equipos, de igual forma realizarlo con técnicos especializados en el tema.

Seguridad física de las Instalaciones del Centro de Cómputo:

Establecer seguridades de control de acceso, seguridades físicas de todas las instalaciones.

5.2.7 VULNERABILIDADES TECNOLOGICAS.

Arquitectura de red:
La arquitectura de red siendo el tema principal de este trabajo se esta tomando en cuenta todas las reglas de seguridad existentes, acompañado con un estudio de mejores prácticas y experiencias en el campo, para desarrollar un producto robusto y seguro, evitando ser un punto de vulnerabilidad dentro del esquema del Seguro de Pensiones. Ver capítulo 3.

Equipos de Telecomunicaciones:

En los equipos de telecomunicaciones para el envió y recepción de la información tales como ruteadores, firewall, switch, etc. Podemos tener las siguientes vulnerabilidades:

- Problemas con energía eléctrica
- Errores de configuración

Servidores:

Los servidores son analizados con prioridades en relación a sus normas de acceso definidas. Se revisan cuales son los tipos de usuarios que tienen derechos a determinada información, se los clasifica y se los relaciona de acuerdo al grado de confidencialidad de la misma para identificar el exceso o falta de privilegios para la ejecución de tareas. El enfoque principal se lo realiza en los ficheros de configuración de los sistemas y en la definición y creación de usuarios que tienen derecho de administración de los sistemas.

Estaciones de Trabajo:

La forma como están configuradas para evitar que los usuarios (con frecuencia de forma inconsciente) permiten la acción de amenazas.

Ejemplos de vulnerabilidades comunes en este tipo de activos:

- Ausencia de protector de pantallas bloqueado por clave, que permite que las máquinas dejadas solas no sean utilizadas por personas no autorizadas.
- Ausencia de configuraciones de seguridad que permitan la instalación o ejecución de ficheros maliciosos.
- Periodicidad de actualización de programas antivirus, forma de organización de los directorios, presencia o ausencia de documentos confidenciales.
- Forma de utilización de la estructura de servidores de archivos, que garanticen de una manera más eficiente la copia de seguridad de los datos, es decir, su disponibilidad.

Servicios de Red:

Correo electrónico E-mail bombing y spamming:

El e-mail bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando el buzón del destinatario. El spamming es una variante de e-mail bombing se refiere a enviar el correo a centenares o millares de usuarios e inclusive a listas de interés. El spamming puede resultar aún más perjudicial si los destinatarios contestan el correo, haciendo que todos reciban la respuesta. El e-mail bombing/spamming se puede combinar con el e-mail spoofing que altera la identidad de la cuenta que envía el correo, logrando así que sea más difícil determinar quién está enviando realmente el correo.

Cuando gran cantidad de correos son dirigidos a un solo sitio, este puede sufrir “una negación de servicio” por perdida de conectividad, caerse el sistema o producirse fallas en el servicio.

Servicios WEB:

Se debe proteger tanto el sistema operativo de los servidores de ser atacado vía Web, como su sitio Web de acceso no autorizado.

Atacar el sistema operativo vía Web implica generalmente alterar un cgi script o lograr que el servidor Web haga algo que no fue pensado que haga. Además de ser cuidadosos con los scripts cgi, hay que revisar las configuraciones de acceso en el servidor Web, los permisos con los que el mismo se ejecuta, y los directorios de datos expuestos.

Navegación en Internet:

La mayoría del software, incluyendo sistemas operativos y aplicaciones, viene con scripts de instalación o programas de instalación. La meta de estos programas de instalación es dejar los sistemas operativos lo más rápido posible, con la mayor

parte de funciones disponibles o habilitadas, y con la ayuda de muy poco trabajo por parte del administrador. Estas vulnerabilidades son aprovechadas por software malicioso que está presente en las páginas del Internet[35].

Una de las vulnerabilidades más comunes en el servicio de Internet que son explotadas por páginas maliciosas es provocar que el servicio finalice abruptamente su ejecución, con un error de excepción.

5.2.8 CONCECUENCIAS DE UN INCIDENTE DE SEGURIDAD.

Base de Datos:

La indisponibilidad, plagio o alteración en la información de la base de datos seria un perjuicio muy significativo para la Institución ya que almacena la información de todos los afiliados y Jubilados, por lo que le ubica en un nivel de importancia crítica y podría paralizar los servicios.

Sistema Administrativo:

Los sistemas del Seguro de Pensiones son los más importantes dentro de las actividades de los servicios que presta la Institución de ahí que un problema de seguridad les dejaría al margen de trabajo a todos los usuarios de los servicios, provocando graves pérdidas, tanto económicas como de imagen.

Servicios WEB:

Debido a que las transacciones se realizan por medio de la Web, el servicio web también es un activo del cual no podemos prescindir, ya que el impacto que nos causaría seria el mismo que el sistema administrativo, los usuarios no podrían realizar sus transacciones debidas y nos provocaría resultados indecibles.

[35] Referencia http://www.vsantivirus.com/20vul.htm

Correo Electrónico:

El correo electrónico es un activo que se utiliza como herramienta importante en la comunicación de la Institución. La suspensión de este servicio por cualquier incidente de seguridad es medianamente significativa ya que la misión principal de la institución esta vinculada con los ítems anteriores. Se podría tener una holgura de tiempo de recuperación, obviamente de pocas horas.

Navegación en Internet:

El servicio de Internet es muy importante para los objetivos de consulta e información de la empresa, pero no juega un papel muy importante para cumplir los objetivos de la empresa. Lo cual nos permite poner una calificación de disponibilidad baja a este servicio.

Medios de Telecomunicaciones:

Es la columna vertebral de la plataforma tecnológica. El mal funcionamiento o una falla por cualquier causa producida sobre alguno de estos activos, podría causarnos la interrupción de determinados servicios, determinada zona o inclusive si el daño es grande podría ocasionar la interrupción total de todos los servicios.

Cuadro 5.5 Clasificación del impacto de las amenazas a la información y servicios.

Sistema / servicio	Confidencialidad	Integridad	Disponibilidad
Bases de Datos	Alta	Alta	Alta
Sistema de Información Administrativos	Alta	Alta	Alta
Servicios WEB	Alta	Alta	Alta
Correo electrónico	Alta	Alta	Media
Acceso Internet	Baja	Baja	Baja
Medios de Telecomunicaciones	Alta	Alta	Alta

5.2.9 DETERMINACION DE REQUERIMIENTOS DE SEGURIDAD.

5.2.9.1 Requerimientos Técnicos de Seguridad.

Se definen conforme a las necesidades de confidencialidad, disponibilidad e integridad que se desprenden en el cuadro 5.2 y se pueden clasificar en dos áreas:

- Controles en el sistema de cómputo que soporta el servicio o sistema de información.
- Servicios de seguridad que garanticen la confidencialidad e integridad de la información (Bases de Datos, correo) y la disponibilidad de servicios (Aplicaciones, Servicio web, Acceso a Internet, sistemas/aplicaciones, medios de comunicación).

Los servicios de seguridad se definen para cada servicio de acuerdo a las exigencias de confidencialidad, integridad y disponibilidad.

Cuadro 5.6 Servicios de seguridad requeridos para la protección de la información y servicios identificados.

Servicio	Disponibilidad de servicios	Confidencialidad de la información transmitida	Integridad
Bases de Datos	Aplicar medidas de prevención planificación de respaldos y recuperación de la misma	Encriptación de la información para manipulación en los sistemas. Control de acceso a la información.	Control de acceso a usuarios o grupos responsables de la manipulación de la información.
Correo	Aplicar medidas de disponibilidad	Encriptación de la información a criterio del usuario	Firma digital

Servicio	Disponibilidad de servicios	Confidencialidad de la información transmitida	Integridad
Sistemas/Aplicaciones	Aplicar medidas de disponibilidad	Control de acceso lógico y físico a los archivos del sistema	Mantenimiento de la integridad del sistema debe ser responsabilidad del grupo usuario o grupo de Soporte a quien pertenece
Servicio WEB de la Institución	Aplicar las medidas de prevención expuesta en la protección de acceso a Internet.	Ningún requerimiento	Verificar la autenticidad de las paginas que se encuentran expuestas en el servidor
Acceso a Internet	Medidas preventivas para evitar una condición de fallo. Protección de la IP contra Spoofing. Protección de ataques de denegación de servicios	Ningún requerimiento	Ningún requerimiento
Medios de telecomunicaciones	Planificación de alta disponibilidad, elaboración de	Control de acceso lógico y físico a los equipos	Revisar y respaldar continuamente la configuración de los equipos. Proteger

Servicio	Disponibilidad de servicios	Confidencialidad de la información transmitida	Integridad
	planes de contingencia con los equipos.		estas con contraseñas.

5.2.9.2 Requerimientos de Seguridad Administrativa.

Estos deben contrarrestar las vulnerabilidades detectadas:

- Identificación/Autentificación.
- Controles acceso lógico.
- Seguridad Física.
- Estandarización de Software.
- Mantenimiento de Hardware y Software.
- Administración Seguridades.

Cuadro 5.7 Definir tareas de administración de la red y servicios.

Cargo	Tareas Administrativas
Jefe Departamento de Tecnología	Creación e implementación de procedimientos generales, interpreta normas y mantiene contacto con las unidades de Dirección para llevar a cabo procesos de elaboración y ejecución de proyectos.
Administrador de áreas tecnológicas	Se encarga de la creación e implementación de procedimientos de cada área. Recomienda y lleva a cabo los planes e investiga sobre las nuevas tecnologías y documentación del entorno.
Operadores	Sigue un conjunto estricto de procedimientos con el fin de realizar el mantenimiento rutinario de un sistema y resolver las eventualidades que se presenten.

Cuadro 5.8 Requerimientos administrativos para la protección de la información y servicios.

Requerimiento	Servicios Administrados	Tareas Especificas
Administrador de los servicios de Internet y red de telecomunicaciones	Acceso Internet	Control de accesos, administración de usuarios y del servicio.
	Equipos de comunicación	Configurar y mantener la disponibilidad del servicio.
	Enlaces	Monitoreo de la disponibilidad del servicio.
	Servicios de Red (DNS, DHCP,FTP)	Implementación, configuración y monitoreo de disponibilidad del servicios, control de acceso
Área de administración de los centros de cómputo, servidores y aplicaciones.	Centro de cómputo	Control de acceso físico, planes de contingencia contra probables amenazas, organización del centro de datos.
	Servidores de Base de Datos	Instalación, Configuración y control de la disponibilidad de los servidores de Bases de Datos unidades de almacenamiento.

Requerimiento	Servicios Administrados	Tareas Especificas
	Servidores aplicaciones Servidores de Archivos	Servidores de Aplicaciones, diseño de planes de contingencia, planificación de equipos.
	Aplicaciones	Realizar pruebas establecidas a las aplicaciones desarrolladas previos a la puesta en producción.
	Correo	Administración del servicio de correo
	Servidores WEB	Administración de los servidores WEB de la institución.
Operadores	Respaldos	Realizar copias de seguridad de los sistemas y de los datos.
	Mantenimiento Aplicaciones	Realizar actualizaciones en las aplicaciones previa aprobación de las pruebas.
	Servidores, ruteadores	Controlar los sistemas en especial los servidores y los ruteadores.

Requerimiento	Servicios Administrados	Tareas Especificas
Área de administración Bases de Datos	Base de datos de los diferentes sistemas	Administración de Bases de Datos, control de acceso a la información, monitoreo de la disponibilidad del servicio planificación y pruebas de respaldos de la información.
Área de administración seguridades	Equipos de seguridad Documentación de seguridad	Realizar Procedimientos, políticas y normas de seguridad, control del cumplimiento de las políticas de seguridad implementadas, administración de equipos de seguridad.
Área de Soporte Técnico	Equipamiento computacional de los usuarios	Instalación y configuración de los equipos de los usuarios, control de virus y soporte a los mismos.

5.3 POLÍTICAS DE SEGURIDAD INFORMÁTICA.

5.3.1 INTRODUCCION.

Una política de seguridad es una declaración de una estrategia de administración con respecto a seguridad. Estas declaraciones están agrupadas bajo las siguientes secciones:

1. Política institucional
2. Políticas de seguridad de la información
3. Políticas de seguridad del personal
4. Políticas de seguridad de computadores y redes
5. Ejecución

5.3.2 POLITICA INSTITUCIONAL

Cada unidad de negocio es responsable de crear sus propias políticas de seguridad bajo la coordinación de la Dirección de Desarrollo Institucional. Estas políticas deberían establecer reglas para la protección de los datos y procesos del negocio que correspondan a las amenazas ó riesgos involucrados y al valor de dichos activos.

5.3.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.3.3.1 Conceptos

- Todos los activos de información deben tener un propietario.
- Cada propietario debe clasificar la información dentro de uno de los niveles sensitivos (que se mencionan abajo), dependiendo de obligaciones legales, costos, políticas institucionales y necesidades del negocio. El propietario es responsable por la protección de esta información.
- El propietario debe definir quién está permitido acceder a sus datos.
- El propietario es responsable por sus datos y debe asegurarlos de acuerdo a su nivel de sensibilidad.

5.3.3.2 Clasificación de la Información.

El sistema de clasificación de la información considera clasificarla en cuatro niveles:

- Información Pública.
- Información Interna.
- Información Confidencial.
- Información Secreta.

Él más bajo (Pública) es el menos sensitivo y el más alto (Secreta) es para los procesos o datos más importantes. Cada nivel es un súper conjunto del nivel previo. Por ejemplo, si un sistema está clasificado como clase Confidencial, entonces el sistema debe seguir las directivas de las clases Pública, Interna y Confidencial. Si un sistema contiene datos de más de una clase sensitiva, debe ser clasificado de acuerdo a la necesidad de los datos más confidenciales en el sistema.

Información Pública:

Los datos en estos sistemas podrían ser públicos sin implicaciones para la institución (es decir, los datos no son confidenciales). La integridad de los datos no es vital. La pérdida del servicio debido a ataques maliciosos es un riesgo aceptable.

Información Interna:

El acceso externo a estos datos debe ser prevenido, pero si estos datos se harían públicos, las consecuencias no son críticas. El acceso interno es selectivo. La integridad de los datos es importante pero no vital. Ejemplos de este tipo de datos se encuentra en los grupos de desarrollo (donde están presentes datos irreales), ciertos datos de clientes, documentos de trabajo “normales”, libretas de teléfonos internas.

Información Confidencial:

Los datos de esta clase son confidenciales dentro de la institución y protegidos del acceso externo. Si dichos datos fueran a ser accesados por personas no autorizadas, podrían afectar la eficacia operacional de la institución, causar una importante perdida financiera o causar una disminución notable en la confidencia del cliente. La integridad de los datos es vital. Ejemplos: salarios, datos personales, datos contables, datos de afiliados y jubilados, proyectos sensitivos y contratos confidenciales. Los centros de datos deben mantener este nivel de seguridad.

Información Secreta:

El acceso no autorizado a estos datos, interno ó externo podría ser crítico a la institución. La integridad de los datos es vital. El número de personas con acceso a estos datos debería ser muy pequeño. Deben reglas muy estrictas en el uso de estos datos.

5.3.4 POLÍTICAS DE SEGURIDAD DEL PERSONAL.

5.3.4.1 Ética.

No está permitido a los usuarios lo siguiente:

- Compartir cuentas o claves con amigos, familiares o compañeros de trabajo
- Ejecutar programas de chequeo de claves en el archivo de claves del sistema,
- Ejecutar programas husmeadores (sniffers) de red.
- Romper seguridades y acceder a otras cuentas.
- Interrumpir el servicio.
- Abusar de los recursos del sistema.
- Hacer mal uso del correo electrónico.

- Examinar los archivos de otros usuarios a no ser que le sea permitido por parte del propietario del archivo.
- Descargar archivos binarios desde el PC.
- Copiar software no licenciado o permitir a otros usuarios copiar software no licenciado.

5.3.4.2 Políticas de Claves.

La identidad de los usuarios en los sistemas está definida por la combinación del nombre de usuario y de la clave. El adoptar una buena política de claves es la barrera más importante para el acceso no autorizado en los sistemas actuales.

Las claves deben cumplir los siguientes requerimientos:

- Tener una longitud mínima de 8 caracteres.
- Tener al menos un carácter numérico, un carácter alfabético.
- Puede ser una combinación de caracteres numéricos y alfabéticos.
- Debe ser fácil de recordar (no necesita escribirlo)
- Debe ser fácil de digitar rápidamente, (pero dificultar a un observador).
- Deben ser validados por una rutina de verificación. La rutina de verificación debe validar que la clave cumpla con los requerimientos mencionados.

En la definición de las claves evitar el uso de:

- Nombres como: esposa, padre, canción, amigo, mes, día, pueblo, mascota.
- Número de: matricula del carro, teléfono.
- Palabras del diccionario común.
- Una serie de letras o números idénticos.
- Secuencias del teclado obvias.
- Alguno de los casos anteriores en inverso o con un número antes o después.

Para la definición de claves se sugiere:

- Escoger una línea ó dos de una canción, poema o cualquier párrafo y usar solo las primeras letras.
- Inventar un acrónimo (siglas).

Para asegurar la privacidad de las claves, tomar en cuenta las siguientes guías:

- No escribirlo en un lugar visible, o revelarlo por el correo electrónico.
- No utilizar claves por defecto.
- No dar su clave a otra persona.
- No compartir la clave del administrador.
- Informar a los usuarios en detalle del éxito o el peligro de que su clave sea revelado. Un usuario bien educado es la mejor manera de asegurar buenas opciones de claves.
- Las claves por defecto definidos por los fabricantes deben ser cambiados antes de que el sistema sea utilizado.
- La clave de acuerdo a su nivel de sensibilidad está clasificado como información secreta.
- Las claves deben ser almacenados en una forma encriptada. La encriptación debe ser sólida, que resista la desencripción por fuerza bruta.
- La clave no debería ser desplegada durante su ingreso, ni debería mostrarse un “*” por cada caractér.
- Debe evitarse a toda costa embeber la clave no encriptada en el software. Así mismo, la clave encriptada no debe estar embebido dentro del software tanto cuanto sea posible.
- El sistema debe chequear el contenido de la clave de acuerdo a las reglas definidas previamente, antes de aceptar la clave.
- Un usuario no debería ser capaz de cambiar la clave de otros usuarios, solo una cuenta administrador puede cambiar otras claves.

- Cuando se utilizan cuentas especiales para aplicaciones (por ejemplo, Oracle bajo UNIX), sus claves deberían ser bloqueadas para prevenir un logón interactivo.
- Forzar el cambio de la clave en el primer login del usuario, si es posible.
- Si es posible, proveer una generación automática de claves (para ayudar al usuario).
- Proveer un proceso para que el usuario pueda cambiar su clave en intervalos regulares. Este proceso debe considerar un nivel adicional de autenticación del usuario.
- Proveer un proceso que permita generar una nueva clave al usuario en caso de olvidos de su clave, de modo similar a cuando ingresa por primera vez.

En el tiempo de vida de las claves considerar:

- El tiempo máximo de vigencia para las claves es de 1 año. El usuario debe tener un período de gracia de 5 días de tal forma que en éste lapso de tiempo el usuario pueda cambiar su clave. Si no lo hace, entonces su cuenta expirará.

5.3.4.3 Políticas Generales de Software.

- El software de dominio público se evitará en los sistemas de información clasificada como confidencial. Sin embargo, cuando sea necesario, solo será permitido luego de que el software esté en uso general por al menos un año en sistemas comparables en otras (bien conocidas y confiables) Instituciones y el software ha sido rigurosamente probado en un ambiente protegido.
- El software de dominio público puede usarse en los sistemas de información clasificada como pública o interna, si el administrador del sistema responsable por la instalación está convencido de la integridad del autor o de las fuentes.
- No debe utilizarse software no licenciado.
- No se permiten programas de juegos en las estaciones de trabajo de los usuarios.

5.3.4.4 Redes.

Información confidencial:

- Los datos confidenciales transmitidos sobre redes públicas deben ser encriptados.

Conexión a redes:

- Un usuario no puede conectar una máquina a cualquier red excepto la LAN institucional.
- El acceso a redes externas (públicas y privadas) debe hacerse a través de un firewall. Todos los firewalls deberán ser instalados y mantenidos por el área de seguridad institucional.

5.3.4.5 Módems.

- Los usuarios no deben tener módems en sus máquinas.
- El acceso vía módem a la LAN institucional es permitido sólo para ciertos usuarios. Todos los accesos vía módem deberán hacerse vía servidores seguros con mecanismos de clave de una sola vez.

5.3.4.6 Correo Electrónico.

- Los usuarios deben estar al tanto de que los sistemas de correo electrónico convencionales a menudo no garantizan privacidad o prueba de origen ó recepción. En muchos sistemas el administrador del sistema puede leer todos los correos electrónicos.
- La información clasificada como interna puede enviarse dentro de la compañía sin encripción. La información clasificada como confidencial debe ser

encriptada. La información clasificada como secreta no puede ser transmitida vía correo electrónico.

- Solo la información pública y la información específicamente orientada para proyectos con entidades externas puede ser enviada por correo electrónico, fuera de la institución.
- Los usuarios deben estar al tanto de los riesgos de abrir documentos con macros, archivos postscript, y programas de instalación recibidos vía correo electrónico.

- Debe considerarse un esquema que permita la autenticación del emisor/receptor de información clasificada como confidencial. Por ejemplo, uso de firmas digitales.

5.3.4.7 Internet.

La conexión al Internet es casi inevitable en el ambiente de hoy, especialmente para los departamentos de investigación. Debido a su carencia de estructura y controles, el Internet ofrece muchos riesgos tales como:

- Revelación de información confidencial.
- La red institucional puede ser penetrada por hackers desde el Internet.
- La información puede ser cambiada o borrada.
- El acceso a los sistemas podría ser negado debido a una sobrecarga del sistema.
- Si los usuarios están permitidos tener acceso al Internet, ellos deben estar al tanto de los riesgos involucrados y la política institucional en cuanto a consideraciones de uso del Internet.
- Todos los accesos hacia el Internet deben hacerse sobre gateways de la institución que hayan sido certificados según la política de seguridad institucional.
- Deben tener acceso al Internet: administradores, gerentes, técnicos y profesionales.

- Los usuarios internos de la institución tiene permitido el acceso al correo electrónico por Internet.
- No se permite el acceso a Internet desde servidores de datos que contienen información clasificada como confidencial.
- El software cliente de Internet permitido es Firefox.
- No usar el acceso a Internet para visualizar o descargar material pornográfico, descargar software peligroso o no licenciado, uso privado excesivo, etc.

5.3.4.8 Laptops y Computadores Portables.

Los computadores portátiles permiten al personal amentar su productividad. Ellos ofrecen flexibilidad para acceder a información en cualquier sitio; pero, desde el punto de vista de seguridad pueden crear riesgos en la divulgación ó robo de información, y quizás ofrecen un punto de acceso no autorizado a la red institucional.

Algunas consideraciones a tener en cuenta son:

- Educar a los usuarios respecto del riesgo de usar laptops.
- Proteger con claves los documentos creados con aplicaciones de oficina como Word no es una protección contra un agresor.
- Los discos removibles permiten al usuario proteger fácilmente la información más importante llevándolos en su bolsillo. Del mismo modo, hacen más fácil robar información.

Las políticas a tomar en cuenta son:

- Las laptops deben ser preparadas e instaladas por personal profesional.
- Si es posible instalar un programa de encripción de archivos el cual provea una encripción fuerte y sea fácil de usar. Un programa de

encripción de discos es una alternativa, pero puede requerir mas carga administrativa y afectar el desempeño del equipo.

Los usuarios son responsables por sus laptops fuera de las oficinas de la institución.

- Deberían usarse mecanismos automáticos de bloqueo de las pantallas y claves de arranque siempre que sea posible.
- Instalar programas antivirus siempre activos en las computadoras.
- Los datos clasificados como confidenciales no deberían llevarse en laptops, a menos que estén encriptados.
- Apagar la computadora cuando no esté en uso.
- Nunca guarde claves en la laptop los cuales permitan acceso a los sistemas de la red institucional.

5.3.5 POLITICAS DE SEGURIDAD DE COMPUTADORES Y REDES

5.3.5.1 Políticas de Administración del Sistema.

El administrador tiene que asegurar que los sistemas estén disponibles cuando sea necesario, que la información confidencial esté sólo disponible para aquellos accesos autorizados y que la información no esté sujeta a cambios no autorizados.

La dirección informática de la institución es responsable de actualizar las políticas de administración del sistema.

Solo el usuario administrador está autorizado para otorgar accesos y aprobar su uso.

No se permite a los usuarios acceso como administrador a sus estaciones de trabajo.

El directorio actual nunca debe estar en la ruta de búsqueda de directorios para usuarios administrativos (prevención de caballos de Troya).

5.3.5.2 Seguridad Física.

Una política de seguridad física debe detallar las medidas a tomar para proteger los edificios y que considere: desastres (inundaciones, incendios, explosiones, terremotos, apagones), robos, control del acceso, seguridades del centro de cómputo y los gabinetes del cableado.

Deben definirse las siguientes zonas:

Zona 1: Áreas abiertas al público.
Zona 2: Áreas no abiertas al público, abiertas sólo para el personal de la institución.
Zona 3: Áreas protegidas. Solamente accesibles con una identificación, acceso estrictamente restringido.

- El personal administrativo de la red es responsable por la destrucción de cintas y discos defectuosos o viejos.
- Se deben cumplir las siguientes directivas para el centro de cómputo (Zona 3):

    a) Todos los dispositivos del centro de cómputo deben estar limpios y etiquetados.
    b) El cableado debe estar limpio, bien arreglado y etiquetado, tal que las conexiones no puedan ser accidentalmente desconectadas o rotas.
    c) Debe haber un diagrama con la ubicación de los equipos y dispositivos instalados en el centro de cómputo.
    d) El transporte de los medios electrónicos (cintas, respaldos, discos) debe hacerse considerando medidas que eviten dañarlos.

- Todos los usuarios deben ser autentificados.
- Los usuarios deben ser capaces de modificar los datos que les pertenecen a ellos.
- Los usuarios deberían estar prevenidos de borrar los archivos de otros usuarios en directorios compartidos.
- Se permite el acceso al sistema como administrador privilegiado (root) solo vía consola o desde las estaciones que él defina.
- Se debe controlar el acceso de los usuarios a todos los objetos en el sistema (archivos, impresoras, dispositivos, bases de datos, comandos, aplicaciones, etc.).
- Los usuarios no deberían ser capaces de conocer el acceso otorgado a otros usuarios.
- Identificar la información de acuerdo a la clasificación de sensitividad previamente definida.
- El sistema debe proveer un control de acceso obligatorio.
- Sólo el administrador debe tener la capacidad de conectarse a los recursos del sistema en modo privilegiado para realizar tareas administrativas.

5.3.5.3 Políticas de Ingreso a los Sistemas.

El principio básico a cumplir es dar al usuario final el mínimo de privilegios y el mínimo tiempo necesario para realizar su trabajo.

- Las cuentas de usuario deben existir sólo para el personal autorizado.
- Cada usuario debe ser identificado por un nombre y pertenecer a un grupo dentro del sistema operativo o a un rol dentro de la base de datos.
- Los usuarios y grupos deben ser administrados por un usuario administrador no por los usuarios en sí.
- No se debe permitir cuentas a las cuales accese un grupo de usuarios.
- Cada usuario debe tener solamente una cuenta sobre el sistema operativo.

- Las cuentas como usuario huésped no son permitidas.
- Cuando un usuario interno es transferido o termina su empleo, su cuenta debe ser eliminada inmediatamente. Los procedimientos administrativos deben contemplar esta situación para que el personal administrativo informe a los administradores del sistema sobre éste particular.
- Un programa de bloqueo de pantalla debería activarse luego de 15 minutos de inactividad y requerir una clave de protección.
- Los usuarios deberían ser informados de acciones que violan la seguridad. Similarmente ellos deben informar a su administrador de seguridades si ellos sospechan de una violación de la seguridad.
- Cuando un usuario se conecte al sistema debe desplegarse:
    1. Información sobre implicaciones legales del abuso del sistema por parte del usuario.
    2. El tiempo del último ingreso exitoso o no (El usuario debería chequear que esta información esté correcta).
    - Los ingresos al sistema para usuarios internos deben ser habilitados solo entre las 8:00 h y las 18:00 h.
    - Si un usuario ingresa mal un nombre de usuario o clave, el mensaje de error debería ser el mismo para ambos casos. Un posible intruso no debería ser informado si una cuenta de usuario es válida o no.
    - Especificar como máximo una sesión simultánea por usuario.
    - Debe proveerse un mecanismo que usando la dirección origen permita restringir el acceso de los usuarios a los sistemas.
    - Cuando un usuario excede 3 intentos de conexión en un intervalo menor o igual a treinta minutos, y no logra ingresar al sistema, su cuenta debe automáticamente ser bloqueada por un lapso de 2 horas.

5.3.5.4 Auditoria.

- Una Auditaría de seguridad debe ser corrida regularmente sobre el sistema. Su periodicidad dependerá del nivel de sensitividad de la información.

- Los nuevos servidores deben ser instalados y preparados por el administrador del sistema. Ellos deberían ser auditados y certificados a uno de los niveles de sensitividad por el equipo de seguridad. Si todas las directivas no pueden ser implementadas por un sistema en particular (debido a limitaciones del sistema operativo, por ejemplo) aquellas excepciones deben ser claramente documentadas en la certificación.

5.3.5.5 Contabilización y Auditoria.

- El registro de las pistas de auditoria y programas ó utilitarios deben ser protegidos. Ellos deben ser accesibles sólo por el personal de seguridad.
- Los registros de auditoria no deben contener claves.
- Las actividades del administrador del sistema deberían ser anotadas en los registros de auditoria.
- Los intentos de ingreso fallidos hacia el sistema deberían ser anotadas en un registro de auditaría y ser notificados al administrador.
- Se debe especificar una auditaría por usuarios o por recursos del sistema.
- Cada entrada dentro del registro de auditaría debe contener al menos: nombre de usuario, fecha y hora, identificador del equipo, nivel de error (para éxito o falla) y descripción del evento.
- Los registros de auditaría deben ser mantenidos sobre un dispositivo de almacenamiento que sea solamente de lectura.
- Los registros de auditaría deben ser archivados en una máquina segura, no almacenar los registros sobre sistemas de archivos compartidos.
- Todas las máquinas deben tener sus relojes sincronizados para garantizar la validez de la auditaría en el momento de estampar la hora en los registros.
- El tamaño del registro (log) de las pistas de Auditaría no debe causar una interrupción o degradación del servicio que presta el sistema. Este tamaño debe fijarlo el administrador del sistema así como su frecuencia de reutilización.

5.3.5.6 Confiabilidad del Servicio.

Políticas de respaldos y recuperación:

- Los respaldos deben hacerse regularmente y copias de estos, deben almacenarse en otra instalación.
- Los respaldos de información confidencial deben almacenarse en lugares con acceso restringido. Todos los respaldos deben ser contabilizados. Las cintas viejas deben ser destruidas.

Por cada sistema o grupo de sistemas, se debe:

- Hacer respaldos incrementales y respaldos totales al menos cada 15 días.
- Realizar con una frecuencia diaria para el incremental y al menos cada quince días para el total. El responsable por chequear su correcta operación será el Operador del Sistema.
- Detallar y documentar los utilitarios que se usarán para restaurar los datos para todas las aplicaciones. Ejemplo: sistema operativo, mecanismos de restauración de la base de datos.
- Describir y documentar los procedimientos para restaurar el sistema operativo después de fallas serias en los discos u otros componentes de hardware.
- Documentar el tiempo de restauración esperado para varios escenarios de desastre.
- Probar las políticas de restauración regularmente. (Por ejemplo, cada año).

Administración de cambios (instalaciones o actualizaciones de software / hardware)

- Solo los administradores del sistema deben instalar o actualizar el software en los servidores.
- Los usuarios no pueden instalar software en las estaciones de trabajo.

- Los sistemas deben ser instalados de modo limpio de acuerdo a las instrucciones de los proveedores.
- Mantener en cada servidor un archivo de cambios, que registre todos los cambios que se realicen en el sistema.
- Se sugiere que como mínimo, un archivo de texto simple sea creado que contenga: fecha, nombre del administrador, archivos cambiados y razón ó comentario.
- Las instalaciones del sistema operativo deben incluir la instalación de todos los parches de software recomendados.
- Identificar todas las máquinas que se instalen mediante etiquetas que se adhieran en forma externa a cada uno de los equipos.
- Las etiquetas deben incluir por ejemplo: nombre del equipo, fabricante ó modelo de la máquina, dirección IP, dirección MAC, identificador del nodo en el cableado (si la topología de la red lo permite), fecha de vencimiento de la garantía y número de teléfono de la línea de ayuda o seguridad, nombre del servidor al que se conecta el equipo.
- Aplicar solo los parches del proveedor original de software.
- Los parches descargados desde redes públicas (Por ejemplo, Internet) deben ser chequeados por integridad usando un mecanismo de hashing (Por ejemplo MD5). Los parches se usarán en cuanto estén disponibles y deberán ser pre-probados en un ambiente de pruebas (por al menos unas pocas semanas si es posible) antes de ser aplicados a los sistemas de producción.

5.3.5.7 Políticas de Redes y Sistemas Distribuidos.

Documentación: La configuración de la red debe estar documentada.

Identificación y Autenticación:

- Debería ser posible identificar y autenticar cualquier sujeto en la red institucional.

- Si es posible, debe haber un solo mecanismo de ingreso para los usuarios de múltiples aplicaciones y sistemas, evitando múltiples nombres de usuarios y claves.

Contabilización y auditoria:

- Auditar las acciones de los usuarios. Los usuarios deben cumplir con la política de red.
- Llevar registros de auditaría de la actividad de los nodos de la red más importantes. Estos registros deben ser regularmente analizados para detectar brechas de seguridad.

Control de Acceso:

- Solo se permiten habilitar los siguientes servicios de red: SMTP, POP3, HTTP, SSH, SFTP, HTTPS. Configurar los servicios de red de modo restrictivo e instalar todos los parches de software relacionados.
- Etiquetar en forma externa las redes disponibles como de acceso abierto, acceso restringido o acceso altamente restringido, de modo que los usuarios o propietarios de los datos estén al tanto de la protección ofrecida.
- Por ejemplo si una LAN está etiquetada como de acceso abierto y se necesita transmitir información confidencial sobre esta LAN, entonces serán necesarias medidas adicionales como encripción a nivel de aplicaciones para corregir la deficiencia de la seguridad de la red.
- En las redes de acceso restringido, el cableado no debe pasar a través de redes públicas, su conducción debe ser protegida y los puntos de conexión deben estar disponibles sólo a las personas autorizadas. Si el cableado es proporcionado por terceros, debe ser inspeccionado y certificado.

Integridad:

- Debe chequearse regularmente la exactitud e integridad de datos de los nodos de la red más importantes.

Intercambio de datos:

- La información confidencial debe ser sólo transmitida a través de mecanismos de transporte certificados.
- Por ejemplo, los sistemas de correo electrónico usados para datos confidenciales deben ser certificados por la administración de seguridad.
- La información de las sesiones de ingreso (Por ejemplo, nombre de usuario y clave) no deben enviarse sobre la red en forma clara.
- Los servicios de red entre hosts deben autenticarse uno a otro.
- Proteger las redes contra programas sniffers) tales como: snoop, etherfind, tcpdump, iptrace etc. Estos programas no deben estar disponibles a los usuarios.
- Dividir las redes en subredes y deshabilitar los puntos de conexión de red no usados.
- Encriptar los datos clasificados como confidenciales antes de su transmisión tanto en las redes internas como en las públicas.
- Cuando la información está siendo transmitida (enviada o recibida), la identidad de quien envía o recibe debe ser unida la información y chequeada por los varios componentes responsables por la transmisión.
- No enviar datos clasificados como confidenciales a usuarios no autorizados o a sistemas con una clasificación de sensitividad más baja.
- En ciertas aplicaciones (Por ejemplo, correo electrónico), deben existir mecanismos para probar que el emisor/receptor hicieron realmente la transmisión/recepción de los datos (Prueba de origen/recepción).

Confiabilidad del Servicio y Disponibilidad:

- La red se requiere disponible las 24 horas del día, 5 días a la semana. El horario de mantenimiento será el día viernes de 18:00 a 22:00 horas o fines de semana
- Monitorear los errores y problemas de desempeño de la red. Tomar acciones preventivas antes de que ocurran interrupciones serias de la red.

- Administración de cambios: Las actualizaciones y los cambios de configuración deben ser registrados y llevados a cabo de acuerdo a procesos de calidad.
- Una etiqueta que contenga la siguiente información debe ser pegada en todas las máquinas durante la instalación: Nombre del equipo, Fabricante Modelo de la máquina, dirección IP, dirección MAC, identificador del nodo en el cableado (si la topología de la red lo permite), fecha de vencimiento de la garantía y número de teléfono de la línea de ayuda o seguridad.

Políticas de acceso remoto: Interfaces con redes externas:

- La red institucional no debe interconectarse con otras redes (Dial-up, Internet, redes de proveedores, redes telefónicas, redes de clientes, etc.) si esto crea una brecha de seguridad. El acceso desde redes externas debe hacerse a través un firewall.
- El firewall debe tener políticas de seguridad y debe ser regularmente monitoreado y auditado.

5.3.5.8 Firewall para Internet.

El Internet es una importante herramienta para compartir y buscar información. Todos los accesos al Internet desde la red de la institución deben hacerse a través de un Firewall.

Confiabilidad:

- La política del firewall y su configuración deben ser documentadas correctamente.
- Los equipos de firewall deben estar sujetos a un monitoreo regular y a una auditaría periódica.

Identificación y Autenticación:

- Las conexiones de los usuarios que acceden desde el Internet deben usar un sistema de autenticación robusto como claves de una sola vez.
- Las cuentas del administrador deben usar además sesiones de login encriptadas.

Auditaría:

- Instalar los equipos de firewall de modo seguro. Todos los servicios del sistema operativo no necesarios deben detenerse.
- Mantener los registros de auditaría del firewall (si es posible en un servidor dedicado y sobre medios write-once).
- Mantener registros históricos de todas las auditorías de seguridad.
- Usar un software de auditaría que generen alarmas para los errores críticos.
- Examinar los registros de auditaría una vez cada semana.
- Deben haber y estar disponibles estadísticas de uso.

Control de Acceso:

- Todos los accesos al Internet desde la red de la institución deben hacerse sobre proxies localizadas en un firewall.
- Los servicios de configuración por defecto están prohibidos.
- Todos los usuarios están permitidos a intercambiar correo electrónico interno.
- Los usuarios de soporte técnico informático están permitidos a usar WWW y FTP (sobre proxies). El resto de usuarios requieren autorización.
- Las áreas de investigación que requieren acceso completo al Internet para probar nuevos servicios no deben instalar estos servicios en la red institucional, sino en una red separada, fuera del firewall.
- Ningún usuario debe ser capaz de ingresar directamente a los equipos de firewall.
- Debe prevenirse donde sea posible el acceso por Internet a material ilícito.

Integridad:

- Debe chequearse regularmente (cada mes) la exactitud e integridad de los archivos localizados en los equipos de firewall.

Intercambio de datos:

- Todas las sesiones de usuario al equipo de firewall deben hacerse usando un acceso encriptado o claves de una sola vez.

Confiabilidad del servicio:

- El firewall debe estar disponible 7x24h, horario de mantenimiento será el día Viernes de 18:00 a 22:00 horas o fines de semana.
- Administración de cambios: Las actualizaciones y cambios de configuración deben ser registradas y llevadas a cabo de acuerdo a procesos de calidad.
- Deben disparase alertas si los procesos o servicios importantes hacen crash.
- Los servicios importantes (tales como WWW y proxy) debe ser configurados para alta disponibilidad.
- Deben hacerse respaldos regulares de datos necesarios (Por ejemplo, archivos de configuración).

5.3.5.9 Interfaces a otras redes.

Interfaces con redes externas:

- Debe existir un documento de políticas para cada interfase, el cual detalle que información va a ser transferida, como se hará la transferencia, y como se adhieren a las políticas de seguridad de la institución.

- Proteger las interfaces con otras redes por un firewall y sujetarlas a un monitoreo y auditaría regulares.
- Establecer acuerdos de niveles de servicio para comunicación con las redes externas.
- Firmar un acuerdo de privacidad con la entidad externa, el cual asegure que ninguno de los detalles de la interfase, ni los datos accesibles por la interfase, pueden ser revelados a terceras partes.
- Proveer esquemas que permitan la autenticación de entidades externas (usuarios especiales). Por ejemplo, uso de certificados digitales.

5.3.5.10 Políticas de Desarrollo de Software.

La seguridad debería ser una parte integral de los nuevos sistemas. Cuando se diseñan los requerimientos funcionales, deberían formularse requerimientos de seguridad que correspondan a la sensitividad y disponibilidad de los datos a ser manejados por el sistema.

Guías Generales:

- Separar los ambientes y datos de desarrollo y producción.
- Obligar a que la seguridad sea una parte integral del desarrollo de aplicaciones.
- Los datos de prueba no deben contener información confidencial.
- Usar un lenguaje seguro (Por ejemplo, Java en lugar de C).
- Usar metodologías de desarrollo bajo estándares ISO9000.
- Todos los nuevos sistemas deben ser aprobados por el área de seguridad de la información.

Guías de Producción:

- Se debe entregar con la aplicación la siguiente documentación: Manuales de Operación, Instalación, Administración, Seguridad, Usuario.

- Para que una aplicación entre a producción debe pasar exitosamente un plan de pruebas.

5.3.6 EJECUCION.

Los usuarios que no se adhieran a estas políticas deben ser advertidos de sus consecuencias y debe ser informada a la línea de administración correspondiente. Un usuario que aún siendo advertido continua ignorando estas políticas puede ser removido de su función.

CAPÍTULO 6

ANALISIS DE COSTOS

6.1 ANÁLISIS DE COSTOS.

En base a la solución planteada en el capítulo 3 para la implementación de la red de datos del Seguro de Pensiones, se ha determinado la adquisición de componentes de hardware los cuales detallamos por cada dependencia, es necesario anotar que los costos aquí mencionados se ha tomado en referencia al costo promedio de las consultas realizadas en el mercado.

6.2 PRESUPUESTO POR DEPENDENCIA.

Cuadro 6.1 Dependencia: Dirección de Pensiones.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Ruteador	1	$ 4.600,00	$ 4.600,00
Switch de Core	2	$ 7.000,00	$ 14.000,00
Switch de borde con Gbic 24puertos	1	$ 6.500,00	$ 6.500,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 6.480,00
Cableado estructurado y accesorios	11	$ 160,00	$ 1.760,00
Red eléctrica y accesorios	11	$ 190,00	$ 2.090,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	8	$ 1.100,00	$ 8.800,00
Impresora Láser tipo1	2	$ 450,00	$ 900,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00

Equipo / componente	Cantidad	Costo Unitario	Costo total
Backbone de fibra óptica	1	$ 1.333,00	$ 1.333,00
UPS de 8KVA	1	$ 4.400,00	$ 4.400,00
COSTO TOTAL			**$ 57.563,00**

Dado que la Dirección de Pensiones y la Subdirección de Contabilidad y Control Presupuestario se encuentran en el mismo edificio, se compartirán los componentes: ruteador, servidor de red, rack de la sala de equipos y UPS, por esta razón, no son tomados en cuenta en la tabla de costos de la Subdirección de Contabilidad y Control Presupuestario. Ver ANEXO V cálculo de costos de Backbone de Fibra Óptica.

Cuadro 6.2 Dependencia: Subdirección de Contabilidad y Control Presupuestario.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Switch de borde con Gbic 24puertos	1	$ 6.500,00	$ 6.500,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 975,00
Cableado estructurado y accesorios	7	$ 160,00	$ 1.120,00
Red eléctrica y accesorios	7	$ 190,00	$ 1.330,00
Computadoras Personales	5	$ 1.100,00	$ 5.500,00
Impresora Láser tipo2	1	$ 1.500,00	$ 1.500,00
COSTO TOTAL			**$ 16.925,00**

Cuadro 6.3 Dependencia: Subdirecciones de Pensiones del Azuay.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	4600	$ 4.600,00
Switch de borde para Stack	1	4900	$ 4.900,00

Equipo / componente	Cantidad	Costo Unitario	Costo total
24puertos			
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y accesorios	25	160	$ 4.000,00
Red eléctrica y accesorios	21	190	$ 3.990,00
Servidor de red Pequeño	1	5000	$ 5.000,00
Computadoras Personales	20	1100	$ 22.000,00
Impresora Láser tipo1	2	450	$ 900,00
Impresora Láser tipo2	2	1500	$ 3.000,00
Rack de la Sala de equipos	1	1700	$ 1.700,00
UPS de 8KVA	1	4400	$ 4.400,00
COSTO TOTAL			**$ 55.915,00**

Cuadro 6.4 Dependencia: Subdirecciones de Pensiones de Pichincha.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	4600	$ 4.600,00
Switch de Core	2	7000	$ 14.000,00
Switch de borde con Gbic 48puertos	1	10490	$ 10.490,00
Switch de borde con Gbic 24puertos	2	6500	$ 13.000,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 3.313,50
Cableado estructurado y accesorios	83	160	$ 13.280,00
Red eléctrica y accesorios	86	190	$ 16.340,00
Servidor de red Mediano	1	10000	$ 10.000,00
Computadoras Personales	69	1100	$ 75.900,00

Equipo / componente	Cantidad	Costo Unitario	Costo total
Impresora Láser tipo1	10	450	$ 4.500,00
Impresora Láser tipo2	3	1500	$ 4.500,00
Backbone de fibra óptica	1	2366	$ 2.366,00
Rack de la Sala de equipos	1	1700	$ 1.700,00
UPS de 25KVA	1	13750	$ 13.750,00
COSTO TOTAL			**$ 187.739,50**

Ver ANEXO V, cálculo de costos de Backbone de Fibra Óptica.

Cuadro 6.5 Dependencia: Subdirección de Pensiones del Guayas.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de Core	2	$ 7.000,00	$ 14.000,00
Switch de borde con Gbic 48puertos	1	$ 10.490,00	$ 10.490,00
Switch de borde con Gbic 24puertos	2	$ 6.500,00	$ 13.000,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 3.313,50
Cableado estructurado y accesorios	83	$ 160,00	$ 13.280,00
Red eléctrica y accesorios	86	$ 190,00	$ 16.340,00
Servidor de red Mediano	1	$ 10.000,00	$ 10.000,00
Computadoras Personales	69	$ 1.100,00	$ 75.900,00
Impresora Láser tipo1	10	$ 450,00	$ 4.500,00
Impresora Láser tipo2	3	$ 1.500,00	$ 4.500,00
Backbone de fibra óptica	1	$ 2.346,00	$ 2.346,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 25KVA	1	$ 13.750,00	$ 13.750,00

Equipo / componente	Cantidad	Costo Unitario	Costo total
COSTO TOTAL			**$ 187.719,50**

Ver ANEXO V cálculo de costos de Backbone de Fibra Óptica.

Cuadro 6.6 Dependencia: Unidad Provincial de Imbabura.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de borde para Stack 24puertos	1	$ 4.900,00	$ 4.900,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y accesorios	17	$ 160,00	$ 2.720,00
Red eléctrica y accesorios	17	$ 190,00	$ 3.230,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	13	$ 1.100,00	$ 14.300,00
Impresora Láser tipo1	3	$ 450,00	$ 1.350,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 6KVA	1	$ 3.300,00	$ 3.300,00
COSTO TOTAL			**$ 42.525,00**

Cuadro 6.7 Dependencia: Unidad Provincial de Tungurahua.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de borde para Stack 24puertos	1	$ 4.900,00	$ 4.900,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y	16	$ 160,00	$ 2.560,00

Equipo / componente	Cantidad	Costo Unitario	Costo total
accesorios			
Red eléctrica y accesorios	16	$ 190,00	$ 3.040,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	12	$ 1.100,00	$ 13.200,00
Impresora Láser tipo1	3	$ 450,00	$ 1.350,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 5KVA	1	$ 2.750,00	$ 2.750,00
COSTO TOTAL			**$ 40.525,00**

Cuadro 6.8 Dependencia: Unidad Provincial de Chimborazo.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de borde para Stack 24puertos	1	$ 4.900,00	$ 4.900,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y accesorios	17	$ 160,00	$ 2.720,00
Red eléctrica y accesorios	17	$ 190,00	$ 3.230,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	13	$ 1.100,00	$ 14.300,00
Impresora Láser tipo1	3	$ 450,00	$ 1.350,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 6KVA	1	$ 3.300,00	$ 3.300,00
COSTO TOTAL			**$ 42.525,00**

Cuadro 6.9 Dependencia: Unidad Provincial de Loja.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de borde para Stack 24puertos	1	$ 4.900,00	$ 4.900,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y accesorios	17	$ 160,00	$ 2.720,00
Red eléctrica y accesorios	17	$ 190,00	$ 3.230,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	13	$ 1.100,00	$ 14.300,00
Impresora Láser tipo1	3	$ 450,00	$ 1.350,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 6KVA	1	$ 3.300,00	$ 3.300,00
COSTO TOTAL			**$ 42.525,00**

Cuadro 6.10 Dependencia: Unidad Provincial de Manabí.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de borde para Stack 24puertos	1	$ 4.900,00	$ 4.900,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y accesorios	21	$ 160,00	$ 3.360,00
Red eléctrica y accesorios	21	$ 190,00	$ 3.990,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	16	$ 1.100,00	$ 17.600,00
Impresora Láser tipo1	4	$ 450,00	$ 1.800,00

Equipo / componente	Cantidad	Costo Unitario	Costo total
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 6KVA	1	$ 3.300,00	$ 3.300,00
COSTO TOTAL			**$ 47.675,00**

Cuadro 6.11 Dependencia: Unidad Provincial de El Oro.

Equipo / componente	Cantidad	Costo Unitario	Costo total
Router	1	$ 4.600,00	$ 4.600,00
Switch de borde para Stack 24puertos	1	$ 4.900,00	$ 4.900,00
Servicio de mantenimiento para el switch ofertado	1	15%	$ 1.425,00
Cableado estructurado y accesorios	16	$ 160,00	$ 2.560,00
Red eléctrica y accesorios	16	$ 190,00	$ 3.040,00
Servidor de red Pequeño	1	$ 5.000,00	$ 5.000,00
Computadoras Personales	12	$ 1.100,00	$ 13.200,00
Impresora Láser tipo1	3	$ 450,00	$ 1.350,00
Rack de la Sala de equipos	1	$ 1.700,00	$ 1.700,00
UPS de 5KVA	1	$ 2.750,00	$ 2.750,00
COSTO TOTAL			**$ 40.525,00**

*6.*3 PRESUPUESTO CONSOLIDADO DE DEPENDENCIAS.

Una vez realizado los cuadros del análisis de costos de cada dependencia, procedemos a realizar un presupuesto consolidado de todas las dependencias.

Cuadro 6.12 Presupuesto Consolidado de las Dependencias.

DEPENDENCIA	TOTAL
DIRECCIÓN DE PENSIONES	$ 57.563,00
SUBDIRECCION DE CONTABILIDAD Y CONTROL PRESUPUESTARIO	$ 16.925,00
SUBDIRECCIONES DE PENSIONES DEL AZUAY	$ 55.915,00
SUBDIRECCION DE PENSIONES DE PICHINCHA	$ 187.739,50
SUBDIRECCION DE PENCIONES DEL GUAYAS	$ 187.719,50
UNIDAD PROVINCIAL DE IMBABURA	$ 42.525,00
UNIDAD PROVINCIAL DE TUNGURAHUA	$ 40.525,00
UNIDAD PROVINCIAL DE CHIMBORAZO	$ 42.525,00
UNIDAD PROVINCIAL DE LOJA	$ 42.525,00
UNIDAD PROVINCIAL DE MANABI	$ 47.675,00
UNIDAD PROVINCIAL DE EL ORO	$ 40.525,00
COSTO TOTAL	**$ 762.162,00**

*6.*4 ANALISIS DE COSTOS DE LOS ENLACES.

Cuadro 6.13 Costos de canales de comunicaciones hacia las diferentes dependencias.

ORIGEN	DESTINO	CAPACIDAD DE CANAL	TIPO DE CANAL	COSTO-INSTALACION	COSTO-SERV
QUITO	GUAYAQUIL	1,5 Mbps.	MPLS	$ 600,00	$ 4.000,00
QUITO	CUENCA	1,5 Mbps.	MPLS	$ 600,00	$ 4.000,00
GUAYAQUIL	CUENCA	1,5 Mbps.	MPLS	$ 600,00	$ 4.000,00
QUITO	SUDIRECCION DE PENSIONES	1.0 Mbps.	Frame Relay	$ 500,00	$ 814,00
QUITO	IBARRA	256 Kbps.	Frame Relay	$ 450,00	$ 700,00
QUITO	TUNGURAHUA	256 Kbps.	Frame Relay	$ 450,00	$ 700,00
QUITO	CHIMBORAZO	256 Kbps.	Frame Relay	$ 450,00	$ 700,00
CUENCA	LOJA	256 Kbps.	Frame Relay	$ 450,00	$ 700,00
GUAYAQUIL	MANABI	256Kbps.	Frame Relay	$ 450,00	$ 700,00
GUAYAQUIL	EL ORO	256Kbps.	Frame Relay	$ 450,00	$ 700,00

El monto total en lo que se refiere a canales de telecomunicaciones está tomado para un rango de tiempo de tres años, pero por tratarse de una entidad del sector público, tenemos que realizar un cálculo anual para efectos de presupuesto.

Costo-Servicio es el costo del servicio Mensual.

Cuadro 6.14 Costo total por canales de comunicación proyectado a tres años.

ORIGEN	DESTINO	COSTO-SERVICIO	FACTOR TIEMPO	COSTO TOTAL PARA 3 AÑOS	COSTO TOTAL ANUAL
QUITO	GUAYAQUIL	$ 4.000,00	36	$ 144.000,00	$ 48.000,00
QUITO	CUENCA	$ 4.000,00	36	$ 144.000,00	$ 48.000,00
GUAYAQUIL	CUENCA	$ 4.000,00	36	$ 144.000,00	$ 48.000,00
QUITO	SUDIRECCION DE PENSIONES	$ 814,00	36	$ 29.304,00	$ 9.768,00
QUITO	IBARRA	$ 700,00	36	$ 25.200,00	$ 8.400,00
QUITO	TUNGURAHUA	$ 700,00	36	$ 25.200,00	$ 8.400,00
QUITO	CHIMBORAZO	$ 700,00	36	$ 25.200,00	$ 8.400,00
CUENCA	LOJA	$ 700,00	36	$ 25.200,00	$ 8.400,00
GUAYAQUIL	MANABI	$ 700,00	36	$ 25.200,00	$ 8.400,00
GUAYAQUIL	EL ORO	$ 700,00	36	$ 25.200,00	$ 8.400,00
COSTO TOTAL				**$ 612.504,00**	**$ 204.168,00**

6.5 COSTOS DE LOS EQUIPOS DEL CENTRO DATOS

Cuadro 6.15 Costo de los equipos del Centro de Datos.

EQUIPO / COMPONENTE	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
SERVIDOR DE CORREO ELECTRONICO	2	$ 14.309,00	$ 28.618,00
SERVIDOR DE APLICACIONES	1	$ 40.000,00	$ 40.000,00
SERVIDOR DE BASE DE DATOS	1	$ 40.000,00	$ 40.000,00
SERVIDORES WEB	4	$ 10.041,00	$ 40.164,00
BALANCEADOR DE CARGA	2	$ 10.000,00	$ 20.000,00

EQUIPO / COMPONENTE	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
SERVIDOR DE DNS, NIS	1	$ 10.041,00	$ 10.041,00
STORAGE	1	$ 58.000,00	$ 58.000,00
FIREWALLS	3	$ 8.000,00	$ 24.000,00
SERVIDOR PROXY	1	$ 10.041,00	$ 10.041,00
RUTEADORES	2	$ 5.000,00	$ 10.000,00
COSTO TOTAL			**$ 280.864,00**

6.6 CONSOLIDACION DE COSTOS FIJOS DEL PROYECTO.

En la siguiente tabla realizamos la consolidación de costos fijos que se han tomado en cuenta para el inicio del proyecto.

Cuadro 6.16 Consolidación de costos fijos del proyecto.

DESCRIPCION	COSTO TOTAL
COMPONENTES DE RED DE LAS DEPENDENCIAS	$ 762.162,00
CANALES DE COMUNICACIÓN COSTO INSTALACION	$ 5.000,00
EQUIPOS DEL CENTRO DE DATOS PRINCIPAL	$ 280.864,00
COSTO TOTAL FIJO DEL PROYECTO	**$ 1.048.026,00**

La inversión inicial del proyecto es de $ 1.048.026,00 (Un millón cuarenta y ocho mil, veinte y seis Dólares con 00/100).

6.7 CONSOLIDACION COSTOS DE TELECOMUNICACIONES.

La consolidación de costos de operación de telecomunicaciones, está calculada por el lapso de tres años ya que estas son las recomendaciones establecidas al

interior de la Institución. Sin embargo como se apuntó anteriormente para efectos de presupuesto se lo realiza también para un año.

El presupuesto de telecomunicaciones calculado a tres años es de
$ 612.504,00 (seis cientos, doce mil, quinientos cuatro Dólares con 00/100).

El presupuesto de telecomunicaciones prorrateado por año es de
$ 204.168,00 (Dos cientos, cuatro mil, ciento sesenta y ocho Dólares con 00/100).

Los valores indicados no incluyen IVA.

CAPITULO 7

CONCLUSIONES Y RECOMENDACIONES.

El nivel de desarrollo que en la actualidad ha tenido las tecnologías de la información ha permitido dinamizar inconmensurablemente la sociedad. El acceso a información ubicada en cualquier parte del mundo, la facilidad de difundir información de una manera segura y oportuna, sin barreras ni distancias, han aportado a consolidar ésta era como la era de la información

El mayor activo de una Organización hoy en día es la información, por lo que para que ésta aporte de una manera efectiva al desarrollo organizacional, es necesario tener un adecuado proceso de administración, que cubra las fases de obtención, procesamiento y difusión.

Las fases referidas, para poder ser ejecutadas, demandan de las Organizaciones, infraestructura adecuada, que facilite el análisis de los datos, en complemento se necesita talento humano suficientemente formado, capaz de generar nueva información.

La correcta asimilación de lo anteriormente planteado, contribuye a tener elementos diferenciadores que permiten a una Organización superar con éxito las amenazas que pueden presentarse.

El Seguro de Pensiones del Instituto Ecuatoriano de Seguridad Social, no está ajeno a esta realidad. Modernizarse y asumir adecuadamente los retos del presente, le permitirán trascender y cumplir su misión.

El proceso de modernización que ha emprendido el Seguro de Pensiones, tiene como objetivo superar las dificultades del presente, mismas que le han puesto en condición de retraso.

Uno de los ejes fundamentales del Plan de Modernización, es la Modernización Tecnológica, que mediante la incorporación de tecnología de punta, apoya la gestación de nuevos proceso internos, que faciliten y den orden a las actividades del Seguro de Pensiones. Esto incidirá directamente en la prestación de mejores servicios, orientados a satisfacer las necesidades de los clientes.

Elemento fundamental de todo este proceso es el talento humano que desempeña sus labores dentro del Seguro de Pensiones, quienes están en la obligación de convertirse en agentes de cambio, no existe otra posibilidad.

Para cumplir con las nuevas metas que la Institución plantea al talento humano, éste debe también tener un proceso de evolución, no es posible continuar con las viejas prácticas laborales y de comportamiento organizacional, que no han contribuido en nada al fortalecimiento de la Institución.

La tecnología esta también para contribuir a este proceso, *la tecnología está al servicio del hombre.*

Es en este marco, en el que se plantea la necesidad de contar con sistemas informáticos que faciliten y hagan eficiente, eficaz y oportuna la prestación de servicios. El Seguro de Pensiones desarrolló su sistema informático, columna vertebral de los diferentes servicios que este brinda.

Adicionalmente con el afán de brindar canales alternativos para atención al cliente, se planteó, que el sistema informático debe operar a través de Internet. Dando un punto de contacto nuevo a los usuarios del Seguro de Pensiones.

Con el desarrollo del presente trabajo, se sienta las bases tecnológicas que serán el soporte para que el sistema de Pensiones pueda operar y constituirse en un canal electrónico de prestación de servicios del Seguro de Pensiones.

El diseño de los diferentes componentes, cableado estructurado, redes LAN, redes WAN, centro de datos, así como también la integración de todos ellos, cumple con el objetivo trazado al inicio para la elaboración del presente trabajo.

Los conceptos bajo los cuales se realizó los diseños, apuntan a construir una infraestructura de alta disponibilidad, capaz de soportar altos volúmenes de carga y que permita la puesta en operación de servicios adicionales en el futuro, como son los de voz y video que son también una necesidad del Seguro de Pensiones.

La solución se acompaña de las especificaciones técnicas del equipamiento, en las que se plasma los requisitos que debe cumplir la infraestructura para poder dar cumplimiento al objetivo del diseño.

El proyecto se desarrolló atendiendo metodologías de análisis y diseño, así como también se introdujo en la solución estándares, recomendaciones y mejores prácticas de la industria.

Se da solución al conjunto de requerimientos de la Organización, en cada uno de los componentes de la misma, con lo que se garantiza que la solución global satisfaga completamente dichos requerimientos.

La instrumentación del presente proyecto, que permita culminar con éxito la automatización del Seguro de Pensiones, recomendamos se haga atendiendo lo siguiente:

El éxito de la puesta en operación de esta nueva tecnología radica en el nivel de asimilación y uso que cada uno de los funcionarios del Seguro de Pensiones le de, por lo que es imprescindible capacitar adecuadamente al talento humano para que haga buen uso de las herramientas.

En los actuales momentos, el Seguro de Pensiones no cuenta con suficiente personal informático y que esté capacitado, que garantice la operación de la

infraestructura, por lo que se recomienda incorporar al equipo de trabajo de informática personal de alta calificación.

REFERENCIA BIBLIOGRÁFICA

- ANDREW S. TANENBAUM. Redes de Computadoras 3ra. Ed. Prentice – Hall, México, año 1997
- ANDREW S. TANENBAUM. Redes de Computadoras 4ta. Ed. Prentice – Hall, México año 2003
- DOUGLAS E. COMER. Redes Globales de Información con Internet y TCP/IP 3ra. Ed. Prentice–Hall, México año 1996.
- CISCO PRESS, Segunda Edición. Arquitecturas de Enrutamiento en Internet, Cisco Systems , año 2001.
- CISCO PRESS. Interconnecting Cisco Network Devices, Cisco Systems CCNA Self – Study, año 2000.
- REGIS J. Comunicaciones Inalámbricas de Banda Ancha, McGraw-Hill, 2003
- BRIAN HATCH / James Lee / George Kurtz, Hackers en Linux, Secretos y Soluciones para Seguridad en Linux. Osborne McGraw-Hill, año 2001.
- STEVE SHAH, Manual de administración de Linux, Osborne McGraw-Hill, año 2001.
- GONZALO ALVAREZ MARAÑÓN, Seguridad informática para empresas y particulares, Mc Graw Hill, 2005
- CISCO NETWORKERS SOLUTIONS FORUM 2006. Routed Fast Converence and High Availability
- WILLIAM STALLINGS, Comunicaciones y Redes de Computadores, Séptima Edición, Prentice Hall, 2004.
- M. CARLING / Stephen Degler / James Dennis, Administración de Sistemas Linux, Prentice Hall.
- PAUL ALBITZ / Cricket Liu, Referencia DNS and Bind, tercera edición, 1998.
- O'REALLY & ASSOCIATES, Managing NFS and NIS, de Hal Stern.
- O'REALLY & ASSOCIATES, Segunda Edición, Referencia Guía de Administración de seguridades en Linux.
- GUEVARA JULCA / José Zulu, Sistemas de comunicación orientadas a la descentralización de las entidades publicas.

SITIOS WEB.

Unión Internacional de Telecomunicaciones: http://www.itu.int

Cisco Systems: http://www.cisco.com

3COM: http://www.3com.com

Superintendencia de Telecomunicaciones del Ecuador.

http://www.supertel.gov.ec/telecomunicaciones/v_agregado/estadisticas/anual.htm

TOMCAT: http://tomcat.apache.org

ANEXO I

FORMATO PARA REALIZAR EL LEVANTAMIENTO DE INFORMACIÓN

DEPENDENCIA:	UBICACIÓN FÍSICA		CONTACTO:		FECHA		
	Ciudad:		Nombre:		DD	MM	Año
	Dirección:		Teléfono:				

PISO	DEPARTAMENTO Proceso	EMPLEADOS		EXISTENTE						REQUERIDO							
				PUNTOS DATOS			PUNTOS ELECTRICOS			PUNTOS DATOS					PUNTOS ELÉCTRICOS		
		Adm	Oper	DATOS	VOZ	TOTAL	Estabil.	Norm	TOTAL	DATOS	VOZ	TOTAL	SIMPLE	DOBLES	Estabilizado	Normal	TOTAL

ESTRUC	**Cat**: Categoría **Pc**: Paneles de conexión **Tm**: Tomas Modulares **Rp**: Rack de piso	ELECT	**Tp:** Tomacorriente polarizado **Tb**: Tablero bypass **Td**: Tablero de Distribución
	Rc: Rack del cuarto de comunicaciones **Pp**: Placas de pared **Ca**: Canalización		**Cp:** Canaleta plástica **Em**: Escalerilla Metálica **Tm:** Tubería Metálica
	Br: Backbone y Reflejos de voz **Bd**: Backbone de datos **Et:** Etiquetado		**St:** Supresor trasientes **Mt:** Malla de tierra **Et**: Etiquetado

ANEXO II

ESPECIFICACIONES TECNICAS GENERALES PARA SWITCH

ESPECIFICACIONES TÉCNICAS REQUERIDAS
1 Los equipos ofertados deben ser garantizados contra defectos de fabricación y fallas de instalación, con la obligación de su inmediato reemplazo (no únicamente reparación), en caso de detectarse daños de esta naturaleza.
2 Los equipos deben ser entregados instalados, probados y funcionando correctamente con las últimas versiones de sistemas operativos.
3 Los oferentes deben presentar los certificados de distribuidores autorizados de los equipos ofertados y disponibilidad y capacidad de mantener provisión de repuestos y accesorios por al menos cinco (5) años, después de haber cumplido el período de vigencia de la garantía técnica.
4 Luego de la entrega - recepción de los equipos y durante el período de la garantía, el contratista estará obligado a ofrecer el servicio de mantenimiento preventivo y correctivo y soporte técnico de hardware y software continuo, sin costo adicional alguno. El oferente deberá dar atención a las llamadas de reportes de daños a través de su personal técnico, dentro del plazo de 2 horas. La reparación o reemplazo de cualquier parte defectuosa se atenderá dentro de las 24 horas siguientes, sin cargo adicional alguno.
5 Incluir contrato de soporte y mantenimiento

SWITCH DE 24 PUERTOS PARA STACK	
DESCRIPCIÓN	**ESPECIFICACIONES TÉCNICAS REQUERIDAS**
MARCA:	INDICAR
MODELO:	INDICAR
Características Generales	Capa 2/3/4.
	Power Over Ethernet, incluidos en todos los puertos
	24 Puertos 100/1000 BASE-TX con detección automática de velocidad.
	Backplane mínimo 130 Gbps.
	Throughput mínimo 100Mpps.
	Soporte de redes virtuales (VLAN)
	Administración local y remota incluido SNMP
	Soporte RMON.
	Capacidad full dúplex en cada uno de sus puertos.
Estándares soportados	802.1Q, 802.1p, 802.3ad, 802.1D, QoS, CoS, 802,1w, 802,1x, 802.3af
Filtrado de paquetes	Filtro ACL capa 2/3/4., dirección MAC fuente y destino, dirección IP fuente y destino, puerto TCP/UDP fuente y destino
Otros	Voltaje de 110V, 60 Hz.
	Cable de Poder.
	Cumplimiento de exigencias del año 2000
Garantía y Servicio	
Tiempo de Garantía	1 año
Tiempo máximo de respuesta a llamadas de servicio técnico durante la garantía (horas)	2
Tiempo máximo de reemplazo de partes defectuosas durante la garantía (horas)	24

SWITCH 24 PUERTOS CON GBIC	
DESCRIPCIÓN	**ESPECIFICACIONES TÉCNICAS REQUERIDAS**
MARCA:	INDICAR
MODELO:	INDICAR
Características Generales	Capa 2/3/4.
	Power Over Ethernet, incluido en todos los puertos
	24 Puertos 100/1000 BASE-TX con detección
	Dos puertos Gigabit ethernet 1000BASE-SX,
	Backplane mín. 130 Gbps.
	Throughput mín. 100 Mbps.
	Soporte de redes virtuales (VLAN)
	Administración local y remota incluido SNMP
	Soporte RMON.
	Capacidad full dúplex en cada uno de sus puertos.
Estándares soportados	802.1Q, 802.1p, 802.3ad, 802.1D, QoS, CoS, 802,1w, 802,1x, 802.3af
Filtrado de paquetes	Filtro ACL capa 2/3/4., dirección MAC fuente y destino, dirección IP fuente y destino, puerto TCP/UDP fuente y destino
Otros	Voltaje de 110V, 60 Hz.
	Cable de Poder.
Garantía y Servicio	
Tiempo de Garantía	1 año
Tiempo máximo de respuesta a llamadas de servicio técnico durante la garantía (horas)	2
Tiempo máximo de reemplazo de partes defectuosas durante la garantía (horas)	24

SWITCH DE 48 PUERTOS CON GBIC	
DESCRIPCIÓN	**ESPECIFICACIONES TÉCNICAS REQUERIDAS**
MARCA:	INDICAR
MODELO:	INDICAR
Características Generales	Capa 2/3/4.
	Power Over Ethernet, incluido en todos los puertos
	48 Puertos 100/1000 BASE-TX con detección automática de velocidad.
	Dos puerto Gigabit ethernet 1000BASE-SX. Conector SC,
	Backplane mín. 180 Gbps.
	Throughput mín. 130 Mpps.
	Soporte de redes virtuales (VLAN)
	Administración local y remota incluido SNMP
	Soporte RMON.
	Capacidad full dúplex en cada uno de sus puertos.
Estándares soportados	802.1Q, 802.1p, 802.3ad, 802.1D, QoS, CoS, 802,1w, 802,1x, 802.3af
Filtrado de paquetes	Filtro ACL capa 2/3/4., dirección MAC fuente y destino, dirección IP fuente y destino, puerto TCP/UDP fuente y destino
Otros	Voltaje de 110V, 60 Hz.
	Cable de Poder.
	Cumplimiento de exigencias del año 2000
Garantía y Servicio	
Tiempo de Garantía	1 año
Tiempo máximo de respuesta a llamadas de servicio técnico durante la garantía (horas)	2
Tiempo máximo de reemplazo de partes defectuosas durante la garantía (horas)	24

SWITCH DE CORE	
BREVE DESCRIPCIÓN	**ESPECIFICACIONES TÉCNICAS REQUERIDAS**
MARCA:	INDICAR
MODELO:	INDICAR
Características Generales	Capa 3
	24 puertos Gigabit ethernet 1000BASE-SX, conector SC
	6 puertos 1000BASE-TX
	Backplane mín. 180Gbps.
	Throughput mín. 100 Mpps
	Soporte de redes virtuales (VLAN) de acuerdo con 802.1Q
	Administración local y remota.
	Protocolos de ruteo incluídos: RIP1, RIP2, Rutas estáticas, OSPF.
	Protocolos adicionales: IGMP v1/v2 SNOOPING, BOOTP.
	Estándares incluidos 802.3ad, 802.1D, 802.1w, 802.1p, QoS, CoS.
	Capacidad full dúplex en cada uno de sus puertos.
Otros	Voltaje de 110V, 60 Hz.
	Cable de Poder.
	Cumplimiento de exigencias del año 2000.
Garantía y Servicio	
Tiempo de Garantía en partes, piezas y mano de obra	1 año
Tiempo máximo de respuesta a llamadas de servicio técnico durante la garantía (horas)	2
Tiempo máximo de reemplazo de partes defectuosas durante la garantía (horas)	4

ESPECIFICACIONES TÉCNICAS ROUTER

ESPECIFICACIONES TÉCNICAS REQUERIDAS
Los equipos ofertados deben ser garantizados contra defectos de fabricación y fallas de instalación, con la obligación de su inmediato reemplazo (no únicamente reparación), en caso de detectarse daños de esta naturaleza.
Los equipos deben ser entregados instalados, probados y funcionando correctamente con las últimas versiones de sistemas operativos.
Los oferentes deben presentar los certificados de distribuidores autorizados de los equipos ofertados y disponibilidad y capacidad de mantener provisión de repuestos y accesorios por al menos cinco (5) años, después de haber cumplido el período de vigencia de la garantía técnica.
Luego de la entrega - recepción de los equipos y durante el período de la garantía, el contratista estará obligado a ofrecer el servicio de mantenimiento preventivo y correctivo y soporte técnico de hardware y software continuo, sin costo adicional alguno. El oferente deberá dar atención a las llamadas de reportes de daños a través de su personal técnico, dentro del plazo de 2 horas. La reparación o reemplazo de cualquier parte defectuosa se atenderá dentro de las 48 horas siguientes, sin cargo adicional alguno.

BREVE DESCRIPCIÓN	ESPECIFICACIONES TÉCNICAS REQUERIDAS
Marca	Especificar
Modelo	Especificar
PUERTOS DE DATOS	1 puerto fast ethernet.
	1 puerto serial V35 con velocidad de hasta 2,048 Mbps.
	1 puerto serial WAN V35/RS232 para backup
COMPRESIÓN	6.3 Kbps. por cada canal de voz.
EXPANSIÓN	2 slots de expansión libres.
MEMORIA	64 MB de DRAM.
PROTOCOLOS	TCP, IP versión 4, Frame Relay, SNMP, RIP1/RIP2, NAT, VoIP.
CALIDAD DE SERVICIO	Priorización de tráfico.
	Compresión de voz.
	Clasificación de paquetes por: dirección destino, dirección fuente, puerto destino, puerto fuente.
	Ancho de banda bajo demanda.
	Fragmentación Dinámica / Segmentación de datos cuando voz esté presente.
CONTRATO SMART ONSIDE	Incluido
Garantía y Servicio	
Tiempo de Garantía	3 años
Tiempo máximo de respuesta a llamadas de servicio técnico durante la garantía (horas)	2
Tiempo máximo de reemplazo de partes defectuosas durante la garantía (horas)	48

ESPECIFICACIONES GENERALES DE SERVIDOR.

ESPECIFICACIONES REQUERIDAS
1. Los equipos ofertados deben ser garantizados contra defectos de fabricación y fallas de instalación, con la obligación de su inmediato reemplazo (no únicamente reparación), en caso de detectarse daños de esta naturaleza.
2. Todos los equipos ofertados deben ser de marca; y sus partes, accesorios y componentes deben ser originales.
3. Los equipos deben ser entregados instalados, probados y funcionando correctamente con las últimas versiones de sistemas operativos.
4. Los oferentes deben presentar los certificados de distribuidores autorizados de los equipos ofertados y disponibilidad y capacidad de mantener provisión de repuestos y accesorios por al menos cinco (5) años, después de haber cumplido el período de vigencia de la garantía técnica.
5. Luego de la entrega - recepción de los equipos y durante el período de la garantía, el contratista estará obligado a ofrecer el servicio de mantenimiento preventivo y correctivo y soporte técnico de hardware y software continuo, sin costo adicional alguno. El oferente deberá dar atención a las llamadas de reportes de daños a través de su personal técnico, dentro del plazo de 2 horas. La reparación o reemplazo de cualquier parte defectuosa se atenderá dentro de las 48 horas siguientes, sin cargo adicional alguno.

SERVIDOR TIPO 1	
DESCRIPCIÓN	**ESPECIFICACIONES REQUERIDAS**
Características Generales	
Marca	Especificar
Modelo	Especificar
Chasis tipo Rack	Incluido kit de instalación
Memoria RAM Instalada mínimo	2 GB, DDR2 de 666Mhz utilizando el mínimo número de slots posible. Indicar
Máximo crecimiento en Memoria RAM	Especificar
Ancho de Banda del bus de sistema	800 Mhz. mínimo
Velocidad del Reloj (mínimo)	1.33GHz
Caché L2 por procesador	1 MB mínimo
Puertos Seriales (mínimo)	1
Puertos USB (mínimo)	2
Unidad de medios óptico	1 unidad de DVD WRITER
Interfaces de red	Dual 100/1000BASE-TX, conector RJ-45
Número y tipo de slots de expansión indicar	Especificar
Procesador	
Procesador	Intel Xeon dual core con tecnología Hyper Threading
# de procesadores Instalados	1
Capacidad de crecimiento a familias de procesadores futuros	Soportado
Redundancia	
Fuentes de poder	1
Ventiladores redundantes	Incluido, indicar número
Almacenamiento disco SCSI	
Volumen de almacenamiento	146 GB Instalado
Capacidad de crecimiento en volumen de almacenamiento	Especificar
Discos con capacidad Hot Swap	1 unidad de 146 GB de10000 rpm (mínimo)
Software Operativo	
Tipo de Sistema Operativo	LINUX Red Hat Enterprise última versión, incluir soporte y actualizaciones por un año.
Dispositivos de I/O	
Monitor	17" Flat Panel LCD, misma marca de CPU
Teclado	Expandido 102 teclas, español, misma marca del CPU
Mouse	2 botones y scroll misma marca del CPU
Garantía y Servicio	
Tiempo de Garantía	3 años
Mantenimiento preventivo dos veces al año, durante el período de la garantía.	Incluido

SERVIDOR DE RED TIPO 2	
DESCRIPCIÓN	**ESPECIFICACIONES REQUERIDAS**
Características Generales	
Marca	Especificar
Modelo	Especificar
Chasis tipo Rack	Incluido
Memoria RAM Instalada mínimo	4 GB, DDR2 de 666Mhz utilizando el mínimo número de slots posible. Indicar
Máximo crecimiento en Memoria RAM	Especificar
Ancho de Banda del bus de sistema	800 Mhz. mínimo
Velocidad del Reloj (mínimo)	1.33GHz
Caché L2 por procesador	1 MB mínimo
Puertos Seriales (mínimo)	1
Puertos Paralelos (mínimo)	1
Puertos USB (mínimo)	2
Unidad de Tape/Backup	Dat/DLT 24GB mínimo
Unidad de medios ópticos	1 unidad de DVD WRITER
Interfaces de red	Dual 100/1000BASE-TX, conector RJ-45, estándar 802.3ad incluido
Número y tipo de slots de expansión indicar	Especificar
Procesador	
Procesador	Intel Xeon dual core con tecnología Hyper Threading
# de procesadores Instalados	2
Capacidad de crecimiento a familias de procesadores futuros	Soportado
Redundancia	
Fuentes de poder con capacidad Hot Swap	2
Ventiladores redundantes	Incluido, indicar número
Almacenamiento disco SCSI	
Volumen de almacenamiento	292 GB Instalado
Capacidad de crecimiento en volumen de almacenamiento	Especificar
Discos con capacidad Hot Swap	2 unidades de 146 GB de10000 rpm (mínimo)
Incluir controlador tecnología RAID (Configuración por Hardware)	0, 1, 0+1, 5
Software Operativo	
Tipo de Sistema Operativo	LINUX Red Hat Enterprise última versión, incluir soporte y actualizaciones por un año.
Dispositivos de I/O	
Monitor	17" Flat Panel LCD, misma marca de CPU.
Teclado	Expandido 102 teclas, español, misma marca del CPU
Mouse	2 botones y scroll misma marca del CPU
Garantía y Servicio	
Tiempo de Garantía	3 años
Mantenimiento preventivo dos veces al año, durante el período de la garantía.	Incluido

SERVIDORES DE SERVICOS	
DESCRIPCIÓN	**REQUERID0**
Cantidad:	1 (UNO) soporte la instalación de los servidores blade requeridos.
Marca	INDICAR
Modelo	INDICAR
Capacidad de crecimiento.	En el chasis se podrá instalar mínimo 10 servidores tipo Blade de las características requeridas.
Características Generales	Los blades deben tener capacidades hot plug
	Debe soportar múltiples arquitecturas de Procesador simultáneamente: AMD, Intel, Otros
Dimensiones	Especificar en unidades de rack, las unidades que ocuparía instalado en rack.
Indicadores	Incluido, de diagnóstico, alarmas y fallas
Conectividad fiber channel en redundancia para SAN:	
Puertos Fiber channel para conexión a sistema de almacenamiento	4 (cuatro) puertos Fiber Channel mínimo, de 4 Gbps cada uno, a través de los cuales cada Blade se conectará al almacenamiento
Módulo de control para administración y monitoreo:	
Módulo de administración y monitoreo integrado	Incluido
Capacidad de acceso vía SSH, CLI	Incluido
Suministro de energía:	
Fuente de poder redundante, diseñada para cubrir los requerimientos de energía con el chasis lleno de servidores Blade.	Incluido
Fuentes deben ser hot-swap	Incluido
Alimentación eléctrica: Soporte a alimentación eléctrica de 110V ó 220V	Incluido
Sistema de ventilación:	
Sistema de ventiladores redundante	Incluido, detallar sistema de ventilación
Las fuentes deben ser hot-swap	Incluido
Accesorios para instalación:	
Debe incluir accesorios de instalación en rack para todos los componentes solicitados	Incluido
Debe incluir kit de estabilización para bastidor	Incluido
SERVIDORES TIPO BLADE	

SERVIDORES DE SERVICOS	
DESCRIPCIÓN	**REQUERID0**
Marca	INDICAR
Modelo	INDICAR
Cantidad:	8 (OCHO)
Procesadores:	
Tipo de Procesador	1 Intel Xeon Quad Core. Por cada Blade.
Capacidad Multithread por core	Incluido
Crecimiento en número de procesadores por cada Blade.	Incluido
Frecuencia	1.86 Ghz mínimo
Buses de I/O:	
Mínimo 2 slots I/O para cada Blade	Incluido
Soporte de módulos estándares de la industria PCI Express (PCI-SIG) hot-plug	Incluido
Memoria RAM:	
Cantidad de memoria RAM incluida de acuerdo al detalle que se indica.	8 Blades con 8 GB de RAM
Máxima cantidad de memoria por cada Blade	Especificar.
Discos:	
Tecnología	Serial Attached SCSI (SAS) hot-swap
Volúmen de almacenamiento	2 discos de 146GB mínimo por cada servidor Blade
Velocidad	Mínimo de 10,000 RPM ó superior por cada disco
Incluir controlador tecnología RAID (Configuración por Hardware)	0, 1, 0+1, 5
Conectividad en redundancia para LAN:	
Cuatro puertos Gigabit Ethernet 10/100/1000BASE-TX por cada Blade	Incluido
Software de administración:	
Software de administración de servidores blade, suministrado por el fabricante	Incluido
Capacidad de utilizar software de administración de terceros: CA, Open-View, Tivoli, Altiris, BMC, etc.	Soportado
Facilidades mínimas requeridas:	
6. Monitoreo	Incluido
7. Control de rendimiento	Incluido
8. Administración de sistemas operativos y parches	Incluido

SERVIDORES DE SERVICOS	
DESCRIPCIÓN	**REQUERID0**
ALMACENAMIENTO EXTERNO (SAN).	
Volumen de almacenamiento	3 TB Instalado
Capacidad de crecimiento en volumen de almacenamiento	Especificar
Discos con capacidad Hot Swap	3 TB instalados con discos de fibra Attached SCSI (SAS) hot-swap de 15Krpm. mínimo.
Incluir controlador tecnología RAID	0, 1, 0+1, 5
Puertos Fiber channel para conexión a servidores Blade	4 (cuatro) puertos Fiber Channel mínimo, de 4 Gbps cada uno
Software de administración del SAN.	Incluido
INSTALACIÓN	
El oferente deberá entregar todos los equipos instalados y funcionando incluyendo todo el hardware, software y accesorios que permitan la instalación y operación de los requerimientos especificados.	Incluido
Fecha de fabricación	La fecha de lanzamiento al mercado de los equipos a adquirirse no deberá ser menor al 2007
Cables y conectores	Todos los equipos deben incluir cables y conectores necesarios para su correcta operación
Consideraciones técnicas	Todos los componentes deben ser de la misma marca u homologados por el fabricante de los equipos De ser necesario, el oferente suministrará todo el hardware necesario para instalar el software de administración; detallar implementación e instalación de este software Si la oferta requiere utilizar un servidor de administración dedicado, éste deberá configurarse con las características de hardware óptimas para asegurar el correcto funcionamiento de la solución Los modelos de equipos servidores ofertados deben tener certificación por parte del fabricante para soportar los Sistemas operativos, Red Hat Enterprise Linux Server, VMWare ESX Enterprise 3 y Sun Solaris 10 ó versiones superiores
Manuales técnicos	Todos los equipos deben incluir manuales técnicos y de operación Catálogos de fábrica con especificaciones de cada uno de los equipos
Calidad de los productos	Todos los componentes deben cumplir o superar las especificaciones técnicas y de calidad, solicitadas en este documento.

SERVIDORES DE SERVICOS	
DESCRIPCIÓN	**REQUERID0**
Certificaciones	Los oferentes deberán presentar una certificación de ser distribuidores autorizados de la marca ofertada Los oferentes deberán presentar certificados emitidos por el fabricante de los equipos, que acrediten que su personal está capacitado para implementar la solución solicitada
Garantía técnica, soporte y Mantenimiento	Garantía del hardware, con soporte técnico ante fallas, mínimo por tres años con períodos de atención 7x24 con 4 horas de tiempo de respuesta Garantía del software mínimo por tres años Los oferentes deben estar en capacidad de proveer partes y piezas en caso de que se presenten daños en los componentes de los equipos durante el período de garantía.
Mantenimiento del Software	Acceso a actualizaciones de software para todos los sistemas ofertados, mínimo durante 3 años
Centro de Servicios	Los oferentes deben presentar una certificación indicando que disponen de un centro de servicio técnico para brindar mantenimiento a los equipos ofertados, en la ciudad de Quito

ESPECIFICACIONES TÉCNICAS GENERALES

SERVIDOR DE APLICACIONES Y BASE DE DATOS

REQUERIDO
Los equipos ofertados deben ser garantizados contra defectos de fabricación y fallas de instalación, con la obligación de su inmediato reemplazo (no únicamente reparación), en caso de detectarse daños de esta naturaleza.
Los equipos deben ser nuevos de fábrica, no se aceptarán equipos remanufacturados ni usados.
Todos los equipos ofertados, sus partes y accesorios, deben ser de marca y originales. No se aceptan clones.
Los equipos deben ser entregados instalados, probados y funcionando correctamente con las últimas versiones del Sistema.
Los oferentes deben presentar los certificados de distribuidores autorizados de los equipos ofertados, disponibilidad y capacidad de mantener provisión de repuestos y accesorios por un período mínimo de cinco (5) años, posterior a la entrega e instalación del equipo, para garantizar la funcionalidad durante el tiempo de vida útil.
Luego de la entrega - recepción de los equipos y durante el período de la garantía, el contratista estará obligado a ofrecer el servicio de mantenimiento preventivo y correctivo y soporte técnico de hardware y software, de acuerdo a las especificaciones técnicas

SERVIDOR DE APLICACIONES Y BASE DE DATOS

DESCRIPCIÓN	ESPECIFICACIONES TÉCNICAS REQUERIDAS
MARCA	**ESPECIFICAR**
MODELO	**ESPECIFICAR**
CANTIDAD	**2 (DOS)**
CARACTERÍSTICAS GENERALES	
Memoria RAM Instalada mínimo	16 GB con corrección de errores, utilizando el menor número de DIMMs posible
Máximo crecimiento en Memoria RAM	Especificar
Longitud de palabra, soportada por hw y sw	64 bits
Velocidad de reloj del procesador (mínimo)	2,1 GHz
Caché L1 de Datos / Instrucciones (mínimo) por procesador	256 KB on-chip
Caché L2 de Datos / Instrucciones (mínimo) por procesador	2 MB on chip
Puertos Seriales (mínimo)	Uno (1)
Canales de fibra óptica FC-AL para conexión de dispositivos de almacenamiento	2 tarjetas PCI HBA FC 4Gbps
Interfases de red 10/100/1000 BASE-TX autoconfigurables	2 tarjetas PCI ethernet 10/100/1000 Mbps con puerto RJ-45 para fileover
Slots PCI hot-plug de 64 bits para tarjeta I/O o comunicaciones (mínimo)	Dos (2)
Slots PCI hot-plug de 64 bits para tarjeta I/O o comunicaciones (máximo)	Especificar
Ancho de Banda del bus del sistema (mínimo)	9.6 GB/seg
Equipo para ser instalado en Rack	Incluido
Tarjeta de video	Incluido
Puertos para monitor, teclado y Mouse	Incluido
Unidad de lectura/escritura de medios óptico	Una (1) unidad de DVD-ROM
Kit de montaje en rack	Incluido
PROCESADOR	
Arquitectura	SPARC
Procesadores Instalados (mínimo)	Cuatro (4)
Procesadores máximo soportado	Al menos hasta 8 procesadores en el mismo chasis, independiente del número de núcleos por procesador
ALMACENAMIENTO	
Discos duros internos Ultra320 SCSI o FC	2 discos Ultra320 SCSI 146GB 15K RPM
CARACTERÍSTICAS DE ALTA DISPONIBILIDAD	
Fuentes de poder redundantes y de intercambio en caliente	Incluido
Ventiladores redundantes y de intercambio en caliente	Incluido
Discos duros de intercambio en	Incluido

DESCRIPCIÓN	ESPECIFICACIONES TÉCNICAS REQUERIDAS
caliente	
Software en línea	Incluido
Monitoreo de Componentes de HW	Incluido
SISTEMA OPERATIVO	
Tipo de Sistema Operativo	Solaris última versión
Cumpla con estándar UNIX	System V Release 4
Soporte de aplicaciones	64 bits
Soporte a protocolos de comunicación	IP, TCP/IP, protocolos de capa de aplicación: NFS, SMPTP, WEB, SMB, etc
Licencia de Usuarios en red o de terminales	Ilimitada
Capacidad para tareas.	Multitarea y multithread
Manejo de memoria virtual	Soportado
Software para realizar tareas de administración	Si
Documentación del sistema operativo en línea	Si
Soporte a lenguajes	C,C++, Java
Soporte a aplicaciones Java	J2EE
Soporte a estándares de ambientes distribuidos	CORBA, RPC.
SOPORTE Y MANTENIMIENTO	
Soporte y mantenimiento para un año	**Mantenimiento preventivo:** Período: 12 meses Visitas al año: 12 visitas mensuales: 1 para mantenimiento preventivo de hardware, diagnósticos, pruebas de rendimiento y revisión de LOGs **Mantenimiento Correctivo:** • Horario: 7x24x365, incluye fines de semana y feriados • Incluye repuestos sin costo • Tiempo de respuesta para casos críticos: máximo 3 horas Soporte en hardware y software: • Soporte telefónico y en sitio para actividades de operación y administración del hardware y software de los equipos • Instalación de parches actualizados y recomendados por el fabricante
GARANTÍA TÉCNICA	
3 años de Garantía	Incluir

ESPECIFICACIONES DE ENLACES DE TELECOMUNICACIONES

ESPECIFICACIONES TÉCNICAS GENERALES	
BREVE DESCRIPCIÓN	**ESPECIFICACIONES TECNICAS REQUERIDAS**
Punto A.	
Punto B.	
Tipo de enlace.	Frame –Relay / Clear Channel , MPLS
Infraestructura de comunicaciones	Privada/Pública. Especificar.
Medio de transmisión	Fibra óptica, Microonda, par de cobre, otros. (Especificar)
Capacidad de Canal	De acuerdo al cuadro adjunto.
Capacidad de crecimiento del canal, sin necesidad de cambio de equipos instalados.	Incluido. Especificar porcentaje de crecimiento.
Tiempo de respuesta máximo (medido sin tráfico).	35 ms. (milisegundos)
Máximo nivel de pérdidas permitido	BER 10^{-7}
Equipos de comunicación incluidos en la solución propuesta, mismos que deben entregar interfaces de red disponibles en las dependencias del IESS: • V.35/V.36 (EIA/TIA RS-449), con conector estándar M34 (Winchester). tipo “hembra “ y de características funcionales y operativas DTE. • Interfases E1 canalizadas.	Especificar.
Garantía de disponibilidad del enlace. Porcentaje de disponibilidad garantizado	99.97% de 365 días como base de tiempo
Tiempo máximo de respuesta, para restaurar fallas mayores	No mayor a 4 horas

ORIGEN	DESTINO	CAPACIDAD DE CANAL
BACKBONE DE TELECOMUNICACIONES		
QUITO	GUAYAQUIL	1,5 Mbps
QUITO	CUENCA	1,5 Mbps
GUAYAQUIL	CUENCA	1,5 Mbps
ENLACES		
QUITO	SUDIRECCION DE PENSIONES	1.0 Mbps
QUITO	IBARRA	256 Kbps
QUITO	TUNGURAHUA	256 Kbps
QUITO	CHIMBORAZO	256 Kbps
CUENCA	LOJA	256 Kbps
GUAYAQUIL	MANABI	256 Kbps
GUAYAQUIL	EL ORO	256 Kbps

BASES TÉCNICAS DE CABLEADO ESTRUCTURADO

ESPECIFICACIONES TÉCNICAS GENERALES
El sistema ofertado debe ser garantizado contra defectos de fabricación y fallas de instalación, con la obligación de su inmediato reemplazo (no únicamente reparación), en caso de detectarse daños de esta naturaleza.
Luego de la entrega - recepción del sistema y durante el período de la garantía, el contratista estará obligado a ofrecer el servicio de mantenimiento preventivo, correctivo y soporte técnico continuo, sin costo adicional alguno. El oferente deberá dar atención a las llamadas de reportes de daños a través de su personal técnico, dentro del plazo de 2 horas. La reparación o reemplazo de cualquier parte defectuosa se atenderá dentro de las 48 horas siguientes, sin cargo adicional alguno.
El sistema de cableado estructurado debe cumplir con estándares internacionales de cableado CAT-6 (se especifican mas adelante), el mismo que debe ser certificado por el fabricante. Es responsabilidad del oferente la certificación del sistema.
El oferente debe elaborar los planos que serán requeridos para las instalaciones, para ello el IESS brindará las facilidades necesarias, así como también la información que se requiera para el efecto. Requerimiento adicional es la elaboración de una memoria técnica del sistema implementado.
El oferente deberá registrar la marca del sistema de cableado a ser instalado. Todos los componentes deben ser de un mismo fabricante, incluido el cable UTP.
El oferente debe entregar etiquetado: tomas de pared, canaletas, patch cords con tamaño mínimo de letra N°20. Los patch panels etiquetar de acuerdo al tamaño que permita el mismo.

El sistema de Cableado Estructurado estará regido por las siguientes normas Internacionales:

REQUERIDO
Marca
Diseño y Administración de la Red. EIA/TIA 569
Control de calidad de la instalación EIA/TIA 568
Administración EIA/TIA 606
Pruebas de Cableado Estructurado EIA/TIA TSB-67
Tierras y aterramientos para sistemas de telecomunicaciones EIA/TIA 607

Cable UTP categoría 6

REQUERIDO
UL444
UL`S LAN
VTFT
Ser del tipo CM
TIA/EIA – 568-B.2
ISO/IEC 11801
TIA/EIA – 568-B.3
Copper wires
4 pares
23 ó 24 AWG
Aislante HDPE
Espesor 0.20mm
Chaqueta PVC
Espesor: 0.55
Diámetro: 5.3 mm
Pruebas eléctricas de acuerdo a las siguientes normas: Rendimiento UL, Rendimiento ASTM D-4566

Paneles de conexión categoría 6

REQUERIDO
EIA/TIA 568, ISO/IEC 11801
Identificadores IDC
Tipo de conector: RJ-45 / Block 110 ó Conector de Impacto
EIA/TIA 568B
Mediciones de transmisión con EIA/TIA – 568B.2
Categoría 6 a 250 Mhz
IDC: 23 – 24 AWG
Mínima interferencia Crosstalk

Tomas Modulares

REQUERIDO
Deberán cumplir con los estándares UL.
Asignación de pines de acuerdo a los estándares T568B
Las tomas deben ser estéticamente bien colocadas, utilizar tornillos para sujeción en la pared (mínimo 2).

Placas (Face Plate)

REQUERIDO
Deberán cumplir con los estándares UL
Material ABS 94V-0
La placa debe contener ranura de alojamiento de etiquetas

Tomas (Jacks)

REQUERIDO
Cubierta: 94v – 0 ABS
Bloque IDC: UL94V
Contactos: 50 micro pulgadas de oro
50 **–** 100 micro pulgadas de nivel en superficie de contacto
IDC: soldado con fósforo de bronce
Circuito: verificado UL y listado como CAT-6
4 pares
23 ó 24 AWG

Rack de Salas de Telecomunicaciones - Tipo Armario

REQUERIDO
CANTIDAD:
Alta resistencia 6061-T6
Ángulos superiores incluidos
Ancho general: 65 cm.
Altura general 20 unidades
Huecos convencionales de 5.8” – 5/8” – ½”
Compatibilidad con estándares EIA
Cinco manejadores horizontales.
Dos manejadores verticales
Puerta posterior perforada.
Panel superior con perforación central.
Dos ventiladores incorporados
Una regleta de 4 tomas de energía cada una, ubicadas en la parte posterior del a.C. Debe incluir supresor de transientes.
Cincuenta tornillos de sujeción.

Rack de Sala de Equipos.

REQUERIDO
CANTIDAD:
Alta resistencia 6061-T6
Ángulos superiores
Ancho general: 75 cm.
Altura general 196 cm.
Profundidad 100 cm.
Huecos convencionales de 5.8” – 5/8” – ½”
Compatibilidad con estándares EIA
Ocho manejadores horizontales.
Dos manejadores verticales
Tres bandejas de alta resistencia
Puerta posterior perforada.
Panel superior con perforación central.
Dos ventiladores incorporados
Dos regletas de 8 tomas de energía cada una, ubicadas en la parte posterior del Rack. Debe incluir supresor de transientes.
Cincuenta tornillos de sujeción.

Cables Categoría 6

REQUERIDO
La bota acoplada al jack en fábrica
Impedancia: 100 Ohm +/- 10%
R.M.D.: 3% (5% para TIA/EIA)
Velocidad mínima de propagación: 0.65C
Fuerza del cable al conector: 400 N
Durabilidad: 750 ciclos mín
Voltaje: 300Vrms a 1.5ª
Retardo de propagación: 536 ns
Velocidad nominal de operación: 72%
R. De contacto: 10 mill. Máximo
Aislante: 500 Megaohmios min.
Contactos: 50 um de oro sobre níquel
Atenuación cable horz.: 31.2db/250 Mhz.
Next cable horiz.: 38.3
ACR: 5.5dB /250 Mhz
RL: 15.6 dB / 250 Mz
PSELFEXT: 16.8 dB/250 Mhz
ELFEXT: 19.8 dB / 250 Mhz
Insertion loss: 32.8 dB/250 Mhz
Pérdida de retorno: 17.3 dB/250MHz
Next patch cable: 46.3 db

Canalización

REQUERIDO
Utilizar tubería metálica EMT,
Utilizar cajas de paso, de acuerdo a norma EIA/TIA 569
Utilizar canaleta decorativa, con todos los accesorios de acoplamiento a techos falsos, placas de pared, codos.
Aplicar código de colores para identificar tubería. Color azul canalización de voz y datos.

Troncales de Voz.

REQUERIDO
Cable multipar.
Patch panels de voz, tanto para troncales.
Realizar conexión al tablero de proveedor de telefonía pública.

Backbone de Datos

REQUERIDO
Fibra óptica multimodo de 6 hilos, todos los hilos conectorizados.
Patch Panels de Fibra óptica, incluido bandeja tipo caja para patch panel, conectores SC.
Patch Core de fibra óptica, conector SC-LC, de 7 pies.

ANEXO III

Archivos de Configuración del Servidor de DNS matriz:

/etc/named.conf

```
acl pensiones {
       192.168.2.32/27;
       192.168.3.0/24;
       192.168.4.128/25;
       192.168.5.64/26;
       192.168.6.32/27;
       192.168.6.64/27;
       192.168.6.96/27;
       192.168.6.128/27;
       192.168.6.160/27;

};
options {
      directory "/var/named";
        allow-query { pensiones; };
//    rrset-order { type A order random; };
rrset-order { type A order random; };
};
zone "'.'" {
      type hint;
      file "named.ca";
};
zone "10.168.192.in-addr.arpa" {
      type master;
      file "10.168.192.in-addr.arpa.zone";
        allow-query { pensiones; };
};
zone "11.168.192.in-addr.arpa" {
      type master;
      file "11.168.192.in-addr.arpa.zone";
        allow-query { pensiones; };

};
zone "0.16.172.in-addr.arpa" {
      type master;
      file "0.16.172.in-addr.arpa.zone";
        allow-query { pensiones; };
};


zone "pensiones.iess.gov.ec" {
      type master;
      file "pensiones.iess.gov.ec.zone";
        allow-query { pensiones; };
};
```

/var/named/pensiones.iess.gov.ec.zone

```
$TTL 86400
@     IN    SOA   pensiones.iess.gov.ec.  root.pensiones.iess.gov.ec.(
                        287 ; serial
                        28800 ; refresh
                        14400 ; retry
                        3600000 ; expire
                        86400 ; ttl
                        )
```

```
@     IN    NS    192.168.10.13

;----- APP PENSIONES ----------
srvuio04    IN     A    192.168.10.28

;------ BASE DE DATOS PRODUCCION ---------
srvuio05        IN       A      192.168.25.18


;------ MAIL SERVER ---------
srvuio10          IN       A      192.168.10.87


;------ SERVIDOR DNS ------------------
srvuio17        IN       A      192.168.11.89


;------ SERVIDORES WEB ---------
srvuio09        IN       A      192.168.11.125
srvuio13        IN       A      192.168.11.124
srvweb02        IN       A      192.168.11.66
srvweb04        IN       A      192.168.11.67


;------ SMTP GATEWAY ---------
srvuio10        IN       A      192.168.11.73

;------ BALANCEADOR SERVIDORES WEB INTERNET---------
balanceo    IN    A       192.168.11.83

;------ BALANCEADOR SERVIDORES WEB INTRANET---------
balanceo    IN    A       192.168.11.84


;------ REGISTRO DEL SERVIDOR DE CORREO

@           IN    MX    1     mail.pensiones.iess.gov.ec.


;------ DEFINIR CANONICAL NAME ---------

www     IN      CNAME   balanceo.pensiones.iess.gov.ec.
mail  IN    CNAME srvuio10.pensiones.iess.gov.ec
```

Configuración del Servidor de Navegación por Internet

/etc/squid/squid.conf

Agregar las siguientes líneas:

```
http_port 8080

cache_mem 256 MB

cache_dir ufs /var/spool/squid 5000 16 256

EJEMPLOS DE LLAMADA DE ARCHIVOS DE DIRECIONES PERMITIDAS

acl PERMITIDAS src "/etc/squid/proxy/auth_nav"
http_access allow PERMITIDAS

EJEMPLO DE ARCHIVOS PARA AUTORIZACION DE ACCESO A MESSENGER

# MESSENGER
acl Mensajeria src "/etc/squid/proxy/auth_mensajeria"
http_access allow Mensajeria
```

/etc/squid/proxy/auth_nav

```
192.168.2.1/27
192.168.2.2/27
192.168.2.11/27
192.168.2.15/27
192.168.2.19/27
192.168.2.20/27
192.168.2.21/27
192.168.2.24/27
192.168.2.25/27
192.168.2.28/27
192.168.2.35/27
192.168.2.36/27
192.168.2.37/27
192.168.2.40/27
192.168.2.43/27
192.168.2.46/27
192.168.2.49/27
192.168.2.61/27
192.168.2.222/27
192.168.2.58/27
192.168.2.64/27
192.168.2.65/27
192.168.2.101/27
192.168.2.117/27
```

"/etc/squid/proxy/auth_mensajeria

```
192.168.6.74/27
192.168.6.186/27
```

Configuración del Servidor de DHCP de la Dirección de Pensiones
Ejemplo de archivo de configuración.

```
authoritative;
one-lease-per-client on;
server-identifier ns1.centro.ies;
default-lease-time 604800;
max-lease-time 604800;
option subnet-mask 255.255.255.224;
option broadcast-address 192.168.2.63;
option routers 192.168.2.62;
option domain-name-servers 192.168.2.33;
option domain-name "pensiones.iess.gov.ec";
ddns-domainname "pensiones.iess.gov.ec";
ddns-update-style ad-hoc;
ddns-updates on;
option netbios-name-servers 192.168.2.33;

subnet 192.168.2.32 netmask 255.255.255.224 {
range 192.168.2.38 192.168.2.58;
}
```

ANEXO IV

Archivos de Configuración del mod_jk.conf, workers.properties, uriworkermap.prperties.

/etc/httpd/conf.d/mod_jk.conf:

```
# Load mod_jk module

# Specify the filename of the mod_jk lib
LoadModule jk_module modules/mod_jk.so

# Where to find workers.properties
JkWorkersFile conf/workers.properties

# Where to put jk logs
JkLogFile logs/mod_jk.log

# Set the jk log level [debug/error/info]
JkLogLevel info

# Select the log format
JkLogStampFormat "[%a %b %d %H:%M:%S %Y]"

# JkOptions indicates to send SSK KEY SIZE
JkOptions +ForwardKeySize +ForwardURICompat -ForwardDirectories

# JkRequestLogFormat
JkRequestLogFormat "%w %V %T"

# Mount your applications
JkMount /application/* loadbalancer

# You can use external file for mount points.
# It will be checked for updates each 60 seconds.
# The format of the file is: /url=worker
# /examples/*=loadbalancer
JkMountFile conf/uriworkermap.properties

# Add shared memory.
# This directive is present with 1.2.10 and
# later versions of mod_jk, and is needed for
# for load balancing to work properly
JkShmFile logs/jk.shm

# Add jkstatus for managing runtime data
<Location /jkstatus/>
JkMount status
Order deny,allow
Deny from all
Allow from 127.0.0.1
</Location>
```

/etc/httpd/conf/workers.properties:

```
# Define list of workers that will be used
# for mapping requests
worker.list=loadbalancer,status

# JBoss 1
```

```
worker.node1.port=8009
worker.node1.host=192.168.10.53
worker.node1.type=ajp13
worker.node1.lbfactor=1
worker.node1.socket_keepalive=1

# JBoss 2
worker.node2.port=8009
worker.node2.host=192.168.10.80
worker.node2.type=ajp13
worker.node2.lbfactor=1
worker.node2.socket_keepalive=1

# JBoss 3
worker.node3.port=8009
worker.node3.host=192.168.10.100
worker.node3.type=ajp13
worker.node3.lbfactor=1
worker.node3.socket_keepalive=1

# JBoss 4
worker.node4.port=8009
worker.node4.host=192.168.10.63
worker.node4.type=ajp13
worker.node4.lbfactor=1
worker.node4.socket_keepalive=1

# Load-balancing behaviour
worker.loadbalancer.type=lb
worker.loadbalancer.balance_workers=node1,node2,node3,node4
worker.loadbalancer.sticky_session=1

# Status worker for managing load balancer
worker.status.type=status
```

/etc/httpd/conf/uriworkermap.properties:

```
# Simple worker configuration file
# Mount the Servlet context to the ajp13 worker

#/jmx-console=loadbalancer
#/jmx-console/*=loadbalancer
#/web-console=loadbalancer
#/web-console/*=loadbalancer

/pensiones-web=loadbalancer
/pensiones-concesion-web/*=loadbalancer
```

Archivo de configuración httpd.conf

/etc/httpd/conf/httpd.conf:

```
...
<IfModule prefork.c>
StartServers       8
MinSpareServers    5
MaxSpareServers   20
ServerLimit      512
MaxClients       512
MaxRequestsPerChild 4000
</IfModule>
...
```

ANEXO V

Tablas de cálculo de los Backbone de Fibra Óptica

Backbone Subdirección de Pichincha

PISO	RECORRIDO	Longitud $5 x m	Patch Panel $350	Conectores $9	Conexión $40 x hilo
PB	Del rack de la sala de telecomunicaciones de PB al rack de la sala de equipos del piso 5	18	1	12	12
7	Del rack de la sala de telecomunicaciones del 7mo piso al rack de la sala de equipos del piso 5	10	2	12	12
	TOTAL	**$140,00**	**$1.050,00**	**$216,00**	**$960,00**
	TOTAL GENERAL	**$2.366,00**			

Backbone Dirección de Pensiones y Subdirección de Contabilidad

PISO	RECORRIDO	Longitud $5 x m	Patch Panel $350	Conectores $9	Conexión $40 x hilo
PB	Del rack de la sala de telecomunicaciones deL piso 4 al rack de la sala de equipos del piso 1	9	2	12	12
	TOTAL	**$45,00**	**$700,00**	**$108,00**	**$480,00**
	TOTAL GENERAL	**$1.333,00**			

Backbone Subdirección del Guayas

PISO	RECORRIDO	Longitud $5 x m	Patch Panel $350	Conectores $9	Conexión $40 x hilo
PB	Del rack de la sala de telecomunicaciones del piso 7 al rack de la sala de equipos del piso 3	12	1	12	12
7	Del rack de la sala de telecomunicaciones de la planta baja al rack de la sala de equipos del piso 3	12	2	12	12
	TOTAL	**$120,00**	**$1.050,00**	**$216,00**	**$960,00**
	TOTAL GENERAL	**$2.346,00**			