

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA

SEDE VIÑA DEL MAR

“JOSÉ MIGUEL CARRERA”

MÉTODO DE ACCESO SEGURO A ESCUELAS E INSTITUTOS DE LA

UNIVERSIDAD CATÓLICA DE VALPARAÍSO

- MASUCV -

Trabajo de Titulación para optar al
Título de INGENIERO DE EJECUCIÓN
en SISTEMAS COMPUTACIONALES

Alumno:

Fernando Robinson Ortiz Delgado

Profesor Guía:

Dr.-Ing. Raúl Monge Anwandter

AÑO 2002

Estas palabras son para agradecer la comprensión y el apoyo de mi esposa Johana, mi hija Alicia y mi hijo Gabriel, los cuales fueron, son y serán mi sostén en ésta tarea, como en las que me depare el futuro.

Fernando

RESUMEN

El presente trabajo de titulación tiene como objetivo principal el permitir intercambiar información de los proyectos de las diferentes escuelas e institutos de Universidad Católica de Valparaíso y que son de carácter confidencial, con el resto de los miembros que conforman dichos proyectos y los cuales no se encuentran en sus dependencias.

Para satisfacer esta problemática se optó por abordarla en base a una plataforma y servicios que fuesen basados en fuente abierta, esto significa que no existe una empresa detrás de ella sino un grupo de personas las cuales utilizando como medio de intercambio Internet, desarrollan proyectos dejándolos disponibles para ser utilizados por quien lo desee. El hecho de utilizar lo antes mencionado se basa en principio en su costo el cual no existe; sin embargo lo más atractivo es que ande alguna falla, existiendo un desarrollo constante, permite que exista una solución en un corto plazo.

Para llegar a la solución primero se establecen los estándares para la existencia de una comunicación segura, realizándose para ello un análisis para constatar cual es el más adecuado, todo esto basado en tres características, autenticación, integridad y confidencialidad. Luego se realiza un sondeo de los proyectos que más se están utilizando y los cuales manejan los estándares antes establecidos, llegando por último a la gestación de la solución en sí en base a estos.

Por finalizar hay que consignar que en base a la premisa del uso de software de fuente abierta, la plataforma que se utiliza es Linux.

ÍNDICE

RESUMEN

INTRODUCCIÓN

CAPÍTULO 1 : AMBIENTE Y DEFINICIÓN DE LA PROBLEMÁTICA

- 1.1 ENTORNO ACTUAL
- 1.2 ASPECTOS RELEVANTES A LA PROBLEMÁTICA
 - 1.2.1 Origen del problema
 - 1.2.2 Identificación del problema
 - 1.2.3 Participantes involucrados en el problema
 - 1.2.4 Factores involucrados
 - 1.2.5 Información relativa al problema
 - 1.2.6 Impacto de solucionar el problema
- 1.3 ALTERNATIVAS DE SOLUCIÓN
 - 1.3.1 Visualización de soluciones
 - 1.3.2 Selección de solución
 - 1.3.3 Objetivo general al que se contribuye y objetivos específicos
 - 1.3.4 Describir el producto/servicio resultante a generar con el proyecto

CAPÍTULO 2: ESTUDIO DE REQUERIMIENTOS Y ESTADO DEL ARTE

- 2.1 ESPECIFICACIÓN DE REQUERIMIENTOS
 - 2.1.1 Control de Acceso a los usuarios
 - 2.1.2 Bajos tiempos de respuesta
 - 2.1.3 Escalable
 - 2.1.4 Estandarización

- 2.1.5 Formular estadísticas
 - 2.1.6 Independencia de terceros
 - 2.1.7 Robusto
 - 2.1.8 Adaptable a la obsolescencia
 - 2.1.9 Uso de métodos de transmisión de datos en forma segura
 - 2.1.10 Aumento de intercambio de información mediante diferentes formas
- 2.2 SERVICIOS
 - 2.2.1 Autenticación
 - 2.2.2 Privacidad
 - 2.2.3 Integridad
- 2.3 ESTADO DEL ARTE
- 2.4 IPSEC
 - 2.4.1 Descripción del protocolo IPSEC
 - 2.4.2 Aplicaciones prácticas de IPSEC
- 2.5 VPN
 - 2.5.1 VPN dinámicas
- 2.6 DISEÑO PRELIMINAR DE SALIDA
- 2.7 ESPECIFICACIONES DE HARDWARE Y SOFTWARE DE LA ALTERNATIVA SELECCIONADA
 - 2.7.1 Especificaciones de software
 - 2.7.2 Especificaciones de comunicaciones

CAPÍTULO 3 : DISEÑO E IMPLEMENTACIÓN

- 3.1 DISEÑO
- 3.2 IMPLEMENTACIÓN

CAPÍTULO 4 : EVALUACIÓN ECONÓMICA Y EXPERIENCIA

4.1 FLUJOS RELEVANTES DEL PROYECTO

4.1.1 Conceptos preliminares

4.1.2 Inversión inicial

4.1.3 Ingresos

4.1.4 Costos

4.1.5 Valor Residual

4.1.6 Flujos de caja

4.2 EXPERIENCIA

4.2.1 Problemáticas de instalación

4.2.2 Posibilidades de desarrollo

CONCLUSIONES

BIBLIOGRAFÍA

ANEXOS

ANEXO 1: ESQUEMA DE INSTALACIÓN Y CONFIGURACIÓN DE LINUX

ANEXO 2: ESQUEMA DE INSTALACIÓN DE SERVICIOS VPN

ANEXO 3: CONFIGURACIÓN DE CLIENTE WINDOWS EN AMBIENTE SEGURO

ANEXO 4: GLOSARIO

ÍNDICE DE TABLAS

Tabla 1 - 1. Soluciones a las Problemáticas

Tabla 4 - 1. Cuantificación de la inversión inicial.

Tabla 4 - 2. Valorización de la inversión inicial.

Tabla 4 - 3. Cuantificación de los ingresos proyecto puro

Tabla 4 - 4. Valorización de los ingresos.

Tabla 4 - 5 Cuantificación de los costos

Tabla 4 - 6 Valorización de los costos

Tabla 4 - 7 Flujo de caja para proyecto puro

Tabla 4 - 8 Sensibilización de Ingresos para proyecto puro.

Tabla 4 - 9. Sensibilización de los Egresos para proyecto puro.

Tabla 4 - 10 Tabla de amortización de crédito para proyecto financiado al 50%.

Tabla 4 - 11 Flujo de caja de proyecto financiado al 50%

Tabla 4 - 12 Tabla de sensibilización del ingreso para proyecto financiado al 50%.

Tabla 4 - 13. Tabla de sensibilización del egreso para proyecto financiado al 50 %.

Tabla 4 - 14 Tabla de amortización de crédito para proyecto financiado al 75%.

Tabla 4 - 15. Flujo de caja de proyecto financiado al 75 %.

Tabla 4 - 16. Tabla de sensibilización del ingreso para proyecto financiado al 75 %.

Tabla 4 - 17. Tabla de sensibilización del egreso para proyecto financiado al 75 %.

ÍNDICE DE FIGURAS

Figura 1 - 1. Organigrama Departamental de la DSIC

Figura 1 - 2. Esquema de la situación actual.

Figura 1 - 3. Esquema de la situación con solución.

Figura 2 - 1. Tecnologías utilizadas en IPSEC.

Figura 2 - 2. Estructura de un datagrama AH.

Figura 2 - 3. Funcionamiento del protocolo AH.

Figura 2 - 4. Estructura de un datagrama ESP.

Figura 2 - 5. Funcionamiento del protocolo ESP

Figura 2 - 6. Los modos de funcionamiento: transporte y túnel de IPSEC

Figura 2 - 7. Funcionamiento de protocolo IKE

Figura 2 - 8. Integración de un PKI en IPSEC.

Figura 2 - 9. Interconexión de redes locales en entorno financiero.

Figura 2 - 10. Acceso seguro de usuarios remotos a una corporación

Figura 2 - 11. Extranet aplicada.

Figura 2 - 12. Ilustración de una VPN dinámica.

Figura 2 - 13. Estadística de tráfico.

Figura 3 - 1. Esquema de interconexión de acceso seguro basado en solución propuesta.

Figura 3 - 2. Esquema de la zona confidencial de una escuela o instituto.

Figura 3 - 3 Comunicación entre el cliente VPN y el servidor de enlace VPN.

Figura 3 - 4 Diagrama de flujo de procesos

ÍNDICE DE FIGURAS ANEXAS

Figura A1 - 1. Caja con distribución RedHat de Linux.

Figura A3 - 1. Asistente de conexiones a redes.

Figura A3 - 2. Selección del tipo de conexión de red.

Figura A3 - 3. Selección de la red pública para el asistente de conexión.

Figura A3 - 4. Selección de la dirección destino del servidor de enlace VPN.

Figura A3 - 5. Selección de la disponibilidad de conexión.

Figura A3 - 6. Selección compartida de esta conexión.

Figura A3 - 7. Finalización de la conexión a una red segura.

Figura A3 - 8. Ventana de acceso a la conexión segura.

Figura A3 - 9. Ventana de conexión por medio de la cual se accede al entorno protegido.

ÍNDICE DE GRÁFICOS

Gráfico 4 - 1 Tendencia de la disminución de ingresos para proyecto puro

Gráfico 4 – 2. Tendencia de la sensibilización de los egresos para proyecto puro.

Grafico 4 - 3. Tendencia de la disminución de ingresos para proyecto financiado al 50%.

Grafico 4 - 4. Tendencia de la sensibilización del egreso para proyecto financiado al 50%.

Gráfico 4 - 5. Tendencia de la disminución de ingresos para proyecto financiado al 75%.

Gráfico 4 - 6. Tendencia de la disminución de los egresos para proyecto financiado al 75%.

INTRODUCCIÓN

Hoy por hoy la seguridad se ha vuelto un elemento fundamental en las comunicaciones, y más aún cuando la información que está transitando de un lugar a otro del mundo, al hacer uso de Internet, está a la vista y paciencia de quien tenga los conocimientos necesarios para obtenerla. Es por ello que los métodos de securización de ésta se han propagado rápidamente, siendo las redes privadas virtuales las más utilizadas en estos días.

De lo anterior se puede establecer que el uso de ésta técnica en cualquier ambiente puede brindar lo necesario para un normal desarrollo de las actividades de intercambio de información, y es por ello que la Universidad Católica de Valparaíso al encontrarse en una situación donde la información que maneja de manera confidencial eventualmente podría verse expuesta, concibe el utilizar medios como éste para salvaguardar de manera eficaz ciertas actividades, siendo los proyectos su mayor preocupación hoy día. De allí nace la inquietud de desarrollar este proyecto, el cual les permitirá entregar una forma de interactuar de manera segura en lo que dice relación con el intercambio de información entre los miembros de los proyectos, de manera tal que no se vulnere el principio de la confidencialidad, esto, debido a que no todos ellos se encuentran en las dependencias físicas de la organización.

En el capítulo 1 se abordará el medio en el cual la problemática se encuentra inserta, para posteriormente identificarla y generar una visión de las posibles soluciones a ésta. Para por último seleccionar una de ellas, basándose en cualidades como el medio de comunicación que se utilizará y quién llevará a cabo la solución.

Para el capítulo 2 se establecerán los requerimientos de las escuelas e institutos, se definirá lo que involucra la confidencialidad y se identificarán los estándares en materia de seguridad.

Posteriormente en este capítulo 3 se llevara a efecto el diseño de la solución, estableciéndose aquellas áreas que estarán siendo protegidas por la misma. Junto con

ello se definirá la forma de llevarlo a cabo, la cual conllevará desde la instalación del equipamiento hasta el momento en que se brindará el servicio y su posterior puesta en funcionamiento.

Y por último, en este capítulo 4 se establecerá la viabilidad económica del proyecto; junto con las experiencias obtenidas de los diferentes problemas que se presentaron al llevar esta a cabo, además se establecen las posibilidades de desarrollo en base a la misma.

Para finalizar, se han considerado 3 anexos en los cuales se guía en la instalación de los software que se utilizaron en la solución; sin embargo hay que hacer notar que el manejo de éste tipo de software de fuente abierta en algunos casos dificulta su uso, debido a lo engorroso que puede ser su instalación.

CAPÍTULO 1: AMBIENTE Y DEFINICIÓN DE LA PROBLEMÁTICA

1.1 **ENTORNO ACTUAL**

La Universidad Católica de Valparaíso, nace en 1928 en el mes de Marzo gracias a la generosidad de Doña Isabel Caces de Brown, quien destaca en la historia de la ciudad de Valparaíso. A su vez esta institución se vincula a la Iglesia Católica a través de la diócesis de la ciudad, por ello se tiene a un gran canciller como elemento gravitante en las decisiones de ella.

En la medida que ha transcurrido el tiempo la institución ha establecido una serie de premisas que la han llevado a constituirse en una de las 4 o 5 mejores universidades del país, es por ello que en vista de lo anterior se plasmó esto a través de una estrategia organizacional, la cual consiste en ser reconocida tanto a nivel nacional como internacional, todo lo cual se basa en un crecimiento en el saber apoyado en procesos formativos de excelencia. De aquí se puede distinguir 5 ámbitos de importancia, los cuales son: docencia, investigación, estudios avanzados, vinculación con la comunidad nacional y con el entorno internacional.

Podemos apreciar que el área de negocios de la organización es la educación, siendo el pregrado el elemento primario de atención, a éste confluyen las personas que han terminado su enseñanza media y desean obtener un primer título de carácter universitario; también tenemos que se brinda postgrados, orientados a individuos que ya poseen un título o grado y desean perfeccionarse en su área; por último tenemos las capacitaciones tanto a nivel interno como externo, trabajando en la medida que es posible en conjunto con el SENCE.

Aún cuando lo anterior es el fundamento de ser de la institución, ha aparecido un elemento que emerge de la estrategia organizacional, siendo éstos los proyectos, elementos gravitantes en el logro de las políticas institucionales; todo esto lleva a trabajar con entidades gubernamentales, la empresa privada, otras instituciones de educación superior tanto nacionales como internacionales, con lo cual se brinda la

posibilidad del desarrollo de las distintas disciplinas con que cuenta esta casa de estudios superiores y la cual es apoyada por los estamentos docentes que la componen, los cuales son las escuelas e institutos.

A los estamentos antes señalados los apoya la UIC¹ de la organización, la cual posee la experticia suficiente para llevar a buen término las actividades relacionadas con TI² y que forman parte de la mayoría de los proyectos que se concretan, es por ello que se han realizado cambios para poder lograrlo, siendo la modificación del organigrama departamental el cambio base para afrontar estos nuevos desafíos.

El esquema departamental que existía antes de este cambio era centrado en la figura del director del departamento, mientras que ahora aparecen áreas en las cuales se establecen funciones para con los diferentes ámbitos en los cuales tiene ingerencia este departamento, que se puede apreciar de mejor manera en la siguiente figura:

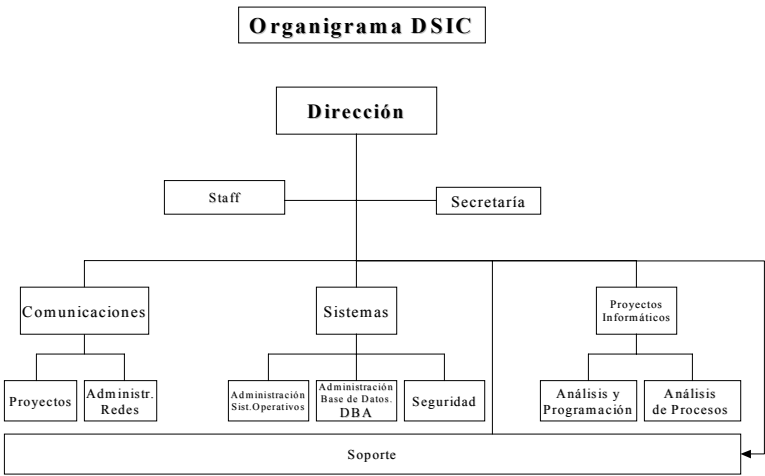


Figura 1 - 1. Organigrama Departamental de la DSIC³

¹ Unidad de Computación e Informática

² Tecnología de la Información

³ Dirección de Servicios de Informática y Comunicaciones

En vista de todo lo expuesto, son los proyectos los elementos gravitantes para la organización y esto se aprecia claramente en las palabras de la Vicerectoría Asuntos Docentes y Estudiantiles, la cual se pasa a citar: “Es el objetivo de esta Vicerectoría el promover el desarrollo de Proyectos de Mejoramiento y Calidad de la docencia de pregrado a través de la utilización de recursos tecnológicos y procesos de innovación de prácticas de docencia universitaria, en las siguientes líneas de trabajo: Uso de TICs⁴ como apoyo a la Docencia Presencial : Diseño y desarrollo de cursos mediante la utilización de la plataforma del Campus Virtual- UCV como apoyo a la docencia presencial en Asignaturas dictadas en el Segundo Semestre 2002 y/o Primer Semestre 2003”. A partir de esto se debe tener claridad el tipo de proyectos en los cuales una casa de estudios superiores participa, pudiendo ser FONDEF y FONDECYT; éstos corresponden a iniciativas de carácter estatal, en las cuales participan entidades educacionales y privadas como socios, los cuales cuentan con ciertas características y están claramente establecidas en las bases que se entregan al momento de postular, sus objetivos son:

- El aumento de competitividad de los sectores productivos del país mediante la aplicación de la ciencia y la tecnología.
- El desarrollo de la capacidad científica y tecnológica nacional en los planos institucional y geográfico.
- La vinculación entre la capacidad científica nacional y los requerimientos de las empresas chilenas.

⁴ Tecnologías de la Computación

1.2. ASPECTOS RELEVANTES A LA PROBLEMÁTICA

1.2.1 Origen del problema

Las escuelas e institutos de la Universidad Católica de Valparaíso se encuentran involucradas en proyectos, principalmente FONDEF y FONDECYT, los cuales generan una serie de información que es de carácter reservado, basado en las cláusulas existentes en los contratos que se firman y las cuales establecen lo siguiente, se pasa a citar : “Asimismo, se deja constancia que tanto durante la ejecución del PROYECTO como a su término, toda la información generada y los resultados del mismo son absolutamente confidenciales, de manera que la empresa en caso o modo alguno puede darlos a conocer a terceros sin la autorización expresa de la ORGANIZACIÓN, la que sólo podrá ser otorgada una vez que esta última haya adoptado las medidas necesarias para su protección legal, si fuera pertinente. A mayor abundamiento, la empresa se compromete a tomar los resguardos para que su personal no falte a la confidencialidad requerida para este contrato”. Todo esto viene acompañado de una segunda cláusula la cual establece lo siguiente, se pasa a citar : “Si la terminación anticipada del proyecto tuviere como causa la negligencia de la beneficiaria en el cumplimiento de sus obligaciones, previo informe del director ejecutivo y sin perjuicio de lo previsto , la beneficiaria negligente deberá restituir la totalidad del subsidio recibido medido en unidades de fomento, las que serán convertidas en moneda nacional en la fecha de devolución del subsidio”.

Aunque por los precedentes antes expuestos no se puede compartir la información generada por el proyecto, consta la posibilidad de si poder comunicar ésta a quienes sean partícipes del mismo.

1.2.2 Identificación del problema

Hoy día ciertos estamentos de la organización se encuentran envueltos en un medio que requiere que ellos entreguen información que resulta relevante para otros entes y que no se encuentran circunscritos a su ámbito de trabajo interno, es por ello que muchas veces el enviar o recibir información resulte poco fiable si se tiene como premisa que los medios con los cuales se cuenta hoy día no conceden la seguridad necesaria que dicha información pudiera requerir en un momento determinado. Por lo tanto no se tiene la certeza que esta, la información, pueda ser observada, modificada o eliminada por un agente externo y el cual no es la contraparte válida de la misma.

Hoy día el acceso a la información es más necesario que nunca dentro de la organización, es así como hay personas y entelequias (empresas) externas a ella que desean tener acceso a la misma, es por ello que dicha información se encuentra normalmente en áreas a las cuales sólo pueden acceder los integrantes del proyecto, resguardándose físicamente con porteros electrónicos. Por lo mismo el tránsito de ésta no es posible de llevar a cabo utilizando TI por la falta de un medio seguro por donde hacerla transitar y de esa manera brindarles la confiabilidad que esta requiere. Por lo tanto se utiliza el enviar ésta información mediante valijas o bien correspondencia certificada tanto a nivel nacional como internacional.

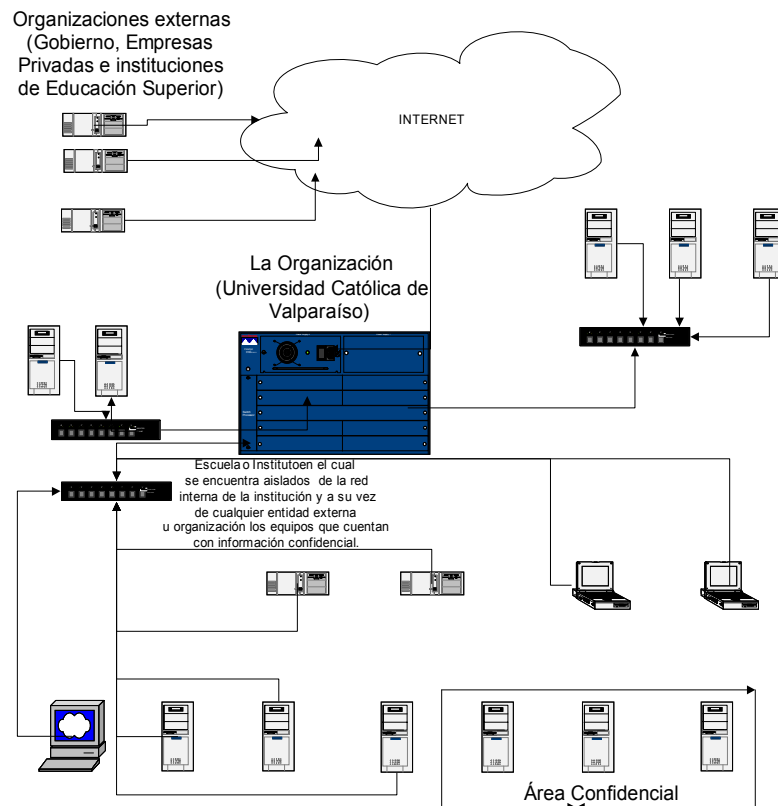


Figura 1 - 2. Esquema de la situación actual

1.2.3 Participantes Involucrados en el problema

Son los estamentos docentes de la organización, las cuales componen las escuelas e institutos, siendo éstos los precursores de la participación de la organización con los diferentes elementos externos, como lo son las empresas, el gobierno y las universidades; aunque esto eventualmente afectará al resto de la organización, en especial al aparato administrativo.

1.2.4 Factores involucrados

Tanto las empresas como el gobierno y las universidades son los actores principales en torno a esta problemática, esto debido a que son ellos los que requieren de parte de las escuelas e institutos de información que hoy día se les entrega sin la

utilización masiva de TI, por lo cual sólo pueden proveer de información poco relevante a ellos debido a que se utiliza un procedimiento manual para todo aquello que resulte ser confidencial, a partir de aquí se puede apreciar que no es la forma óptima que se desearía utilizar para este tipo de situaciones, pensando que éste es un medio finito y no escalable, por ejemplo un cdrom, esto pensando en la existencia de un gran volumen de información disponible.

1.2.5 Información relativa al problema

En base a observaciones que se han realizado se pudo establecer la importancia de contar con una solución que permita ampliar la posibilidad de tener un trabajo más expedito con respecto a la entrega de información de carácter confidencial, para ello se considera que la utilización de TI es un elemento que brindaría el empuje necesario para poder lograr un desenvolvimiento mayor. Teniendo en vista que hoy día tanto las empresas estatales como las privadas ven en organizaciones como ésta, una universidad, se puede obtener la experticia del equipo humano que allí labora vinculado con la infraestructura existente, es que se pueden lograr hitos que de trabajar en solitario no podrían ser alcanzados.

1.2.6 Impacto de solucionar el problema

Los beneficios son múltiples, éstos comienzan con el poder contar con la asesoría de una organización educacional la cual cuenta con los recursos humanos y de infraestructura acorde a los desafíos que marcan la búsqueda de soluciones, a problemáticas apoyándose en la capacidad de poseer una visión para el establecimiento de necesidades antes no expuestas, lo que significa un extra a lo que a simple vista se puede apreciar. Además redunda en la capacidad de poder tener más opciones en la adjudicación de nuevos proyectos y su figuración tanto a nivel nacional como

internacional en las diferentes áreas en las cuales puede verse envuelto por la gran diversidad con que cuenta dentro de los diferentes estamentos docentes.

1.3 ALTERNATIVAS DE SOLUCIÓN

1.3.1 Visualización de soluciones

Se visualizan las siguientes soluciones a la problemática:

Externalizar la solución (Alternativa 1): Esto consistiría en traspasar el problema a una empresa externa la cual proveería una solución, en pocas palabras se haría outsourcing.

Acceso conmutado y seguro (Alternativa 2): A través de una empresa de telecomunicaciones se brindaría el acceso a la organización por medio de un sistema conmutado, con un pool de módems, para posteriormente la organización validar quién está ingresando.

Acceso vía Internet de modo seguro (Alternativa 3): Utilizar la red global llamada Internet, como medio de ingreso a la organización, junto con esto se le entregaría un acceso seguro al área que se determine.

Acceso mediante líneas dedicadas (Alternativa 4): Utilización de líneas proporcionadas por compañías de Telecomunicaciones y que son de exclusivo uso de quien las contrata, en este caso la organización, dejando la validación de quien ingresa a la organización.

De acuerdo a lo anterior se obtiene la siguiente tabla:

Tabla 1-1 Soluciones a las Problemáticas.

Ítemes	Alternativa 1	Alternativa 2	Alternativa 3	Alternativa 4
Factibilidad Operativa	4	4	4	3
Impacto en el Desarrollo personal	1	2	4	2
Cambio en el modo de Trabajo	4	3	4	3
Aceleración en la toma de decisiones	3	3	4	3
Mejoramiento de los procesos	2	3	3	3
Disponibilidad de Recursos Humanos	4	2	2	2
Grado de estructuración que apoya	4	4	4	4
Dificultad Organizacional o compromiso del Usuario	2	3	4	3
Innovador	3	3	4	3
Marca una diferenciación	3	2	4	2
Impacto en la Organización.	4	3	3	3
Disponibilidad	3	3	4	4
Experiencia	4	4	4	4
Confidencialidad	2	2	4	3
Total	43	41	52	42

Donde Excelente tiene el valor 4, Bueno tiene un valor 3, Aceptable un 2, Deficiente un 1 y Malo un 0.

1.3.2 Selección de solución

De la tabla 1-1 se puede establecer que la alternativa 3 sería la mejor. Esto en principio por ser aquella que mejor evaluación obtuvo tomándose en cuenta los ítemes que se consideraron, en conjunción con lo anterior hay que hacer notar 3 componentes que toman gran relevancia y los cuales son: el entorno en el cual se ve inscrito, el cual es ni más ni menos que Internet, con lo cual la cobertura que se brinda es la más grande que existe en nuestros días; también se considera el aspecto de investigación el cual la UIC viene desplegando desde hace un tiempo y que lo hace aparecer como una entidad que goza de un beneficio extra con respecto al resto y, por último, algo que es el punto álgido de la problemática y la cual lo constituye la confidencialidad. Esta última puede ser llevada en algún grado de responsabilidad - ya sea alto, medio o bajo - por alguna unidad externa, nunca podrá equipararse con un trabajo interno, utilizando para ello a la UIC, que tiene un principio de lealtad con la institución.

1.3.3 Objetivo general al que se contribuye y objetivos específicos.

Con esta solución se accede a la organización teniendo en mente la seguridad de que los trabajos que se realizan sean en gran medida, inmunes a ser manipulados por personas ajenas a las que están participando en la intercambio de la misma. Pero específicamente ayuda a las escuelas e institutos a establecer un medio a través del cual podrá ser parte de proyectos que involucren confidencialidad, todo lo cual lleva a pensar en planes de gran envergadura teniendo como respaldo este nuevo entorno.

1.3.4 Describir el producto/servicio resultante a generar con el proyecto

El producto que resulta es la especificación de una infraestructura la cual constaría de una antesala “lógica” de recepción de los requerimientos de acceso a la organización, se entiende por lógica aquella que dice referirse a un espacio intangible el cual consta de una interfaz de comunicación, la cual pasa por un equipamiento que recibe y utiliza ésta para llevar y traer los datos de un extremo a otro. En este esquema se contempla lo siguiente:

- Un equipamiento activo de comunicaciones el cual recibirá las peticiones de conexiones hacia el interior de la Institución, específicamente al área definida por las escuelas y/o institutos que lo requieran.
- Junto con lo anterior se proveerá de un segundo equipamiento de comunicaciones o bien de un software que se anexaría el descrito en el punto anterior por medio del cual se permitirá establecer la creación de un “túnel”⁵ el cual suministrará la comunicación que goza de seguridad entre un extremo y otro de la misma, siendo esta última un sujeto fuera de las potestades de la organización.

Este se puede apreciar en mejor a través de la siguiente figura:

⁵ túnel: esquema de conexión de comunicación que se establece una vez que se ha negociado entre los dos extremos el inicio de la misma.

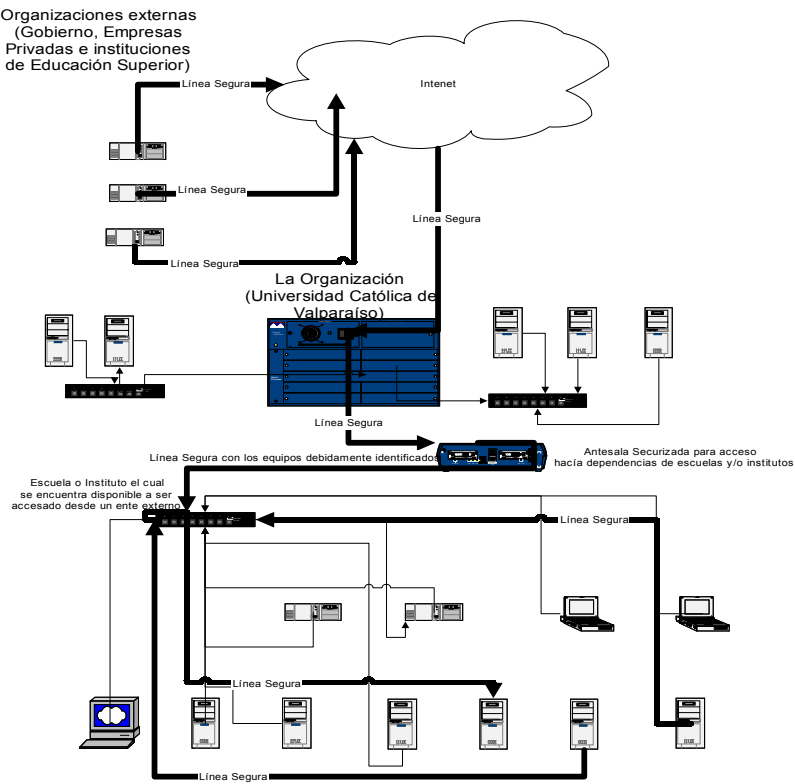


Figura 1 - 3. Esquema de la situación con solución.

CAPÍTULO 2: ESTUDIO DE REQUERIMIENTOS Y ESTADO DEL ARTE

2.1 ESPECIFICACIÓN DE REQUERIMIENTOS

De acuerdo a una definición entregada por los usuarios, considérese como estos a los docentes o investigadores, se extraen los siguientes requerimientos:

2.1.1 Control de acceso a los usuarios

Debido a que la información es un elemento que en nuestro caso es de tipo confidencial, es necesario establecer quiénes tienen derecho a usufructuar de ella.

2.1.2 Bajos tiempos de respuesta

La facilidad y rapidez en el acceso a la información hace necesario que la obtención de ésta sea lo mas expedita posible.

2.1.3 Escalable

Aún cuando hoy día pudiera haber un uso exiguo del medio por el cual se está accediendo a la información, se vislumbra un nivel de crecimiento relativamente alto en un corto plazo, basado en la incorporación de nuevos actores que estarían involucrándose.

2.1.4 Estandarización

Hoy por hoy la existencia de estándares en todo orden de cosas es grande, por ello es necesario que se establezca aquel que englobe al resto de manera tal de que haya una sola medida a ser considerada.

2.1.5 Formular estadísticas

Ya teniendo a la escalabilidad como un elemento a considerar, resulta necesario a su vez contar con alguna forma de poder establecer cuándo realizar un mejoramiento tomando como base el uso que se hace de la solución.

2.1.6 Independencia de terceros

Aún cuando existen empresas que pueden brindar este tipo de servicios, llámense empresas de telecomunicaciones, por la importancia que tienen los proyectos en los que se participa es necesario que este trabajo lo realice el área que brinda este tipo de servicios en la organización y que corresponde a la UIC de la organización.

2.1.7 Robusto

El continuo ir y venir de las tecnologías hace necesario que se cuente con un elemento que posea la capacidad de ir evolucionando de acuerdo a los nuevos elementos que se vayan presentando en el área, esto corresponde a nuevas funcionalidades que van de la mano de nuevas prestaciones que se establezcan.

2.1.8 Adaptable a la obsolescencia

Normalmente cuando se habla de soluciones que involucran tecnología siempre se piensa en la vida útil que va a prestar, es por ello que es necesario que ésta posea la cualidad de ir evolucionando de manera tal de evitar esta situación.

2.1.9 Uso de métodos de transmisión de datos en forma segura

Es necesario que las partes involucradas tengan la certeza que lo que se trafica entre ellos no puede ser manipulada de alguna forma por terceros.

2.1.10 Aumento de intercambio de información mediante diferentes formas

Así como hoy existe necesidades puntuales como lo puede ser el envío de archivos, debe considerarse que la información puede ser puesta a disposición de las escuelas e institutos, esto puede ser por medio de una base de datos o una página Web.

2.2 **SERVICIOS**

A partir de los requerimientos anteriormente señalados se establece que deben existir una serie de servicios que son necesarios para poder acometer de buena manera el logro de estos.

A continuación se presentan los servicios a considerar:

2.2.1 Autenticación

Es la forma por medio de la cual se establece que el sujeto que está intentando acceder a la información que se encuentra disponible en equipos que no están a la vista de cualquiera, se validen por algún medio. Para ello existen varios métodos. Los métodos criptográficos son los más usados en redes, donde se destacan dos:

- Validación mediante la utilización de un secreto compartido, el cual consiste en la utilización de ciertas funciones a través de las cuales se genera una cadena de

caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación; aún cuando resulta ser una buena manera de proveer este servicio, en esta metodología se gesta una cadena diferente para cada par de nodos que desean comunicarse.

- Uso de certificados digitales, con lo cual podemos distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía.

2.2.2 Privacidad

A lo anterior se debe asociar el servicio que proveerá el cifrado de los datos que viajan de un punto a otro en la comunicación que se esta realizando y, aunque puede ser visto por terceros, estos son incapaces de saber lo que se está intercambiando.

2.2.3 Integridad

Por último, se nos presenta un servicio que consiste en mantener la integridad de los datos que se encuentran circulando entre los extremos que establecen la comunicación, ante esto se debe contar con algún método que permita certificar que lo que está llegando es lo que realmente fue enviado desde el origen.

2.3 ESTADO DEL ARTE

Después de establecer los servicios que son necesarios a considerar para lograr satisfacer los requerimientos antes mencionados, apreciamos que en el orbe tenemos tres grandes estándares, los cuales son: PPTP⁶, L2TP⁷ e IPSEC⁸.

De estos podemos decir que en el primer caso, PPTP, es una especificación desarrollada por varias compañías. Normalmente se asocia con Microsoft ya que Windows incluye soporte para establecer este protocolo; sin embargo hoy día Linux también lo utiliza. La mejor característica de PPTP radica en su habilidad de soportar protocolos no IP; sin embargo el principal inconveniente es su fallo al elegir una única encriptación y autenticación estándar, lo cual lleva a que dos productos que acceden con la especificación PPTP puede llegar a ser completamente incompatibles, simplemente porque la encriptación de los datos es diferente.

La segunda opción que se encuentra en el mercado es L2TP, el cual consiste en la unión de PPTP y L2F que fue desarrollado por CISCO, creándose el estándar antes mencionado. Este protocolo existe en la capa de enlace de datos del modelo ISO/OSI⁹. L2TP al igual que PPTP soporta clientes no IP, pero también conserva los problemas al definir una encriptación estándar.

Por último tenemos a IPSEC, que está constituido de una colección de múltiples protocolos relacionados y posee la facilidad de ser una solución completa o bien brindar un esquema del tipo PPTP o L2TP. Existe en la capa de red del modelo OSI, para de esa manera extender IP en el soporte de servicios más seguros basados en Internet.

⁶ Point to Point Tunneling Protocol

⁷ Layer two Tunneling Protocol

⁸ Internet Protocol Security

⁹ International Organization for Standardization/Open Systems Interconnection

Después de haber analizado los diferentes estándares que resultan ser más dominantes, se concluye, que IPSEC por la robustez que éste presenta es la elección a utilizar.

2.4 IPSEC

Como se había establecido anteriormente, IPSEC es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros).

Este viene a llenar un espacio dentro de lo que es la seguridad en las comunicaciones, porque hasta antes de su aparición todas las soluciones eran propietarias, lo cual provocaba que existiese una falta de interoperatividad en el establecimiento de comunicaciones seguras.

Este estándar tiene una ventaja que lo hace destacar sobre sus competidores y el cual consiste en estar apoyado en estándares del IETF¹⁰, lo cual proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSEC se integra en la versión actual de IP (IP versión 4) y, lo que es muy importante, es que por omisión también está incluida en la versión 6 de la misma. Otra de las características destacables de IPSEC es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI¹¹ y, aunque establece ciertos algoritmos comunes, por razones de interoperatividad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Entre los beneficios que aporta IPSEC, cabe señalar que:

¹⁰ Fuerza de tarea de Ingeniería de Internet

¹¹ Infraestructura de clave pública

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la cual realizar transacciones usando cualquier aplicación. Las extranets son un ejemplo.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el costo de líneas dedicadas.
- Ofrece al tele trabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad de tránsito.

Aquí es importante el siguiente alcance, cuando se habla de “seguro” se refiere no sólo a la confidencialidad de la comunicación, sino también a la integridad de los datos.

2.4.1 Descripción del protocolo IPSEC

IPSEC, como se mencionó anteriormente, es un conjunto de estándares que se unen para poder integrar en IP funciones de seguridad basadas en criptografía. Proporcionan con ello confidencialidad, integridad y autenticidad de datagramas IP, combinando diferentes tecnologías como lo son: clave pública (RSA), algoritmos de cifrado simétrico (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales (X509v3). A continuación se puede apreciar en la figura lo antes expresado.



Figura 2 - 1. Tecnologías utilizadas en IPSEC

El protocolo IPSEC resulta ser modular, lo cual permite que se pueda seleccionar los algoritmos que uno desee sin afectar a otras implementaciones que se puedan estar realizando; sin embargo se han establecidos ciertos algoritmos estándares que debe soportar cualquier implementación para de esa manera asegurar la interoperatividad en el mundo de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado simétrico, así como MD5 y SHA-1, como funciones de hash. Pero como se explicó anteriormente es posible el uso de otros algoritmos que pudieran ser considerados más seguros o bien más adecuados para un entorno específico: como por ejemplo, para lo que es cifrado de clave simétrica IDEA, Blowfish o el más reciente AES.

Dentro del protocolo IPSEC se distinguen los siguientes componentes:

- Dos protocolos de seguridad IP: Authentication Header (AH) e Encapsulating Security Payload (ESP) que proporciona mecanismos de seguridad para proteger el tráfico IP.
- Un protocolo de gestión de claves, Internet Key Exchange (IKE), que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El protocolo AH, es el procedimiento previsto dentro de IPSEC para garantizar la integridad y autenticación de los datagramas IP. Con lo cual proporciona un medio al receptor de los paquetes IP, para autenticar el origen de los datos y al mismo tiempo

verificar que dichos datos no han sido alterados en su viaje. Pero no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

Tal como lo indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, el cual puede ser un mensaje TCP, UDP, ICMP o bien un datagrama IP completo. Este protocolo IP es relativamente nuevo y su principal cualidad es que indica la naturaleza de los datos de la capa superior por medio del valor que se le asigna y que es 51 en vez de los valores 6 o 17 que se asocian a TCP y UDP respectivamente. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, exceptuando los campos variables como: TOS, TTL, flags, offset y checksum. Para tener una mejor visión de lo antes expuesto se presenta la siguiente figura:

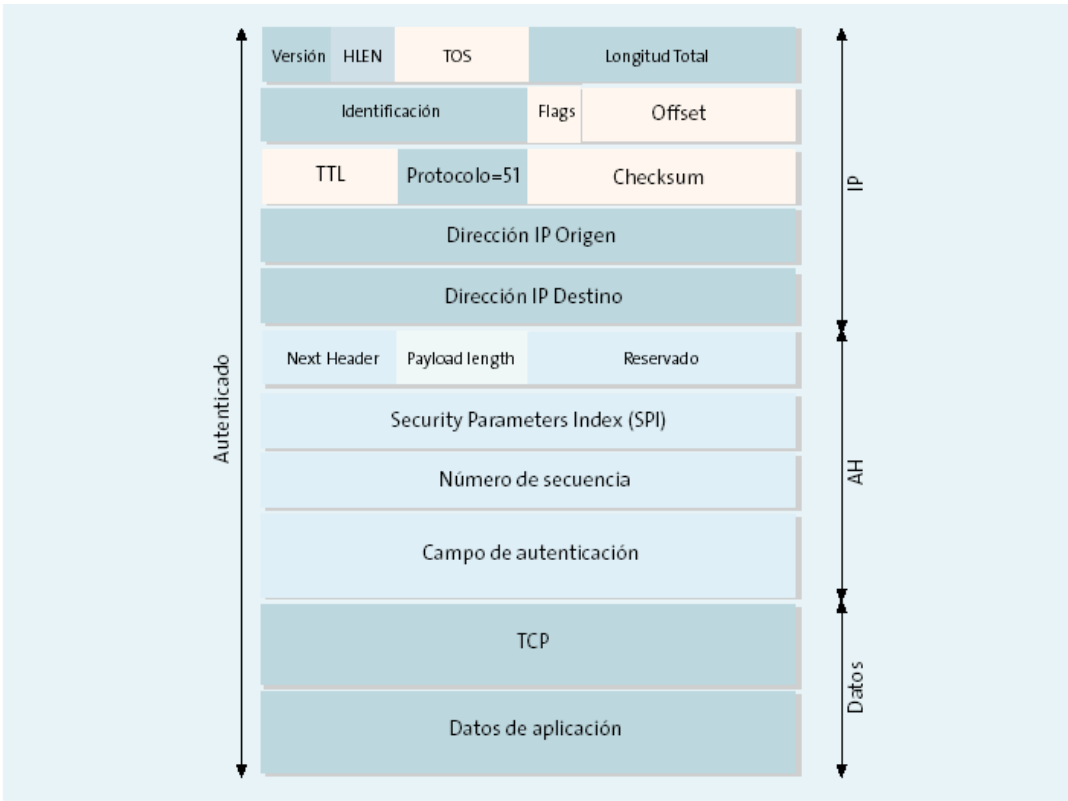


Figura 2 - 2. Estructura de un datagrama AH

El funcionamiento de este protocolo se basa en el algoritmo HMAC¹², el cual es un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función de hash a la combinación de datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que se denomina extracto, que tiene la propiedad de ser como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave. En la siguiente figura se muestra como trabaja el protocolo.

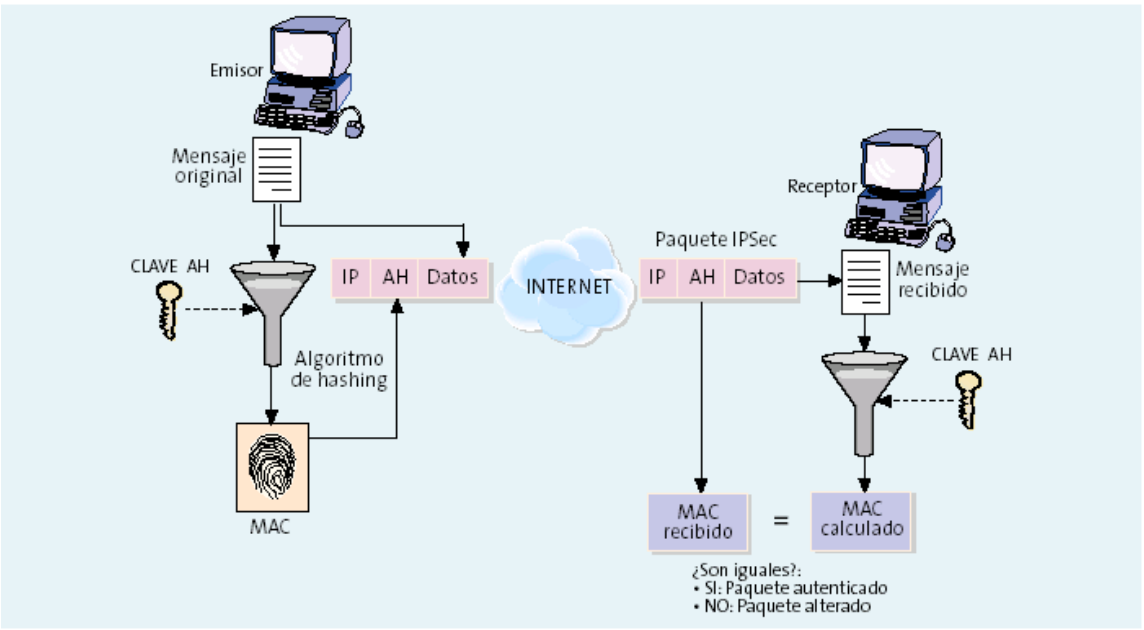


Figura 2 - 3. Funcionamiento del protocolo AH

Si analizamos con detalle el protocolo AH, se concluye que su seguridad reside en que el cálculo del extracto (MAC) es imposible de generar y verificar sino se tiene la clave, y dicha clave, como lo muestra la figura 2 - 3, sólo la conocen el emisor y el receptor.

¹² MAC con hash, donde MAC es Código de autenticación de mensaje.

Además del protocolo AH, existe ESP¹³, que a diferencia del anterior tiene como principal objetivo proporcionar confidencialidad. Para lograrlo se especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente provee servicios de integridad y autenticación del origen de los datos similar a AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; éste consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden pertenecer a protocolo TCP/IP (por ejemplo, TCP, UDP o ICMP). En la figura que se presenta a continuación se muestra la estructura del datagrama ESP.

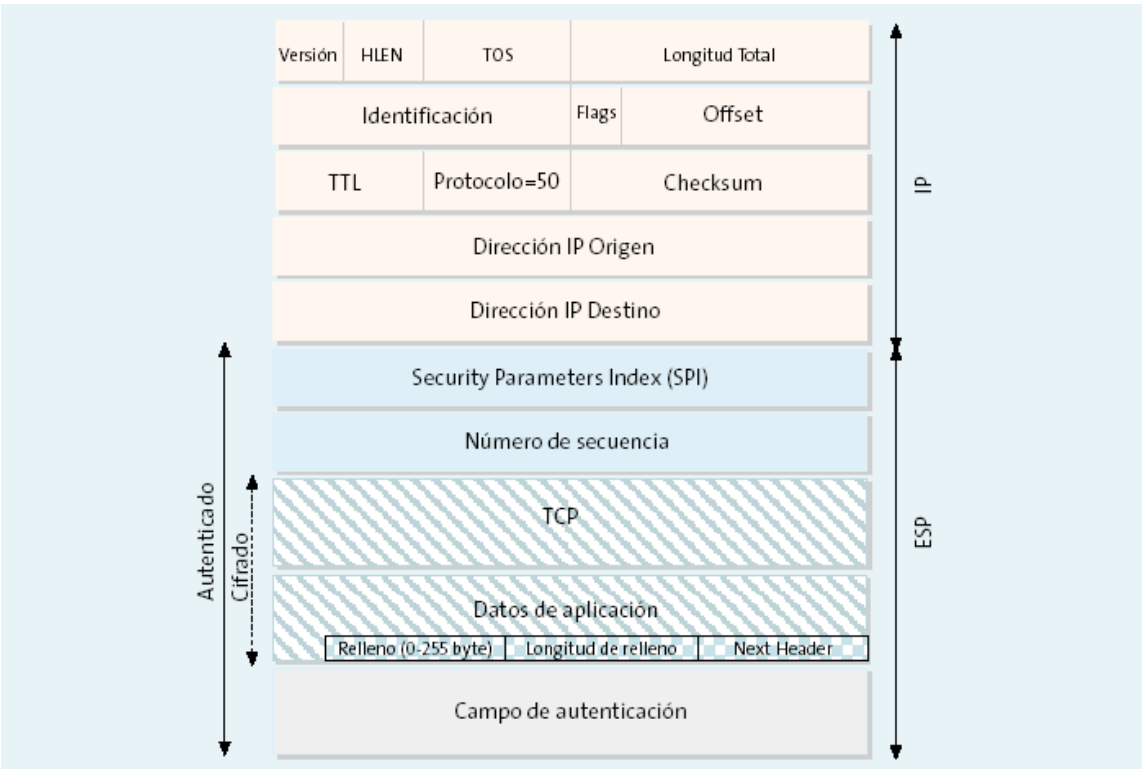


Figura 2 - 4. Estructura de un datagrama ESP

¹³ Encapsulating Security Payload

En la imagen se aprecia cómo el contenido de la carga útil viaja cifrado.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado de bloque, de modo que la longitud de los datos a cifrar tiene que ser múltiplo del tamaño del bloque (8 o 16 bytes en la mayoría de los casos). Es por ello que existe un campo de relleno, tal como se aprecia en la figura 2 - 4, el cual tiene una función adicional y que consiste en poder añadir caracteres de relleno al campo de datos para ocultar así su longitud real, y por lo tanto, las características del tráfico; junto con lo anterior debe también ser múltiplo exacto del tamaño del bloque. En la siguiente representación se presenta cómo este protocolo permite enviar datos de forma confidencial.

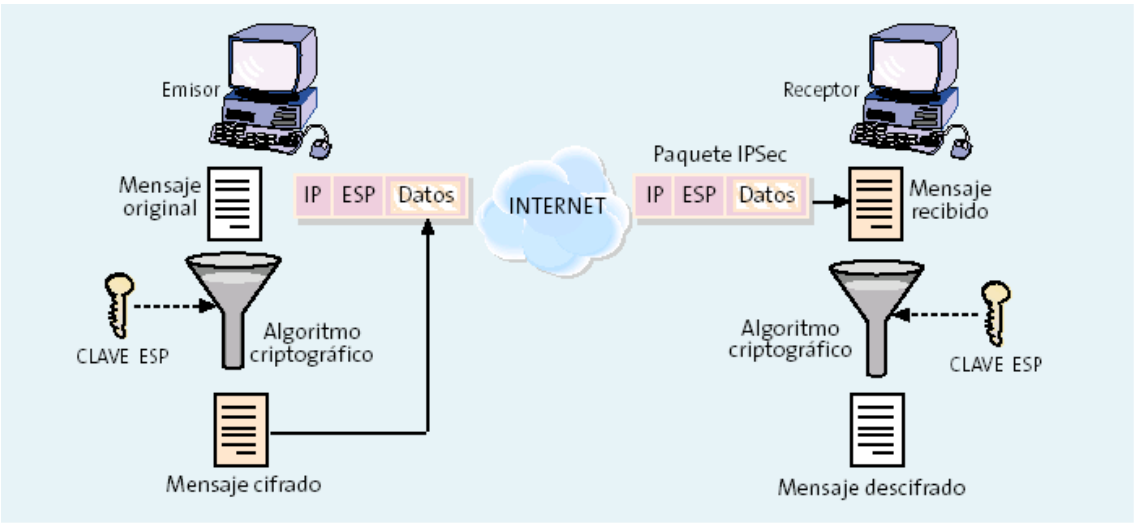


Figura 2 - 5. Funcionamiento del protocolo ESP

Como se ve en la figura 2 - 5 este protocolo basa su robustez en el algoritmo de cifrado, es decir, que si alguien quisiera descifrar lo que está transitando entre el emisor y el receptor no podría realizar dicha tarea sin conocer la clave, la cual sólo es conocida por el emisor y el receptor.

Después del análisis de los protocolos AH y ESP, es necesario ver los modos de funcionamiento que permite IPSEC. Tanto ESP como AH proporcionan dos modos de uso:

- El modo transporte. En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por lo tanto, la cabecera IPSEC se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. Este modo tiene la ventaja que se asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSEC.
- El modo túnel. En éste el contenido del datagrama AH o ESP es un datagrama completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSEC. Este modo es empleado principalmente por los gateways IPSEC, con el objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el proceso de tráfico IPSEC en un equipo. También es útil cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación de este modo, ya sea utilizando ESP o AH, es poder establecer Redes Privadas Virtuales (VPN) a través de redes públicas, es decir interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet.

A continuación se presenta un retrato que mostrará lo antes explicado.

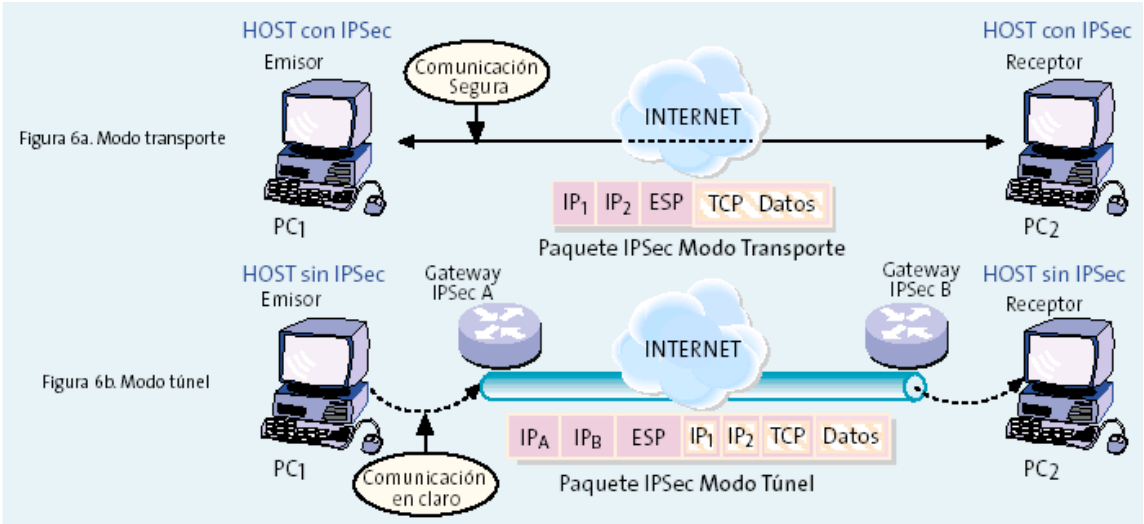


Figura 2 - 6. Los modos de funcionamiento: transporte y túnel de IPSEC

Como se ha visto la distribución de claves seguras es un requisito esencial para el funcionamiento de ESP como de AH, además que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash, como en el resto de los parámetros. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE¹⁴.

El protocolo IKE lo definió el IETF para realizar tanto la función de gestión automática de claves como del establecimiento de las SAs, las cuales consisten en comunicaciones unidireccionales que conectan dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Para comunicación bidireccional se requieren dos SAs.

El objetivo principal del IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades. Dicha negociación se lleva a cabo en dos fases:

- La primera es la fase común a cualquier aplicación, y es en la que ambos nodos establecen un canal seguro y autenticado. Esto se consigue mediante el uso de un algoritmo de cifrado simétrico y un

¹⁴ Internet Key Exchange

algoritmo HMAC y las claves se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Se hace notar que este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.

Existen varios métodos de autenticación, los dos más comunes se describen a continuación: El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales. En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la PKI (Infraestructura de Clave Pública), cuya integración se tratará con detalle más adelante.

- En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec. Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

En la figura 2 - 7 se representa de forma esquemática el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH.

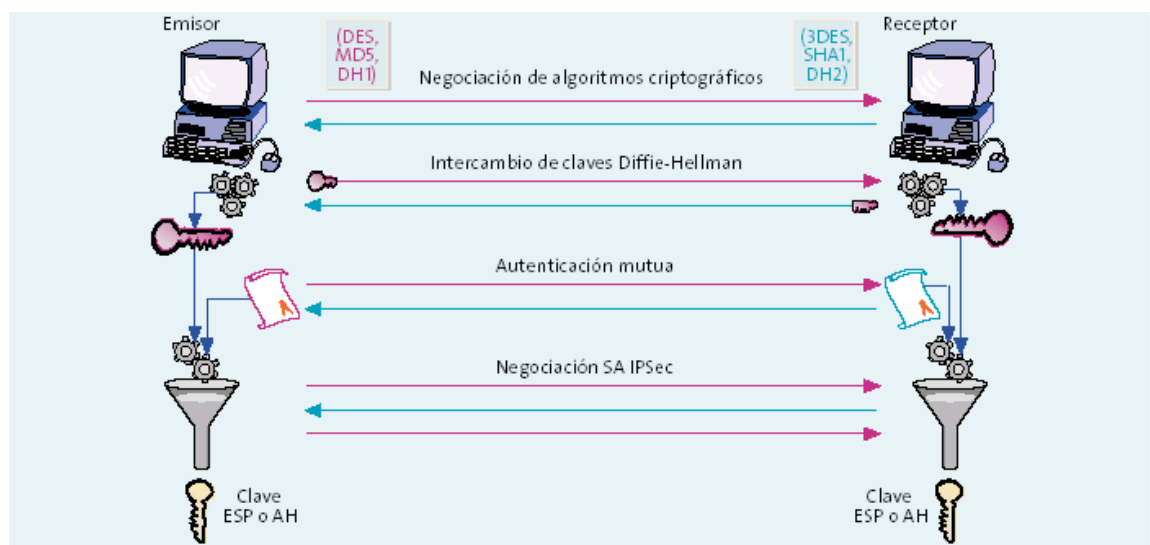


Figura 2 - 7. Funcionamiento de protocolo IKE

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. La existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación de IPSec en un entorno de teletrabajadores o usuarios móviles.

Bajo el nombre de PKI¹⁵ se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS¹⁶, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la CA¹⁷ en adelante, integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3, este consiste de una serie de campos que permiten tener la certeza que quien dice ser es quien es, siendo estos: la versión del número de serie que corresponde a la identificación del nombre basado en el algoritmo de criptografía del remitente, a continuación se tiene el período de la validez del nombre del portador del certificado,

¹⁵ Infraestructura de Clave Pública

¹⁶ Servicio de Resolución de Nombres

¹⁷ Autoridad de Certificación

luego la llave pública del portador del certificado más el de la identificación del algoritmo criptográfico con la llave pública de la identificación exclusiva del remitente y posteriormente la identificación exclusiva del portador del certificado más los campos para las extensiones y la información extra que incluye al algoritmo de la firma de la Autoridad Certificadora, todo esto es el formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado. Esto hace que existan varias alternativas según el fabricante de que se trate. En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la CRL¹⁸, que se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta LDAP¹⁹ al directorio de la PKI. Típicamente, los periodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación. Para la solicitud y descarga de certificados existe un protocolo denominado SCEP²⁰, que se ha convertido en un estándar de facto en las operaciones de registro y descarga de certificados para aplicaciones IPSec. SCEP es un protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS²¹, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados.

¹⁸ Lista de Certificados Revocados

¹⁹ Lightweight Directory Access Protocol

²⁰ Simple Certificate Enrollment Protocol

²¹ Public-Key Cryptography Standards

En la figura 2 - 8 se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL.

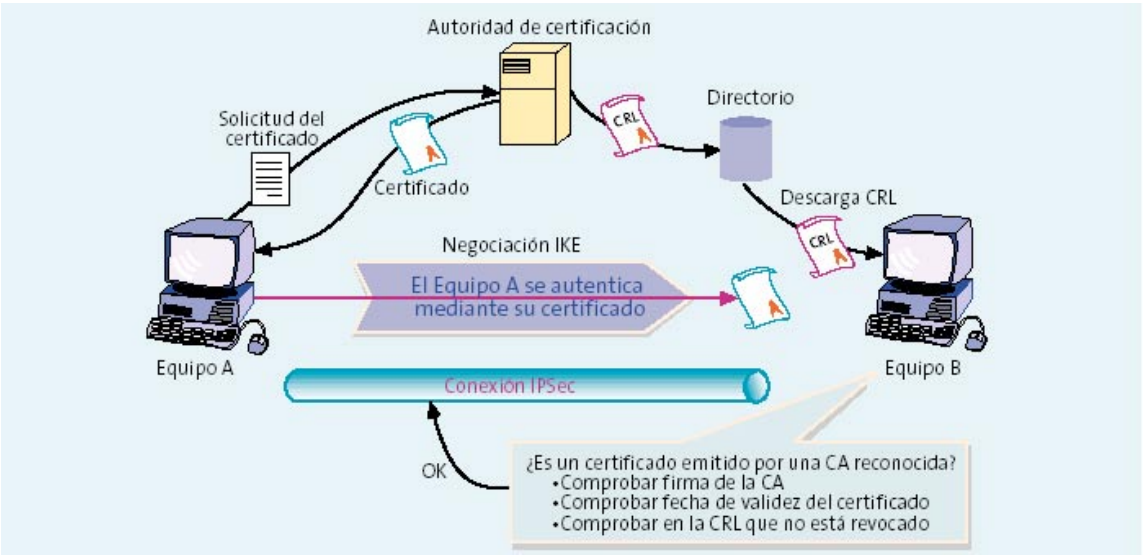


Figura 2 - 8. Integración de un PKI en IPSEC.

A continuación se analizan las características de los servicios de seguridad que ofrece IPSEC. Dichos servicios son:

- Integridad y autenticación del origen de los datos: El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se

comentó anteriormente, esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

- Confidencialidad: El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido. Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Ésta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado. El análisis de tráfico es un riesgo que debe considerarse seriamente, recientemente se ha documentado la viabilidad para deducir información a partir del tráfico cifrado de una conexión SSH. Es previsible que este tipo de ataques se harán más habituales y sofisticados en el futuro, conforme se generalice el cifrado de las comunicaciones.
- Detección de repeticiones: La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un

número de secuencia incluido en la cabecera ESP o AH, el emisor incrementa dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados. Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

- Control de acceso: autenticación y autorización: Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec, esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen y destino, el byte TOS ²² y otros campos. Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro corporativo, pero impidiendo el paso de tráfico hacia máquinas especialmente protegidas.
- No repudio: El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma

²² Type Of Service

digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

2.4.2 Aplicaciones prácticas de IPSEC

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cuál sea el medio de transporte (FR, PPP, xDSL o ATM). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP. A continuación se presenta cómo el protocolo IPSec proporciona una solución viable para tres escenarios:

- Interconexión segura de redes locales.
- Acceso seguro de usuarios remotos.
- Extranet o conexión de una corporación con partners y proveedores.

Para cada uno de los escenarios veremos cómo se desarrolla una aplicación práctica concreta y se presentan las ventajas de utilizar IPSec.

1. La interconexión segura de redes locales (intranet). En la mayoría de las corporaciones se utiliza IP como medio de transporte universal; las que todavía no usan IP tienen planes de migrar completamente a esta tecnología en un futuro próximo, es así como Novell en sus productos está utilizando IP en vez de IPX, sin abandonarlo por completo, debido a que TCP/IP es de facto el protocolo por excelencia. Asimismo, la

naturaleza distribuida de las empresas hace necesaria una infraestructura de comunicaciones que interconecte todas sus oficinas o puntos de venta. Por *intranet* se entiende una red de comunicaciones basada en una infraestructura de comunicaciones pública o privada que conecta todos los puntos de trabajo de una empresa y que tiene como medio común IP. En la Figura 2 - 9 se muestra un ejemplo de intranet.

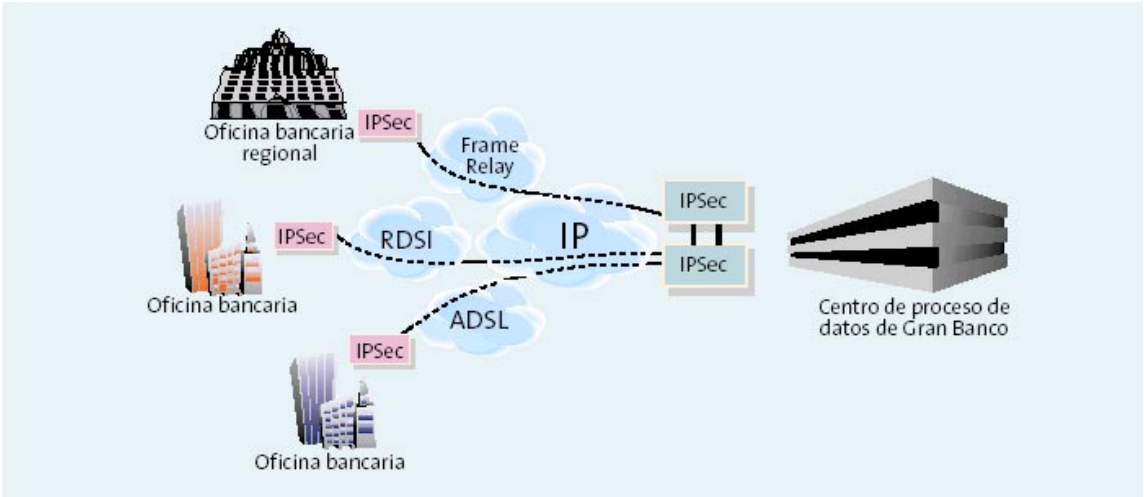


Figura 2 - 9. Interconexión de redes locales en entorno financiero.

Dicha intranet conecta todas las oficinas bancarias con el centro de proceso de datos (CPD) de un gran banco. La seguridad es vital en este entorno, y los requisitos de confidencialidad e integridad de las comunicaciones se cubren perfectamente mediante el uso de la tecnología IPSec. En la actualidad, incluso las oficinas bancarias más pequeñas disponen de una infraestructura informática que consta de una red local con varios PCs que usan una variedad de aplicaciones y protocolos para los que es imposible o muy costoso añadir mecanismos de seguridad. Sin embargo, todo el tráfico de esta red local está basado en IP o puede ser encapsulado en IP, de modo que la instalación de un gateway IPSec es la mejor solución para garantizar la seguridad de las comunicaciones de la oficina con el exterior. Como puede observarse en la Figura 1-12, es habitual que

las oficinas bancarias, debido a su elevado número, presenten una gran diversidad de tecnologías de acceso. Para grandes bancos con presencia multinacional y oficinas dispersas en muchos países esta diversidad será mayor, de forma que incluso podría plantearse la conexión de algunas oficinas directamente a través de Internet. En cualquier caso, IPSec garantiza la protección de las comunicaciones con independencia de la tecnología de acceso empleada. En cuanto al centro de proceso de datos, los requisitos críticos son la fiabilidad y la capacidad para mantener un elevado número de sesiones simultáneas. En el mercado están disponibles *gateways* IPSec comerciales que incorporan la posibilidad de configuración redundante y el establecimiento de 25.000 túneles simultáneos o más. Estas prestaciones son suficientes incluso para las redes bancarias más grandes.

2. El acceso seguro de usuarios remotos. La gran mayoría de las empresas necesitan proporcionar a sus usuarios algún procedimiento para el acceso remoto a los recursos corporativos. Estos usuarios con necesidades de acceso remoto pueden ser agentes de ventas, tele trabajadores o directivos en viaje de negocios; en todos los casos se requiere la necesidad de poder acceder de forma segura a los sistemas informáticos de la empresa a cualquier hora y desde cualquier lugar, incluso del extranjero. Además, las previsiones de futuro apuntan a que estas necesidades de acceso remoto van a crecer espectacularmente. La tecnología IPSec permite comunicar el PC del usuario remoto a las máquinas del centro corporativo, de modo que se soporten todas las aplicaciones IP de forma transparente. Mediante la instalación de un software en el PC, denominado "cliente IPSec", es posible conectar remotamente dicho equipo móvil a la red local de la corporación de forma totalmente segura, con la ventaja de que el usuario remoto, desde cualquier lugar del mundo, del mismo modo que si estuviese físicamente en su oficina, podrá:

- Leer y enviar correo.
- Acceder a discos compartidos en red.
- Acceder al servidor Web corporativo.

- Consultar la agenda.
- Utilizar la red de VOIP²³ con que pudiera contar la empresa

El uso del estándar IPSec permite garantizar la confidencialidad y la autenticación de las comunicaciones extremo a extremo, de modo que esta solución de acceso remoto se integra perfectamente con los sistemas de seguridad de la red corporativa.

En la Figura 2 - 10 se presenta un escenario típico de acceso remoto seguro a una corporación.

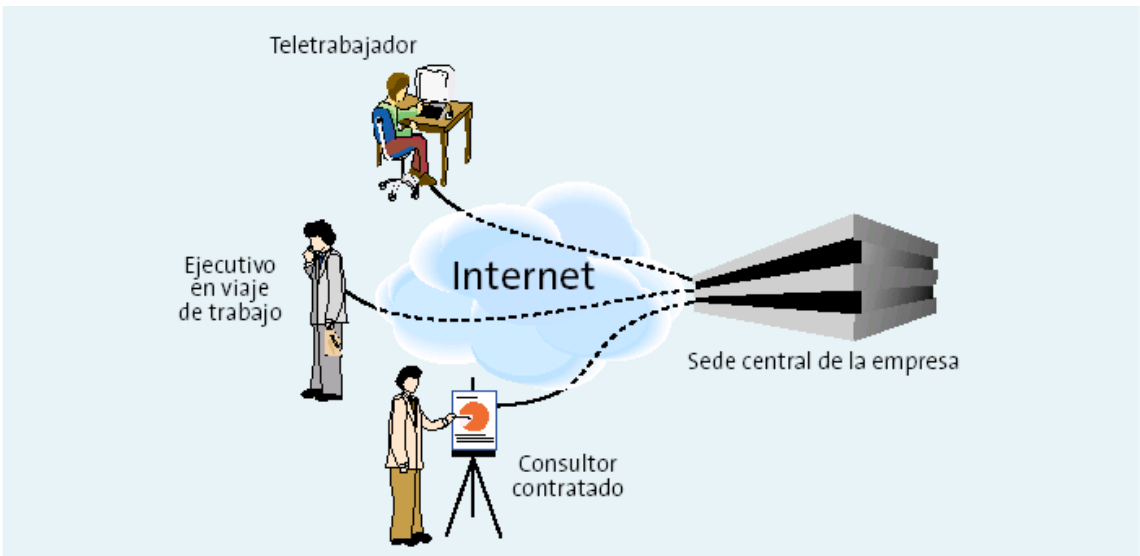


Figura 2 - 10. Acceso seguro de usuarios remotos a una corporación

Como nos podemos dar cuenta, en cualquier compañía del sector de las tecnologías de la información, se comparte una serie de características únicas. Podemos destacar la deslocalización de los recursos humanos, ya que cada vez es más habitual que los empleados trabajen fuera de su oficina, bien por estar en viaje de trabajo o bien

²³ Voz sobre ip

por estar en su casa como tele trabajadores. También será muy frecuente la colaboración en proyectos de consultores externos contratados, para los cuales es necesario habilitar acceso a los recursos de la empresa. Dada la creciente competitividad en el sector informático, la protección de la propiedad intelectual, de la información estratégica y de nuevos productos, e incluso de la propia imagen de la empresa, imponen requisitos de control de acceso y de confidencialidad que hacen imprescindible la implantación de un sistema de acceso remoto que sea suficientemente seguro. El protocolo IPSec permite construir una solución que cumple estos requisitos de seguridad. En este entorno, los usuarios remotos dispondrán de un software instalado en su PC de trabajo que les permitirá establecer una conexión segura con la red local de la compañía. La variedad de sistemas operativos no supone dificultad alguna, ya que todos los sistemas operativos recientes como Windows 2000 o Solaris 9 incluyen un cliente IPSec. Asimismo, para los sistemas operativos más difundidos, y que no integran IPSec, existen aplicaciones de cliente IPSec, tanto comerciales como de libre distribución. Incluso existe un cliente IPSec para Palm Pilot. Para garantizar la seguridad de esta solución y evitar intrusiones, como las que han afectado a muchas compañías de envergadura, es necesario complementar la tecnología IPSec con el uso, en los equipos remotos, de cortafuegos personales y autenticación fuerte mediante certificados digitales X.509 residentes en tarjeta inteligente. Desde el punto de vista del administrador de la red informática de la corporación, los requisitos prioritarios serán la facilidad de gestión y la necesidad de autenticar de forma fiable a cada usuario. La integración de IPSec con una infraestructura de clave pública (PKI) proporciona una respuesta adecuada a estos requisitos.

3. Por último tenemos el tema de la extranet. Esta se entiende como una red de comunicaciones que interconecta a una empresa con todos los agentes con los cuales mantiene relaciones comerciales: consumidores, proveedores y *partners*. En este escenario la interoperabilidad que ofrece el estándar IPSec es una ventaja clave frente a otras soluciones; cada empresa comprará equipos de fabricantes distintos, pero todos

ellos podrán conectarse de forma segura utilizando IPSec como lenguaje común. La tendencia actual es la aparición de extranets en las que convergen todas las empresas que participan en un mismo sector productivo. Previsiblemente, el comercio electrónico B2B²⁴ evolucionará en este sentido, para proporcionar puntos de encuentro virtuales en los que se establezcan relaciones comerciales de empresa a empresa de forma segura. Estos mercados virtuales especializados se articularán de forma natural en torno a la elaboración de un producto o la provisión de un servicio concreto: fabricación del automóvil y el tipo de industria que lleva asociada, distribución y comercialización de alimentos, sector asegurador, etc.

Para poder tener una visión mas clara de lo anterior, tenemos el caso de una empresa aseguradora en la cual se presenta la siguiente situación: Esta posee una extranet que conecta las compañías aseguradoras y los agentes de ventas, la cual debe cumplir estrictos requisitos de seguridad, que incluso están regulados por normativas legales. En este caso el utilizar IPSec aparece como la solución más apropiada, dado que es una tecnología avalada por estándares internacionales, garantiza la interoperabilidad entre los equipos de distintos fabricantes y proporciona el más alto nivel de seguridad gracias a las técnicas criptográficas más modernas.

En la figura siguiente se muestra un esquema de una *extranet*.

²⁴ negocio a negocio

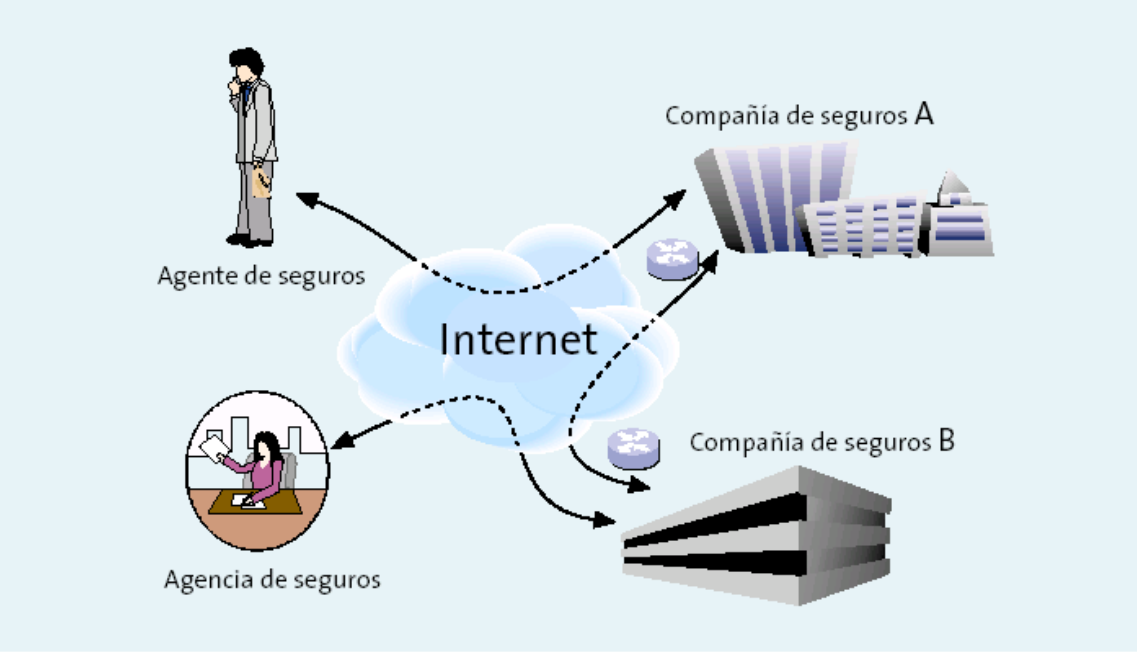


Figura 2 - 11. Extranet aplicada

En la figura anterior se puede observar como dos compañías se comunican de forma segura para intercambiar información. Al mismo tiempo los agentes de ventas y las oficinas de seguros pueden acceder a la información comercial necesaria para su negocio. Una extranet como ésta puede llevarse a cabo perfectamente usando IPSec; para ello se requiere la instalación de un gateway IPSec en cada uno de los puntos de presencia de la extranet, mientras que el equipamiento de los agentes de ventas se reduce a un PC portátil con un cliente IPSec.

Después de ver las bondades de IPSec no queda más que utilizar dichas características, es aquí donde aparece un nuevo elemento que viene a complementar lo anterior y que dice relación con un esquema que está siendo ampliamente difundido tanto a nivel internacional como nacional, principalmente por las empresas de telecomunicaciones, y que consiste en la utilización de VPN, esto debido principalmente a las facilidades que nos da en cuanto a proporcionarnos un espacio seguro al que se accede con todas las características necesarias, como lo son la autenticación, la integridad y la confidencialidad.

2.5 VPN

DEFINICIÓN DE VPN.

Una VPN ²⁵ es la forma de transportar de manera segura por Internet, principalmente datos, utilizando para ello un túnel que se ha establecido entre dos puntos que con anterioridad habían negociado un esquema de encriptación y autenticación para el transporte. Es por ello que este método permite el acceso remoto a servicios de red de forma transparente y segura con el grado de conveniencia y seguridad que los usuarios conectados elijan.

Es necesario hacer el alcance que las VPN están implementadas en firewalls, routers o equipos que brinden la capacidad de realizar encriptación y autenticación.

Con lo anterior se habilitan redes privadas distribuidas para comunicar de forma segura cada uno de los nodos de una red pública y de esa manera evitar que los datos sean interceptados. Es así que con el uso de una VPN, los usuarios remotos, que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de redes públicas.

CARACTERÍSTICAS DE UNA VPN.

a) DESCRIPCIÓN.

Una Red Privada Virtual (VPN) consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos computadores son encriptados estableciéndose una sesión punto a punto, para posteriormente ser enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN).

²⁵ Red Privada Virtual

Una Red Privada Virtual es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Así, las VPN constituyen una estupenda combinación entre la seguridad que garantizan, el bajo costo y el gran alcance, pudiendo ser asequibles desde cualquier punto de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPNs una infraestructura confiable y de bajo costo que satisface necesidades de comunicación de cualquier organización.

Las VPNs permiten:

- La administración y ampliación de la red corporativa al mejor costo.
- La facilidad y seguridad para los usuarios remotos de conectarse a la organización.

Los requisitos indispensables para esta ínter conectividad son:

- Políticas de seguridad.
- Requerimiento de aplicaciones en tiempo real.
- Compartir datos, aplicaciones y recursos.
- Servidor de acceso y autenticación.
- Aplicación de autenticación.

b) PROTOCOLOS.

Han sido implementados varios protocolos de red para el uso de las VPN. Estos protocolos intentan cerrar todos los “hoyos” de seguridad inherentes en VPN. Estos

protocolos continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro, aunque como hemos visto esto ha cambiado debido a la gran fuerza que ha impuesto IPSEC y por el apoyo del IETF en el que esta sustentado.

Estos protocolos son los siguientes: Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), Internet Protocol Security (IPsec) y SOCKS Networks Security Protocol, este último sistema proporciona otra alternativa a los protocolos de VPN. SOCKS se aloja en el nivel de sesión de OSI. Como SOCKS trabaja en un nivel OSI más alto que los protocolos anteriores, permite a los administradores limitar el tráfico VPN.

c) CLIENTES Y SERVIDORES.

Un Servidor VPN normalmente es un componente de hardware, aunque también lo puede ser de software. Puede actuar como un gateway en una red o en un único computador. Debe estar siempre conectado y esperando a que clientes VPN se conecten a él. El software para el Servidor VPN es bastante frecuente. Sistemas como Windows 2000 Server permiten alojar un Servidor VPN. El hardware de los Servidores VPN es bastante caro: el precio, a finales del año 2001, oscilaba entre los U\$1700 y los U\$3000.

Un Cliente VPN es en la mayoría de los casos un componente de software, aunque puede ser también un componente de hardware. Un cliente realiza una llamada al servidor y se conecta. Entonces el computador cliente podrá comunicarse con el Servidor VPN, ya que ellos se encuentran en la misma red virtual. El software para un cliente VPN es bastante común. Cuando se carga en el computador, este software permite crear un túnel seguro VPN a través de Internet para poder comunicarse con el Servidor VPN.

Como referencia podemos mencionar que un Router basado en Servidores VPN puede tener una velocidad de 600Kbps. Este dato es para tener una visión de qué se debe esperar en cuando a la tasa de transferencia entre los puntos que se conectan, lo que en definitiva dependerá de la infraestructura de comunicaciones con que se cuente.

2.5.1 VPN dinámicas

Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Entonces, surge la siguiente interrogante ¿Cómo establecer y mantener la confianza en un entorno que fue diseñado desde el comienzo para permitir un acceso libre a la información?, es decir, ¿Cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperabilidad y facilidad de uso?

La respuesta apropiada se encuentra en la utilización de VPNs Dinámicas. A diferencia de una VPN tradicional, una VPN Dinámica proporciona además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad, ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información.

Alguna de las características que se proporciona son las siguientes:

- Proporciona una seguridad importante para la empresa.
- Se ajusta dinámicamente al conjunto de usuarios, que puede ser muy diferente de una organización a otra.
- Permite la posibilidad de intercambio de información en diversos formatos.

El ajuste que hace para cada usuario lo consigue gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc.

Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple, pero controlado.

Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

a) Funcionamiento de las VPN Dinámicas.

Las VPNs Dinámicas constan de una plataforma de seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad.

Siguiendo los pasos ilustrados en la figura 2 – 12 que se presenta a continuación, un usuario realiza una petición de información a un servidor, por ejemplo, pulsando con su ratón en un hipervínculo. Los pasos que vienen a continuación se pueden describir a través de los siguientes puntos:

- Un usuario solicita información usando una aplicación tal como un navegador de Internet, desde un computador de escritorio: El intercambio de información comienza cuando un usuario envía información a otro usuario o solicita información al servidor. En el supuesto de que un usuario haya accedido a un hipervínculo desde dentro de algún documento Web, dicho hipervínculo será seguro y solamente podrá ser accedido por usuarios autorizados.
- La aplicación envía y asegura el mensaje: Cuando un cliente y un servidor detectan que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un protocolo de autenticación mutua. Este paso verifica la identidad de ambas partes antes de llevar a cabo cualquier acción. Una vez que se produce la autenticación se asegura el mensaje encriptándolo. Adicionalmente, se puede asociar a un certificado o firma electrónica del usuario.
- El mensaje se transmite a través de Internet: Para que la petición alcance el servidor debe dejar la LAN y viajar a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma. Durante este viaje, puede darse el caso de que atravesase uno o más firewalls antes de alcanzar su objetivo. Una vez atravesado el firewall,

la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.

- El mensaje recibido debe pasar controles de seguridad: El mensaje se transfiere al servidor. El servidor conoce la identidad del usuario cliente cuando recibe la petición.
- Durante la petición, se verifican los derechos de acceso de los usuarios: En una VPN dinámica, el sistema debe poder restringir qué usuarios pueden y no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace usando mecanismos de control, alojados en el Sistema de Control de Acceso. De este modo, incluso si un usuario presenta un certificado válido, puede ser que se le deniegue el acceso basándose en otros criterios.
- La petición de información es devuelta por Internet, previamente asegurada: El servidor de información encripta la información y opcionalmente la certifica. Las claves establecidas durante los pasos de autenticación mutua se usan para encriptar y desencriptar el mensaje. De esta forma, un usuario tiene su documento asegurado.

Para concebir de mejor manera lo anteriormente expresado, tenemos la siguiente figura:

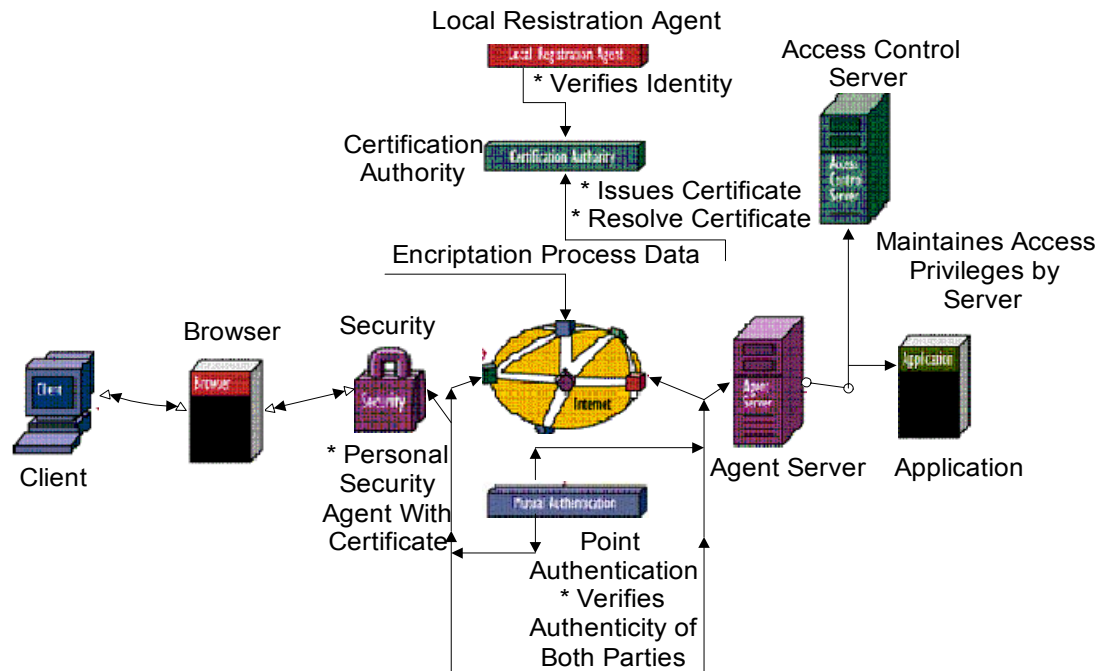


Figura 2 - 12. Ilustración de una VPN dinámica.

2.6 DISEÑO PRELIMINAR DE SALIDA

Uno de los elementos que resultan ser de mucha importancia, y que se desprende de la especificación de requerimientos, son el análisis del nivel de utilización de la solución de manera tal de poder saber en un momento determinado si es necesario realizar algún tipo de actualización o cambio en la solución.

A continuación tenemos la salida que estaría proporcionando la facilidad, para la toma de decisión con respecto a lo anteriormente expuesto.

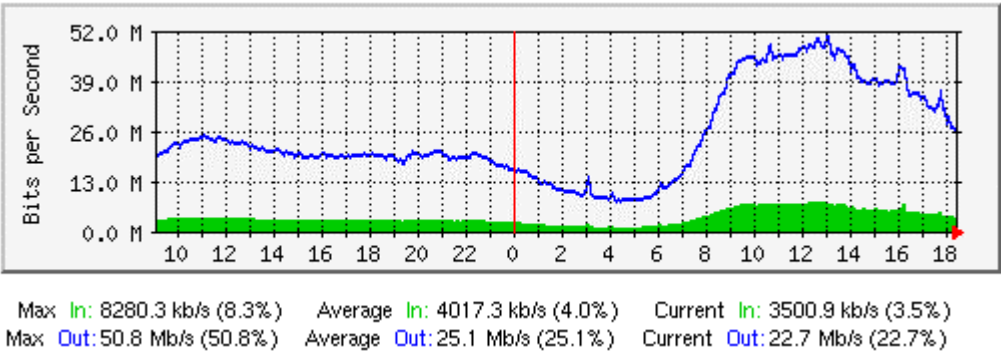


Figura 2 - 13. Estadística de tráfico.

La figura 2 – 13 muestra el tráfico de una organización, no la que ésta involucrada en este proyecto, a manera de ejemplo de la salida que se determinó en el análisis de requerimiento; sin embargo lo que puede deducirse de ésta es que existe una salida de datos, señalado como out o salida, la cual denota una gran cantidad, y por otro lado tenemos una entrada o in que muestra ser poca. Esto es acorde a lo que debiera ser el comportamiento de esta solución, ya que son los elementos externos los que descargarán en sus máquinas la información que se deje disponible. De aquí se pueden definir pautas de crecimiento de manera tal que al verse topado el out se pueda realizar una inversión para proporcionar un mayor ancho de banda, lo que involucraría una mejora en el acceso al área segura, junto con la compra de tarjetas de red para el equipo que proporciona el servicio de enlace VPN.

2.7 ESPECIFICACIONES DE HARDWARE Y SOFTWARE DE LA ALTERNATIVA SELECCIONADA

2.7.1 Especificaciones de hardware

Para satisfacer los requerimientos planteados se necesitará de:

a) Equipo que brinde servicio de VPN

Servidor de alto rendimiento con las características siguientes:

- Tarjeta Madre: Intel Server Board SBT2
- Procesadores: 2 CPU Pentium III Xeon 1.0 Ghz
- Memoria : 1 GB ampliable a 4 GB PC133 ECC Registered SDRAM
- Almacenamiento: 1 Disco Duro de 18,9 GB Maxtor Ultra Wide SCSI 10.000 rpm
- Tarjeta de video: ATI Range II 4MB integrados en la tarjeta madre
- Disquetera de 3½"
- CDROM 52x LG
- Tarjetas de red: 1 3Com 10/100 y otra que se encuentra integrada en la tarjeta madre (tarjeta de red Intel 10/100)
- Monitor de 14" Viewsonic
- Teclado (PS2)
- Mouse (Ratón) (PS2)
- Gabinete Intel SC5000 con fuentes redundantes.
- Mouse (Ratón) (PS2)
- Gabinete.

b) Unidades de respaldo de energía

Una unidad APC Smart-UPS 1000 VA.

2.7.2 Especificaciones de software

a) Sistema operativo

El sistema operativo seleccionado para todos los equipos activos es Red Hat Linux Versión 7.3, utilizando la versión de kernel 2.4.18 o superior, esto porque presentan mayor robustez en lo que se refiere a instalación de software VPN. Algunas de las razones por las cuales se optó por el sistema operativo Linux y no otro son:

- Precio. Es gratis si se descarga de la red y en caso de comprarse con caja esta no supera los \$45.000 y puede instalarse en todos los equipos que uno desee.
- Estabilidad, presenta una autonomía mucho mayor que otros sistemas operativos.
- Seguridad, existen un sinnúmero de software que facilita este tipo de funciones y el cual en constante actualización.
- Compatibilidad, permite integrarse a cualquier ambiente distinto a UNIX, pudiendo ser este MAC, Windows, Novell u otro.
- Velocidad, al tener un control más profundo del código del corazón del sistema operativo, se puede sacar un mejor provecho del hardware.
- Posee el apoyo de miles de programadores a nivel mundial.
- El paquete incluye el código fuente, lo que permite modificarlo de acuerdo a las necesidades del usuario o la aplicación.
- Puede manejar múltiples procesadores.
- La corporación DATA Internacional predice que el crecimiento de este programa será del orden de un 25 por ciento anual en el nuevo milenio.

b) Software funcional:

- VPNd
- FreeSWAN
- PoPToP
- MRTG

El software anteriormente mencionado, participa en forma independiente uno del otro, es así que si deseamos tener un tipo específico de VPN, sólo uno de ellos estará entregando su servicio, quedando el resto en espera a ser activado cuando sea necesario, esto debido a que cada uno de ellos cumple con una función distinta por el hecho de brindar un servicio diferente a los otros. Es por ello que tenemos

1. VPNd, es un servicio que permite conectar dos redes entregando acceso a la red privada que pudiera poseer alguna de ellas o ambas, mediante el uso de claves simétricas, con lo cual estaría inserta en una solución de VPN no dinámica, que utiliza el estándar IPsec. En este caso todas las transferencias de datos se realizan encriptadas utilizando el algoritmo de encriptación Blowfish, el cual se puede usar libremente.
2. FreeSWAN, en este otro caso el servicio es provisto por medio del estándar IPsec, corresponde a una solución basada en una VPN dinámica, ésta entrega seguridad a nivel de capa IP utilizando además extensiones del kernel e IKE, el cual interactúa con otras implementaciones, como por ejemplo la que posee OPENBSD. Esta implementación posee la cualidad de poder utilizar los certificados X509v3 para la autenticación de los puntos que se comunicarán.
3. PoPToP, es un servicio basado en un ambiente VPN PPTP, soporta en su estado actual las versiones de Windows 95/98/NT/2000 en cuanto a clientes, al igual que clientes Linux PPTP.

Todas las aplicaciones de servicios mencionadas anteriormente proveen de distintas facilidades que permiten realizar una comunicación segura, con lo anterior se asegura una mayor versatilidad ante los requerimientos actuales o bien futuros que pudiese aparecer. Hay que hacer notar que estos paquetes de software son hoy día los de uso más común, sin embargo día a día están apareciendo nuevos desarrollos que pudieran superar a estos, lo cual conllevaría a una evaluación, y en la eventualidad que éstos fuesen mejores realizar un cambio que en ningún caso debiera afectar a los clientes que ya están haciendo uso del software de la solución actual.

En el caso del software MRTG entrega la herramienta de análisis de nivel de tráfico para el proceso de estadísticas mencionado en la especificación de requerimientos.

2.7.3 Especificaciones de comunicaciones

La red con que cuenta la organización se encuentra en una fase de cambio, ésta se encuentra inmersa en un proceso de renovación, lo que conlleva a vislumbrar que los cambios que se vayan a realizar, irán en directa relación con un mejoramiento de las comunicaciones de la cual gozan ciertas áreas hoy día y que se verá extendida en el corto plazo al resto de la organización, al haber una red que soporte un nivel de tráfico mayor, que se pueda aplicar un sistema de filtrado y en el cual se pueda garantizar QoS²⁶. Las comunicaciones se verán mejoradas en cuanto a su tiempo acceso a aquellos servicios que se encuentran hoy día definidos para ciertos usuarios, ya sea internos, pero en su mayoría externos a la institución.

²⁶ Quality of Service (Calidad de Servicio)

CAPÍTULO 3: DISEÑO E IMPLEMENTACIÓN

3.1 DISEÑO

De acuerdo con la especificación que se realizó en al capítulo anterior, se establece el siguiente esquema de interconexión.

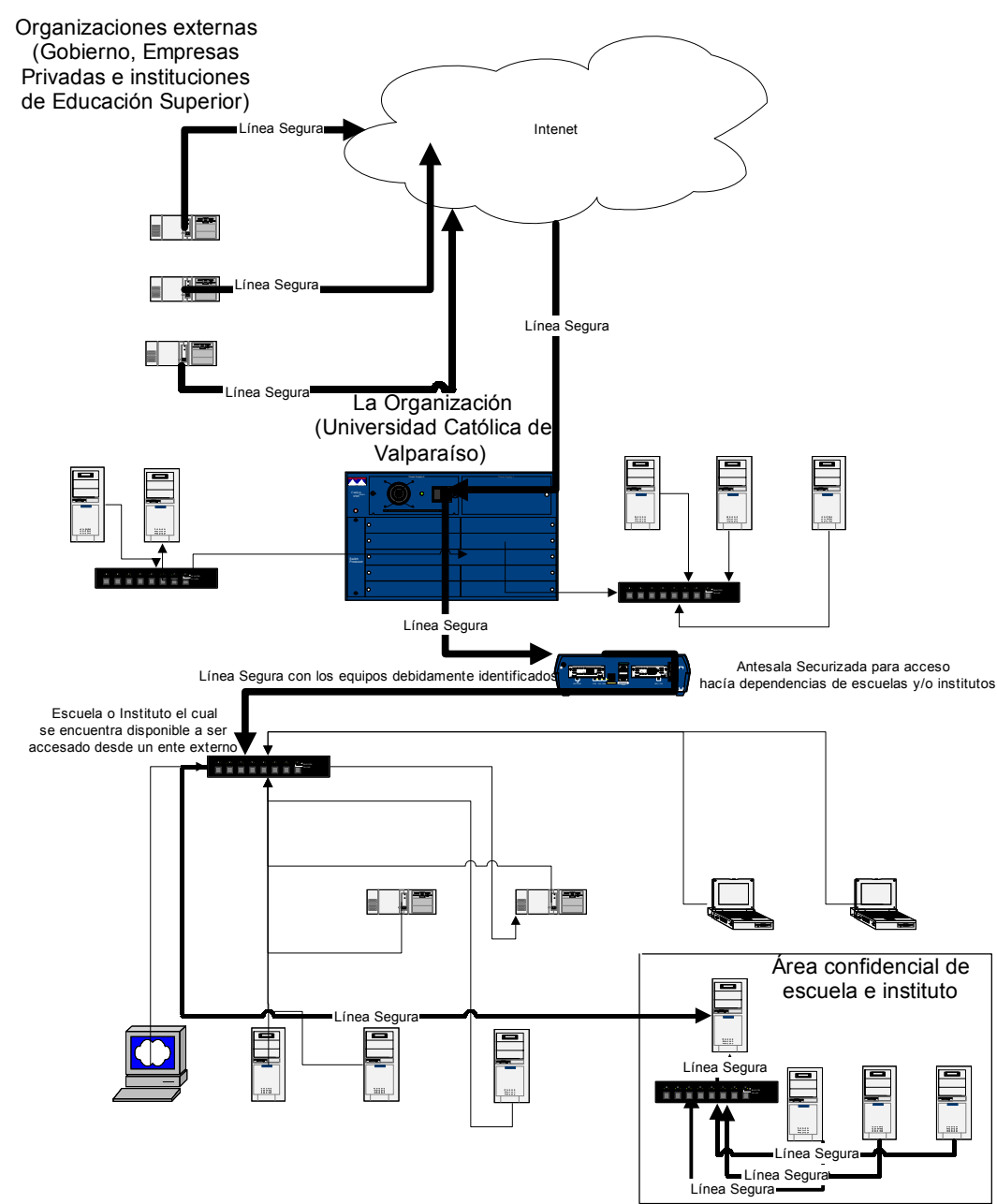


Figura 3 - 1. Esquema de interconexión de acceso seguro basado en solución propuesta.

De acuerdo con la figura 3 – 1 podemos establecer la existencia de un área confidencial, la cual consta de dos sub-áreas, en la primera de ellas se encuentra el equipamiento especificado de acuerdo con el hardware y software que fue presentado anteriormente y el cual cumple las funciones de un servidor de enlace VPN. Para referencia podemos decir que el equipo en sí es aquel que cuenta con el sistema operativo Linux y el software que permite brindar el servicio VPN; lo anterior involucra que por medio de él se podrá tener acceso a los equipos que residen en la segunda sub-área y que corresponden al equipamiento a proteger de la escuela o instituto, éste se visualiza en la figura 3 – 1 como aquel que se encuentra conectado al equipo activo de comunicaciones en el área confidencial. En base a lo antes expuesto se presenta el siguiente modelo:

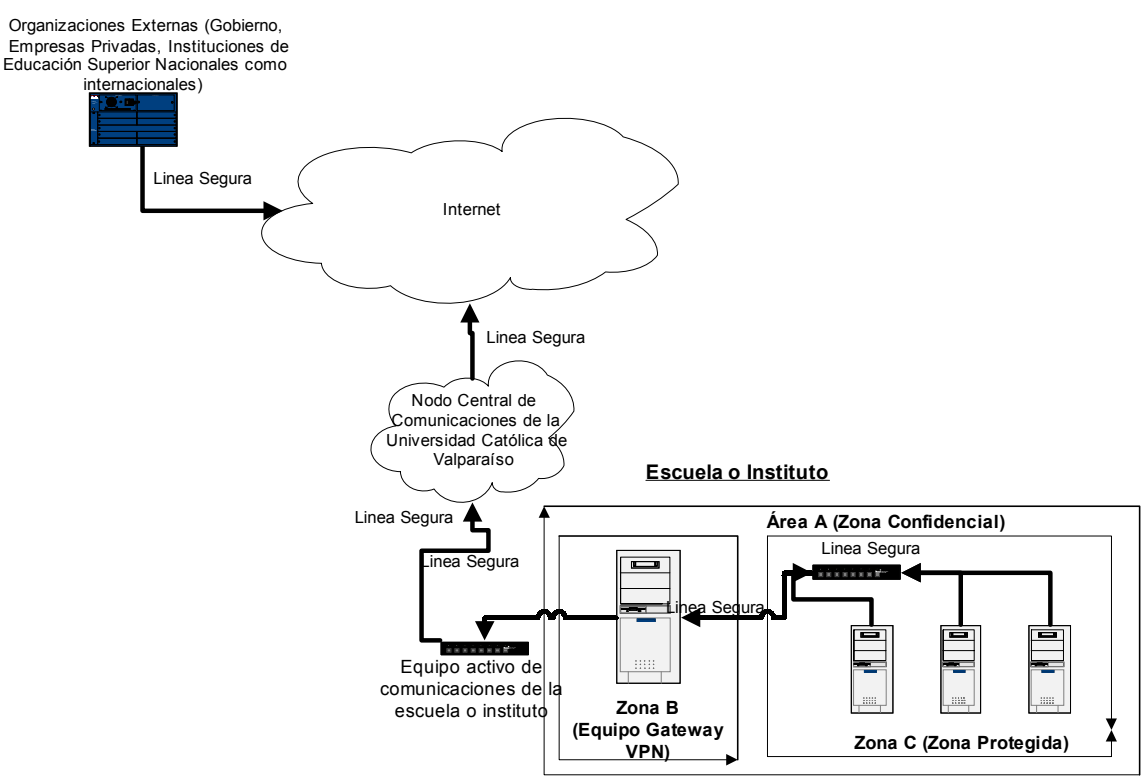


Figura 3 - 2. Esquema de la zona confidencial de una escuela o instituto.

A partir del esquema de la zona confidencial se constituyen los elementos a considerar para el diseño de la solución. Es aquí donde reside el equipamiento que cumple con la función de servir de puerta de entrada, desde la denominada zona B hacia la zona C, la cuál corresponde al área protegida, por lo tanto este equipamiento tendrá instalado el sistema operativo Linux, en su distribución Redhat 7.3 y deberá estar actualizado su kernel²⁷ a la versión más reciente; deberá poseer dos tarjetas de red, una para interconectarse con el equipo de comunicaciones que permite acceder al nodo central de comunicación de la organización, y éste a su vez a Internet. La segunda tarjeta permitirá establecer el vínculo con la zona confidencial, logrando con esto la interconexión de las áreas segura e insegura.

Una vez que la plataforma está instalada, se procede a emplazar el software que brindará el servicio de VPN, para ello se deberá contar con los programas ya como “paquete”²⁸ de instalación, la cual lleva por nombre “rpm”, o bien teniendo el código fuente de los mismos, el cual se deberá compilar e instalar de acuerdo con las instrucciones.

Con respecto al cliente VPN, tenemos una serie de ellos que son gratuitos y otros por los que se debe pagar; sin embargo para efectos del diseño de la solución se establece que la gran mayoría utiliza Windows como plataforma de escritorio, ya que hasta nuestros días es el sistema operativo de facto, y TCP/IP como protocolo de comunicaciones de acceso a Internet. Hay que tener en cuenta que Windows desde su versión 95 en adelante ya dispone de la facilidad de crear una comunicación segura por medio de una aplicación que viene preinstalada. En la eventualidad que no se contara con la plataforma antes señalada puede utilizarse alguno de los siguiente programas: cliente Cisco VPN (para plataforma Linux, Windows, Macintosh o Solaris), que es pagado, o bien el cliente PGP VPN (para plataforma Windows y Macintosh) que es gratis bajo ciertas condiciones. Además de los antes señalados existen una serie de

²⁷ Corazón o parte fundamental del sistema operativo.

²⁸ Formato que presentan los software a ser instalados en la distribución RedHat

aplicaciones cliente en Internet, las cuales pueden descargarse gratuitamente en algunos casos y ser utilizadas para establecer el vínculo con el servidor de enlace VPN.

Por lo tanto un cliente VPN mediante IPsec conforma una conexión con el servidor de enlace VPN, ya sea usando claves simétricas o bien certificados digitales (X509v3), pudiendo hacer uso de uno de ellos a la vez, con lo cual se ve satisfecha la necesidad que pudiera existir entre el emisor y el receptor de realizar una comunicación segura haciendo uso de alguna de esas metodologías.

La siguiente figura hace presente la forma en que interactuarán el cliente VPN y el servidor de enlace VPN.

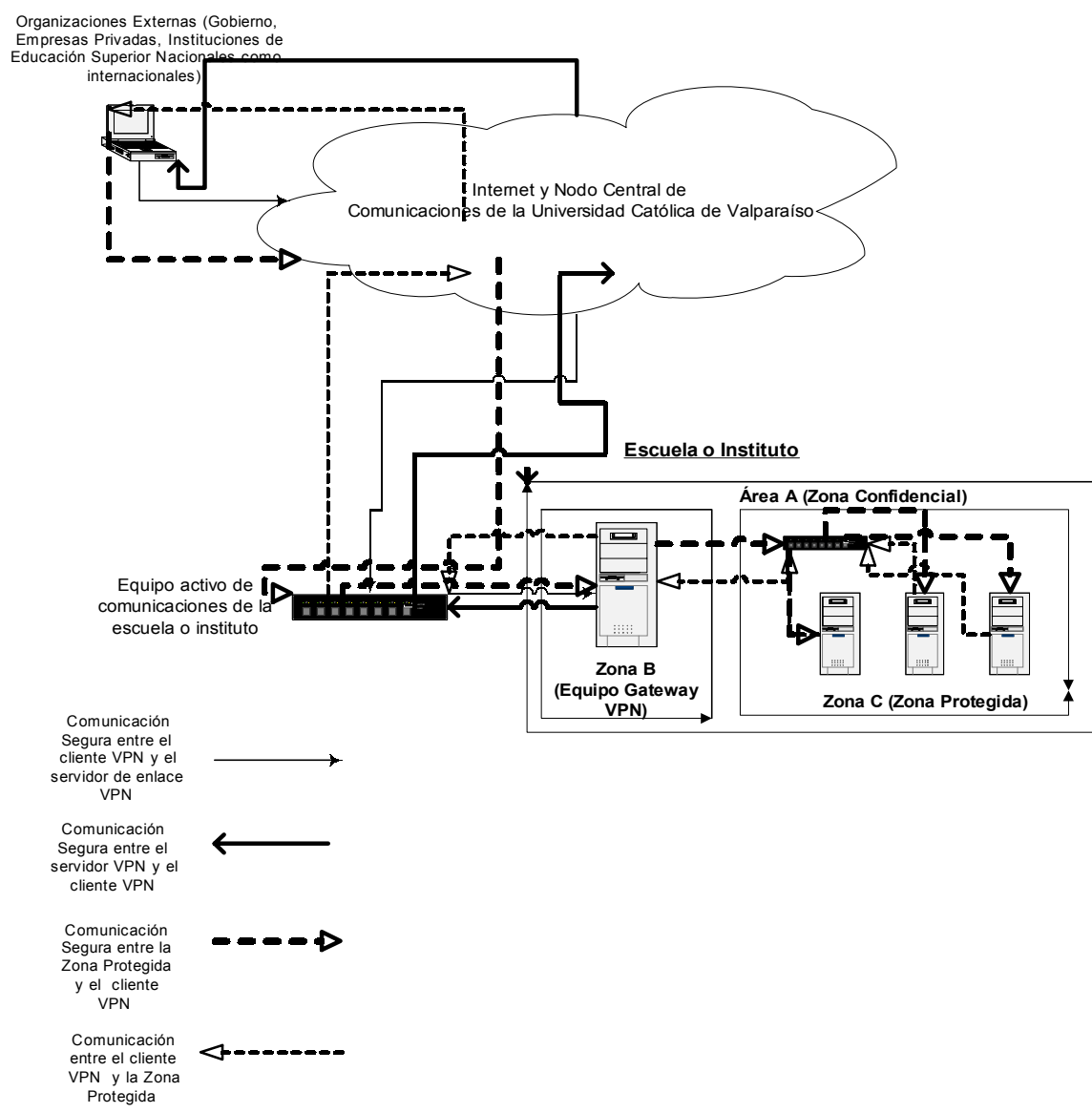


Figura 3 - 3 Comunicación entre el cliente VPN y el servidor de enlace VPN.

A partir del proceso mostrado en la figura anterior establecemos que el cliente, el cual se encuentra fuera de los dominios de la organización, poseerá un software cliente VPN mediante el cual establecerá una comunicación con el servidor de enlace VPN, éste lo autenticará y si es válido permitirá que se comunique con los equipos que se encuentran en el área protegida, produciéndose el intercambio de información entre ellos, todo esto en forma segura.

3.2 **IMPLEMENTACIÓN**

Para la realización de la implementación se debe tener en cuenta los procesos que deben llevarse a cabo para realizar esta tarea, es así como se distinguen los siguientes acontecimientos:

- Recepción del equipo que entregará el servicio de puerta de enlace VPN junto con la unidad de respaldo de energía (UPS) correspondiente.
- Instalación física del equipamiento en el lugar definido en común acuerdo con la escuela o instituto.
- Instalación de la plataforma en la que estará soportado el servicio de VPN.
- Instalación de los servicios necesarios para brindar la comunicación segura (VPN).
- Por último se configurará el o los clientes que se conectarán al área protegida.
Para aquellos usuarios que se encuentren geográficamente imposibilitados de poder realizarles éste trabajo, se les entregará un manual de procedimiento para el caso.

Para tener una visión más acabada de lo anteriormente expuesto se presenta el siguiente diagrama de flujo de procesos.



Figura 3 - 4. Diagrama de flujo de procesos.

Una vez definidos los procesos necesarios para la implementación y teniendo en cuenta la elección del equipamiento, que fue establecido en el capítulo anterior y que corresponde a la denominada puerta de enlace VPN, se instalará la plataforma sobre la que sustentará el servicio de comunicación segura. Para ello se escogió la distribución de Linux Redhat, en su versión 7.3, aunque podría ser alguna que apareciera posteriormente, previa evaluación; ésta deberá contar con un nivel o versión de kernel igual o superior 2.4.18-10, debido a que ésta es la última con que se cuenta; sin embargo

la aparición de nuevas versiones es muy dinámica, por lo que puede variar en el corto plazo, es por ello que se deberá chequear que no exista alguna más nueva al momento de realizarse el proceso de implementación. Si ello ocurriera se deberá actualizar en la medida que los servicios de VPN lo ameriten, lo cual pasa por una evaluación de la misma. Esta involucra establecer el nivel de actualización del sistema instalado, tanto a nivel de kernel, como de aquellos “paquetes” que tengan directa relación con el servicio, esto se logra mediante la utilización de sitios como rpmfind.net, el cual en base a las actualizaciones que se deseen realizar muestra las dependencias existentes con el resto del sistema.

Para realizar la instalación de la plataforma, Linux, se deben realizar los siguientes pasos:

- Contar con los cdrom de instalación de la distribución.
- Realizar la instalación propiamente tal, utilizando el perfil del servidor.
- Configurar los servicios anexos a los de VPN que se pudieran requerir, como lo pueden ser el servicio Web u otro.

Para mayores detalles de este procedimiento refiérase al anexo 1.

Una vez que la plataforma se encuentra instalada, se procede a incorporar los servicios de VPN, los cuales se obtienen mediante la incorporación de los siguientes software: Vpnd, FreeSwan y PoPTop, en los tres casos la instalación de ellos se puede realizar por medio de archivos rpm, los cuales se instalan mediante la utilización de una herramienta que lleva por nombre “rpm” o bien obteniendo los archivos fuente, los cuales vienen comprimidos y se obtienen de los sitios²⁹ de quienes los han desarrollado, para posteriormente compilar dichas aplicaciones, y proceder a instalar de acuerdo al procedimiento entregado por quienes los crearon. Hay que hacer notar que en el caso del servicio FreeSwan se debe tener cuidado con la versión en “rpm” de él, debido a que

²⁹ <http://freshmeat.net>, <http://sourceforge.net> o <http://rpmfind.net>

ésta debe coincidir con la versión de kernel de la distribución que se instaló. Para una visión mas acabada del procedimiento refiérase al anexo 2.

Una vez que el servidor de enlace se encuentra listo para establecer conexiones seguras, se procede a realizar la instalación y/o ejecución de la aplicación cliente VPN, que se realiza desde el lugar desde el cual se desea conectar. Con esto se da término al proceso de implementación, para mas detalles de cómo debe realizarse la instalación y/o configuración del cliente refiérase al anexo 3.

Para realizar toda esta labor es necesario contar con personal del área técnica, específicamente un ingeniero con bastante experiencia en el área de seguridad y redes, el cual llevará a cabo el proceso de implementación y posterior mantención. Además se debe considerar contar con un espacio físico adecuado para la instalación del equipamiento, debidamente acondicionado tanto en lo que se refiere a la climatización como a su alimentación eléctrica.

CAPÍTULO 4: EVALUACIÓN ECONÓMICA Y EXPERIENCIA

4.1 FLUJOS RELEVANTES DEL PROYECTO

4.1.1 Conceptos premilitares:

Enfoque para evaluación: El proyecto se contempla que sea realizado en un periodo de 3 años, para los efectos del proyecto se considera un dólar americano a \$730 pesos chilenos y una Unidad de Fomento de \$16.616. Además se establece que se denotara como Pre-Proyecto al tiempo que se invirtió en la concepción de este estudio el cual se conceptualizará en horas entregadas para éste fin. Además se considera una tasa de descuento del 12% en base a una formula que posee la institución para el análisis financiero de los proyectos que involucren TI.

4.1.2 Inversión inicial

La inversión inicial consta de 3 elementos, los cuales son: los activos fijos del proyecto, gastos de puesta en marcha, el capital de trabajo y el pre-proyecto. A continuación se identificará, cuantificará y valorizará cada uno de ellos. La depreciación de los activos fijos es de 6 años, pero se aplicará una depreciación acelerada debido al plazo del proyecto.

a) Identificación.

Activo fijo.

- Equipamiento Computacional. Esto involucra el equipo para brindar el acceso seguro.
- Unidad de respaldo de energía (UPS).

Gastos de puesta en marcha.

- Horas Hombre (HH) para la implementación de la solución por parte de un ingeniero en sistemas

- Puesta en marcha, ésta corresponde a las pruebas de conectividad entre el servidor de enlace VPN y los clientes.

Capital de Trabajo

- Se considera un monto de U\$534, el cual constituye el costo operativo de un mes y que el equivalente al valor de un mes de ahorro.

Pre-Proyecto.

- Horas Hombre (HH) involucradas en el desarrollo de ésta solución.

b) Cuantificación

Tabla 4 – 1. Cuantificación de la inversión inicial.

Ítem	Cantidad
Equipamiento Computacional	1 Servidor de alto rendimiento (servidor de enlace VPN)
Componente Hardware	1 UPS (Unidad de respaldo de Energía)
Equipamiento Computacional	Sistema Operativo Linux Redhat 7.3
Componente Software	Software Servicio VPN
Puesta en Marcha	1 Ingeniero en Sistemas (por 20 Horas)
Implementación	1 Ingeniero en Sistemas (por 12 Horas)
Pre-Proyecto	1 Ingeniero en Sistemas (por 208 Horas)

c) Valorización.

Tabla 4 – 2. Valorización de la inversión inicial.

Ítem	Cantidad	Valor total en dólares
Equipamiento Computacional	1 Servidor de alto rendimiento (servidor de enlace VPN)	U\$1644
Componente Hardware	1 UPS (Unidad de respaldo de Energía)	U\$420
Equipamiento Computacional	Sistema Operativo Linux Redhat 7.3	U\$0
Componente Software	Software Servicio VPN	U\$0
Puesta en Marcha	1 Ingeniero en Sistemas (por 20 Horas)	(20*822)/176 U\$94
Implementación	1 Ingeniero en Sistemas (por 12 Horas)	(12*822)/176 U\$56
Pre-Proyecto	1 Ingeniero en Sistemas (por 208 Horas)	(208*822)/176 U\$972
Total		U\$3186

4.1.3 Ingresos

A partir del hecho que hoy día no existe posibilidad de realizar ahorros por parte del Departamento de Informática, es que se solicita que las escuelas e institutos aporten con aquellos recursos que aparecen a partir de la disminución de sus costos por las mejoras provenientes del proyecto que se está realizando, pasando a ser así parte del

presupuesto de dicha entidad, con lo cual se establece que serán ingresos que se percibirán para el proyecto. A partir de todo lo anterior podemos establecer lo siguiente:

a) Identificación.

- Cobro por mejora en el tráfico de información de manera rápida y segura
- Excedentes provenientes del ahorro en que se incurre al evitar los siguientes gastos:
 - Insumos (cdrom y cintas)
 - Horas Hombre (HH) de un docente para realizar los respaldos en los medios antes señalados.
 - Envío de medios magnéticos a nivel nacional (cdrom y cintas).
 - Envío de medios magnéticos a nivel internacional (cdrom y cintas).
 - Llamadas internacionales

b) Cuantificación.

Tabla 4 – 3. Cuantificación de los ingresos.

Ítem	Cantidad
Mejora del servicio de tráfico	2.5 UF mensuales
Insumos	
CDROM	8 unidades mensuales.
Cintas	8 unidades mensuales.
Horas Hombre docente	8 Horas mensuales
Envío nacional de medios magnéticos (cdrom y cintas)	4 envíos mensuales
Envío internacional de medios magnéticos (cdrom y cintas)	4 envíos mensuales.
Llamadas internacionales	45 minutos mensuales

c) Valorización.

Tabla 4 – 4. Valorización de los ingresos.

Ítem	Cantidad	Valor Total
Mejora el servicio de tráfico	2,5 UF	$(22,76 \times 2,5) \times 12$ U\$683
Insumos		
CDROM	8 unidades mensuales.	$(8 \times 0.42) \times 12$ U\$41
Cintas	8 unidades mensuales.	$(8 \times 50) \times 12$ U\$4800
Horas Hombre docente	8 Horas mensuales	$((8 \times 1233) / 176) \times 12$ U\$672
Envío nacional de medios magnéticos (cdrom y cintas)	4 envíos mensuales	$((200 \text{ gr.} \times 23) / 1000) \times 4 \times 12$ U\$221
Envío internacional de medios magnéticos (cdrom y cintas)	4 envíos mensuales.	$((200 \text{ gr} \times 54) / 1000) \times 4 \times 12$ U\$519
Llamadas internacionales	45 minutos mensuales	$(45 \times 0.28) \times 12$ U\$152
Total		U\$7088

4.1.4 Costos

En este proyecto sólo se tienen costos fijos.

- a) Identificación
 - Horas Hombre (HH) de un ingeniero en sistemas para la mantención.
- b) Cuantificación

Tabla 4 – 5. Cuantificación de los costos.

Ítem	Cantidad
Horas Hombre ingeniero en sistemas	9 horas mensuales

- c) Valorización.

Tabla 4 – 6. Valorización de los costos.

Ítem	Cantidad	Valor Total en dólares
Horas Hombre ingeniero en sistemas	9 horas mensuales	$((9 * 822) / 176) * 12$ U\$504

4.1.5 Valor Residual

El Valor residual de los activos que se adquirieron será de un 10% de su valor original, por lo tanto éste asciende a U\$207.

4.1.6 Flujos de caja

A partir del establecimiento de la inversión inicial, ingresos y egresos, se establece por medio de las siguientes planillas tres distintas situaciones. La primera corresponde a la de un proyecto puro donde el inversionista, en este caso la organización, facilita todo el presupuesto necesario para el desarrollo del proyecto; una segunda posibilidad es que sea financiado en un 50 % y, por último, que el financiamiento se eleve a un 75 %.

Para la situación con proyecto puro tenemos que en la figura que precede se establece el flujo de caja que se obtiene a partir de la información definida en el punto 4-1.

Tabla 4 - 7. Flujo de caja para proyecto puro

Periodos	0	1	2	3
(+) Ingresos		7088,00	7088,00	7088,00
(-) Egresos		-504,00	-504,00	-504,00
(=) Margen		6584,00	6584,00	6584,00
(-) Depreciación				
(-) Valor Libro				
(+) Valor Residual				207
(-) Interés Crédito				
(=) Utilidad antes Imp		5552,00	5552,00	6791,00
(-) Impuesto				
(=) Utilidad desp Imp		5552,00	5552,00	6791,00
(+) Depreciación				
(+) Valor Libro				
(+) Crédito				
(-) Amortiza Crédito				
(-) Inversión Inicial	-3186			
(-)				
/+) Capital de Trabajo	-534			534,00
(=) Flujo de Caja	-3720	6584,00	6584,00	7325,00

Los valores de los elementos a considerar para determinar su viabilidad económica para este proyecto, son el VAN³⁰ el cual presenta un valor de US\$11268,83 dólares americanos, su TIR³¹ el cual asciende a 170% y el período de recuperación de la inversión es en el primer año, con lo cual se confirma su viabilidad económica.

Para la sensibilización del proyecto se consideran las variables ingreso, apreciando el efecto de su disminución, y el egreso, visualizando su comportamiento al ir en aumento.

³⁰ VAN : Valor Actual Neto

³¹ TIR : Tasa de Recuperación de la Inversión

Tabla 4 - 8. Sensibilización de Ingresos para proyecto puro.

Disminución de Ingresos en %	VAN
0	\$11.268,83
-10%	\$9.617,26
-20%	\$8.097,24
-30%	\$6.577,23
-40%	\$5.057,21
-50%	\$3.537,19
-60%	\$2.017,18
-70%	\$497,16
-80%	-\$1.022,85

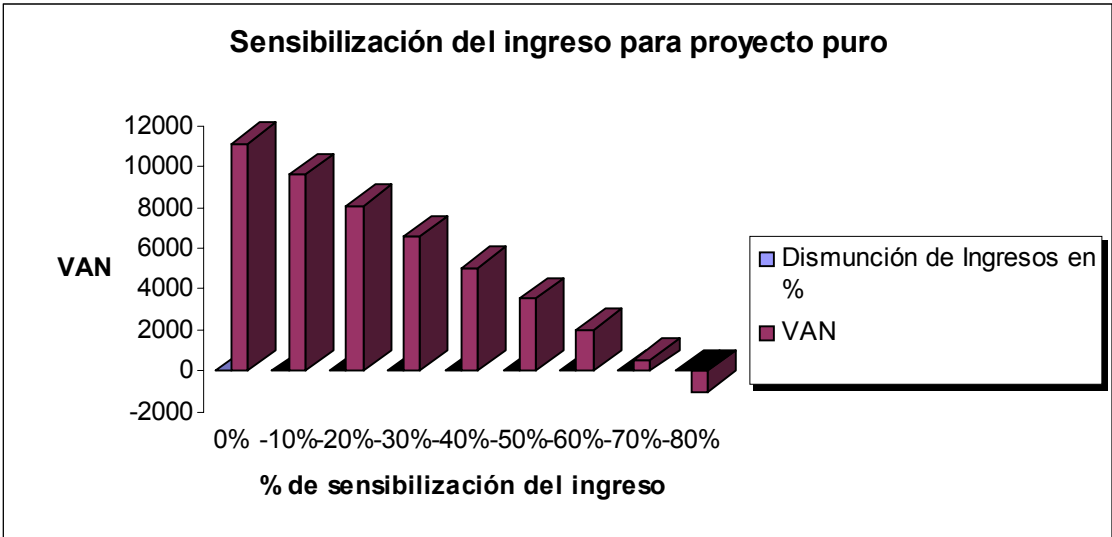


Gráfico 4 – 1. Tendencia de la sensibilización de ingresos para proyecto puro.

En este caso podemos apreciar que al disminuir el ingreso entre un 70% y 80 %, específicamente un 73,2703% el VAN se hace cero con lo cual el proyecto puede como no puede realizarse debido a que no hay margen de utilidad de éste.

Tabla 4 - 9. Sensibilización de los Egresos para proyecto puro.

Aumento de los Egresos	VAN
0	\$ 11.268,83
100%	\$ 10.056,45
200%	\$ 8.975,63
300%	\$ 7.894,80
400%	\$ 6.813,98
500%	\$ 5.733,15
600%	\$ 4.652,33
700%	\$ 3.571,51
800%	\$ 2.490,68
900%	\$ 1.409,86
1000%	\$ 329,03
1100%	-\$ 751,79

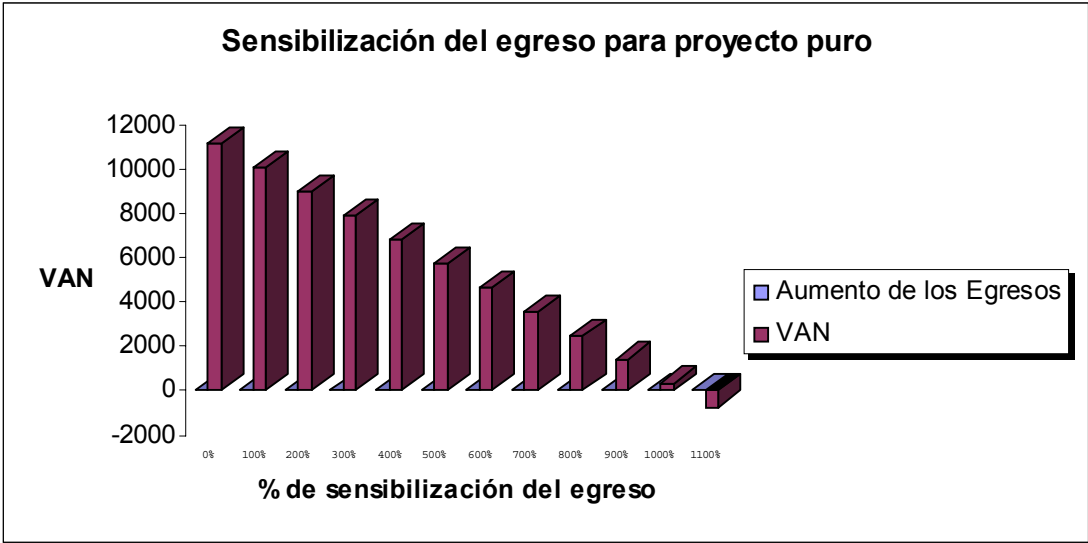


Gráfico 4 – 2. Tendencia de la sensibilización de los egresos para proyecto puro.

En el caso del aumento del egreso este debiera llegar al 1100,30% para que el proyecto fuera poco atractivo de realizar ya que su VAN se hace cero.

Una vez definido el comportamiento frente a una situación de proyecto puro, se analiza el comportamiento de éste en un ambiente donde es financiado en un 50%, para ello se solicita un crédito que asciende a U\$1593 dólares americanos los cuales se pagan

en 3 cuotas anuales vencidas por lo que se tiene el siguiente desglose de pago de interés, junto con los demás ítems a considerar en un crédito.

Fórmula para el cálculo de la Cuota:

$$R = C / [1 - (1 - \text{interés})^{-n} / \text{interés}]$$

Donde: “C “es el capital inicial, interés corresponde al interés que se le aplica el crédito y “n” al número de períodos en los cuales se esta solicitando el crédito.

Tabla 4 - 10. Tabla de amortización de crédito para proyecto financiado al 50 %.

Número de Cuota	Capital Original	Interés	Valor Cuota	Amortización de Capital	Capital Final
1	1593	127,4	618,13666	490,69666	1102,30334
2	1102,30334	88,18	618,13666	529,9523928	572,350947
3	572,350947	45,79	618,13666	572,350947	0

Establecido los intereses, la cuota y la amortización de capital para cada período se tiene el siguiente flujo de caja.

Tabla 4 - 11. Flujo de caja de proyecto financiado al 50 %.

Periodos	0	1	2	3
(+) Ingresos		7088	7088	7088
(-) Egresos		-504	-504	-504
(=) Margen		6584	6584	6584
(-) Depreciación				
(-) Valor Libro				
(+) Valor Residual				207
(-) Interés Crédito		-127,44	-88,1842672	45,7880758
(=) Utilidad antes Imp		5424,56	5463,81573	6836,78808
(-) Impuesto				
(=) Utilidad desp Imp		5424,56	5463,81573	6836,78808
(+) Depreciación				
(+) Valor Libro				
(+) Crédito	1593			
(-) Amortiza Crédito		490,69666	529,952393	572,348584
(-) Inversión Inicial	-3186			
(-)				
/+) Capital de Trabajo	-534			534
(=) Flujo de Caja	-2127	6947,25666	7025,76813	7943,13666

A partir del flujo de caja anterior, se concluye que el VAN obtenido es de U\$13688,01 dólares americanos, un TIR de 325% y un período de recuperación de la inversión en el primer año. Luego de gestar lo anterior, aparece la etapa de sensibilización del proyecto, para lo cual se consideraron las variables ingreso y egreso; a partir de esto se obtuvo la siguiente tabla asociadas a sus respectivos gráficos.

Tabla 4 - 12. Tabla de sensibilización del ingreso para proyecto financiado al 50 %

Disminución de Ingresos en %	VAN
0	\$13.688,01
-10%	\$12.036,44
-20%	\$10.516,43
-30%	\$8.996,41
-40%	\$7.476,40
-50%	\$5.956,38
-60%	\$4.436,36
-70%	\$2.916,35
-80%	\$1.396,33
-90%	-\$123,68

A partir de la información anterior se desprende el gráfico que viene a continuación.

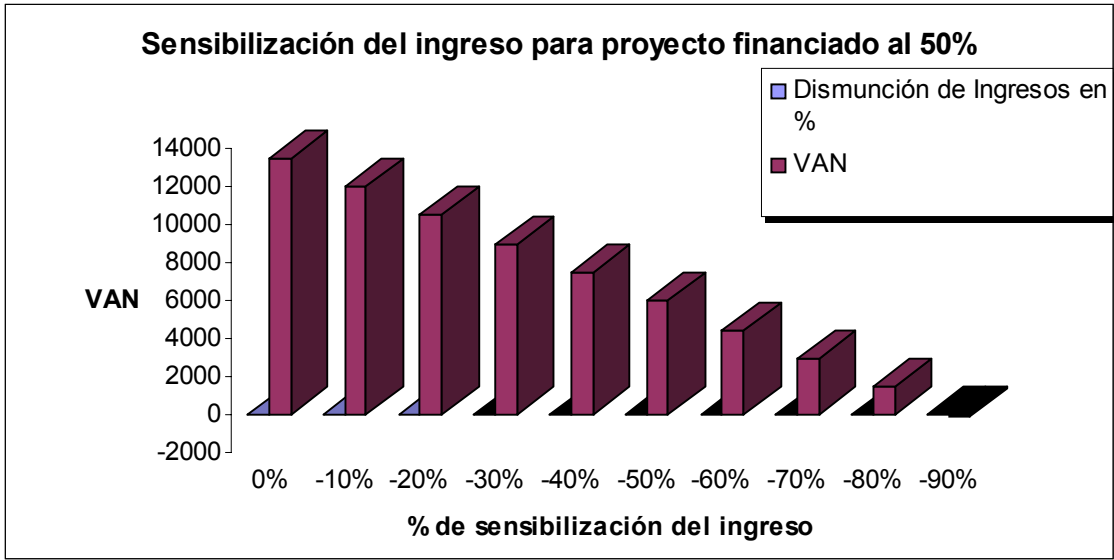


Grafico 4 - 3. Tendencia de la disminución de ingresos para proyecto financiado al 50%.

Los ingresos al ser financiado el proyecto en un 50% se diferencia del proyecto puro en cuanto a que este presenta un valor del VAN cero al disminuir en un 89,18%.

Tabla 4 - 13. Tabla de sensibilización del egreso para proyecto financiado al 50 %

Aumento de los Egresos	VAN
0	\$ 13.688,01
100%	\$ 12.475,64
200%	\$ 11.394,81
300%	\$ 10.313,99
400%	\$ 9.233,16
500%	\$ 8.152,34
600%	\$ 7.071,52
700%	\$ 5.990,69
800%	\$ 4.909,87
900%	\$ 3.829,04
1000%	\$ 2.748,22
1100%	\$ 1.667,40
1200%	\$ 586,57
1300%	-\$ 494,25

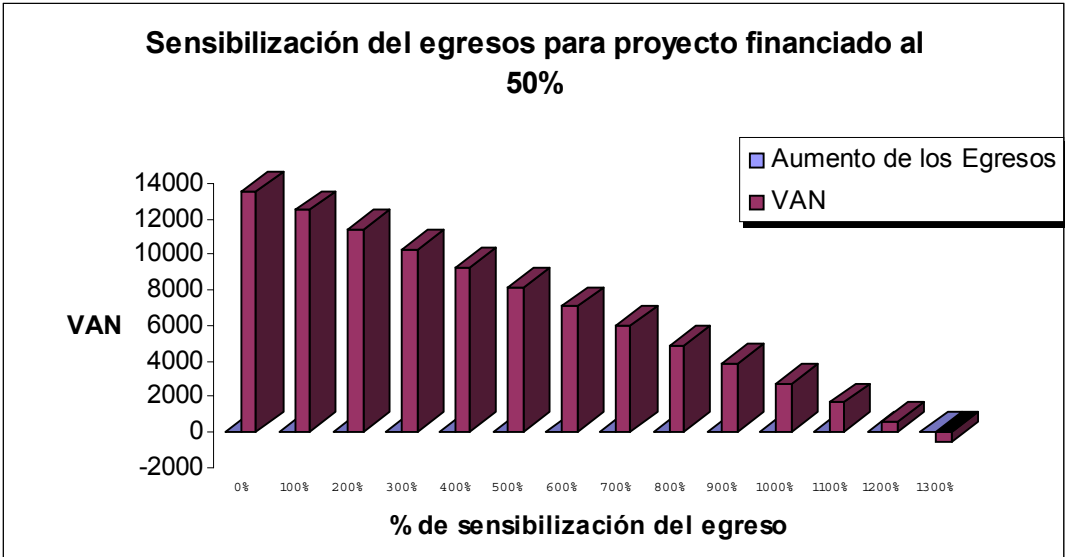


Grafico 4 - 4. Tendencia de la sensibilización del egreso para proyecto financiado al 50%.

En cuanto a los egresos, éstos tienen que aumentar en un 1200,54% para que el proyecto sea poco atractivo, debido a que su VAN se hace cero.

Por último se considero un escenario para la eventualidad que el proyecto se financiase en un 75 %, con lo cual se estableció la cuota en base a la fórmula entregada

anteriormente y de la cual se obtuvo un valor cuota de U\$927,39901 dólares americanos los cuales se pagan en 3 cuotas anuales vencidas por lo que se tiene el siguiente desglose de pago de interés, junto con los demás ítemes a considerar en un crédito.

Tabla 4 - 14. Tabla de amortización de crédito para proyecto financiado al 75 %.

Número de Cuota	Capital Original	Interés	Valor Cuota	Amortización de Capital	Capital Final
1	2390	191,2	927,39901	736,19901	1653,80099
2	1653,80099	132,304079	927,39901	795,094931	858,706059
3	858,706059	68,6964847	927,39901	858,706059	0

Establecido los intereses, la cuota y la amortización de capital para cada período, se tiene el siguiente flujo de caja.

Tabla 4 - 15. Flujo de caja de proyecto financiado al 75 %.

Periodos	0	1	2	3
(+) Ingresos		7088	7088	7088
(-) Egresos		-504	-504	-504
(=) Margen		6584	6584	6584
(-) Depreciación				
(-) Valor Libro				
(+) Valor Residual				207
(-) Interés Crédito		-191,2	-132,304079	-68,6964847
(=) Utilidad antes Imp		5360,8	5419,69592	6722,30352
(-) Impuesto				
(=) Utilidad desp Imp		5360,8	5419,69592	6722,30352
(+) Depreciación				
(+) Valor Libro				
(+) Crédito	2390			
(-) Amortiza Crédito		736,19901	795,094931	858,702525
(-) Inversión Inicial	-3186			
(-)				
/+) Capital de Trabajo	-534			534
(=) Flujo de Caja	-1330	7128,99901	7246,79085	8115,00604

Del flujo de caja que antecede se obtiene que el VAN del proyecto teniendo un financiamiento del 75 % es de US\$14811,05 dólares americanos y un TIR de 537 %. Además con la información anterior establecemos la sensibilización del proyecto, la cual entrega la siguiente tabla.

Tabla 4 - 16. Tabla de sensibilización del ingreso para proyecto financiado al 75 %

Disminución de Ingresos en %	VAN
0	\$14.811,05
-10%	\$13.159,48
-20%	\$11.639,47
-30%	\$10.119,45
-40%	\$8.599,43
-50%	\$7.079,42
-60%	\$5.559,40
-70%	\$4.039,39
-80%	\$2.519,37
-90%	\$ 999,35
-100%	-\$ 520,66

A partir de esta tabla se obtiene el siguiente gráfico que muestra la tendencia del VAN en la medida que el ingreso disminuye.

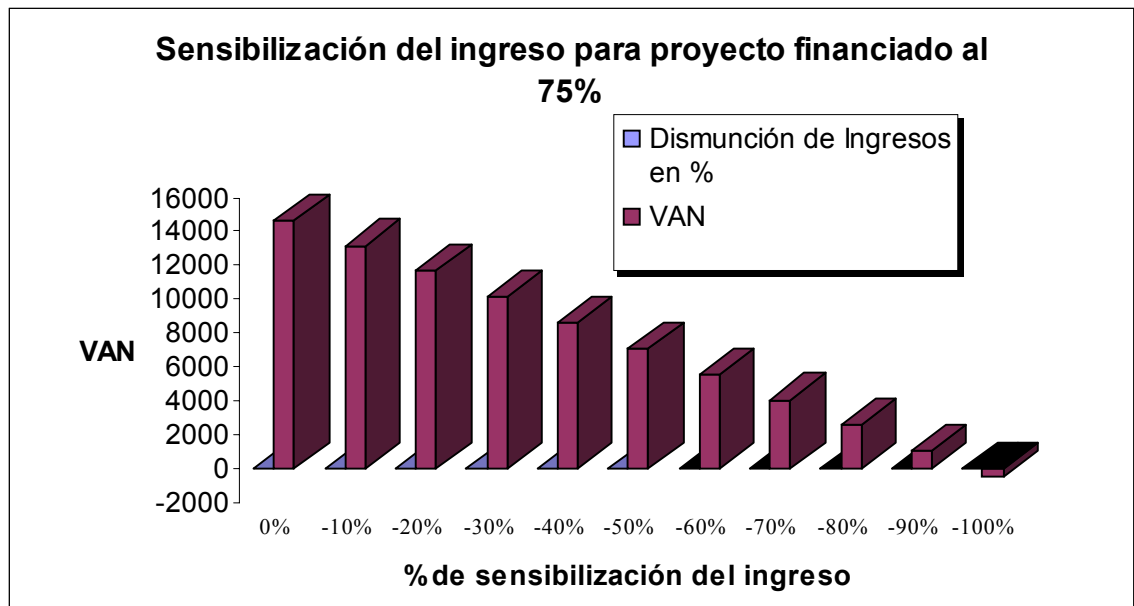


Gráfico 4 - 5. Tendencia de la disminución de ingresos para proyecto financiado al 75%.

En este último escenario se presenta un VAN cero al disminuir el ingreso en un 96,57%.

Tabla 4 - 17. Tabla de sensibilización del egreso para proyecto financiado al 75 %

Aumento de los Egresos	VAN
0	\$ 14.811,05
100%	\$ 13.598,67
200%	\$ 12.517,85
300%	\$ 11.437,03
400%	\$ 10.356,20
500%	\$ 9.275,38
600%	\$ 8.194,55
700%	\$ 7.113,73
800%	\$ 6.032,91
900%	\$ 4.952,08
1000%	\$ 3.871,26
1100%	\$ 2.790,43
1200%	\$ 1.709,61
1300%	\$ 628,78
1400%	-\$ 452,04

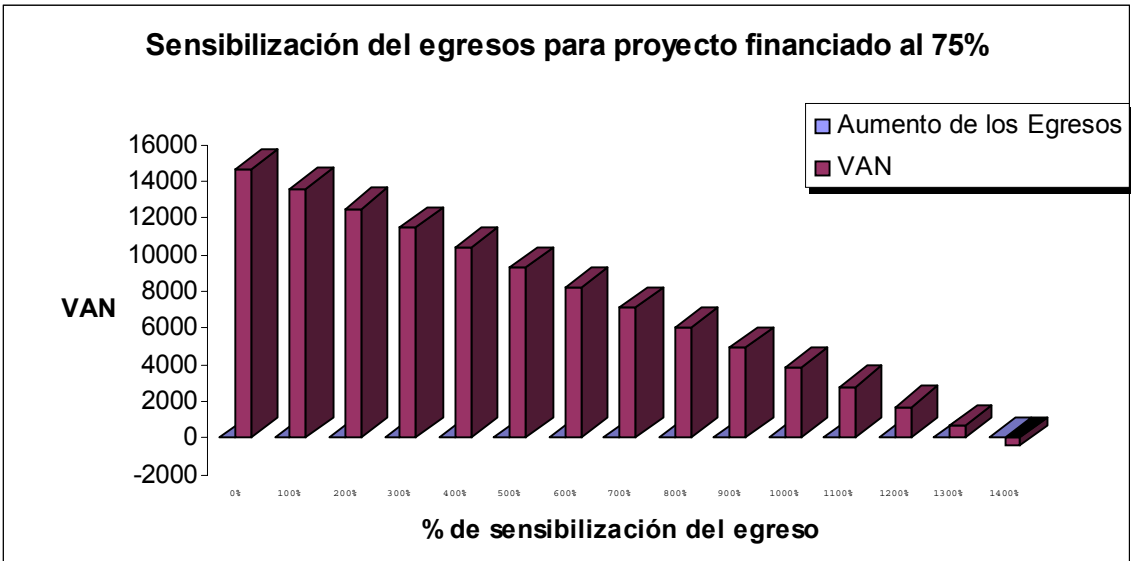


Gráfico 4 - 6. Tendencia de la disminución de los egresos para proyecto financiado al 75%.

Sus egresos al verse aumentados en 1400,58% hacen que su VAN se haga cero con lo cual deja de ser atractivo el proyecto.

A partir de los antecedentes antes entregados, se puede establecer que económicamente es viable por los altos valores que se obtuvieron del VAN en los tres

escenarios a los cuales se expuso; además al evaluar el TIR resultante, este permite sentar la recuperabilidad de lo invertido con creces, esto se refleja que teniendo una tasa de descuento del 12%, se tiene un TIR para la figura de proyecto puro de 169%.

4.2 **EXPERIENCIA**

4.2.1 Problemáticas de instalación

Las pruebas preliminares que se han realizado utilizando el software escogido tanto para la plataforma como el relacionado con la comunicación segura, llamado servicio de enlace VPN, han resultado exitosas; sin embargo no han estado exentas de problemas, los cuales se dividen en 2 grupos:

- Problemas de Plataforma: El principal problema se suscitó al utilizar la distribución de Linux, Redhat 7.3, debido a que aparecía como compatible y cumpliendo con los requisitos necesarios para soportar éste servicio, esto resultó ser infructuoso al hacer uso de ésta, ya que en algunos casos se debió recurrir a la compilación de los mismos, lo que trajo consigo el tener que realizar cambios a los programas fuentes, todos los cuales están escritos en lenguaje C³², principalmente debido a la relación de estos con los llamados archivos de “cabecera”, los cuales contienen funciones y/o definiciones de variables las cuales serán utilizadas posteriormente, cuya extensión es .h provocado por estar mal referenciados, además del uso de funciones que no estaban soportadas ya que habían sido reemplazadas por otras o bien bibliotecas las cuales estaban mal apuntadas.

³²www.cs.cf.ac.uk/Dave/C/CE.html

- Problemas anexos: Son aquellos elementos que aunque no forman parte de la solución en sí, son necesarios. Ellos son los que participan de los protocolos de enrutamiento TCP/IP, los cuales inciden enormemente debido a que los diferentes software que se utilizan para brindar este servicio seguro, no contemplan realizar dichas operaciones y tampoco automatizar dicho proceso, es por ello que resulta necesario el contar con las herramientas adecuadas para dicha labor, siendo estas: ipchains o iptables³³, se presentan 2 debido a que esta versión de RedHat cuenta con los dos, éstas proveen de enrutamiento entre la red externa y el área segura, en éste caso se prefiere utilizar iptables por ser más robusto como aplicación y brindar mayores posibilidades de filtrado y encaminamiento de los flujos de datos; además se cuenta con el comando route³⁴, quien entrega la facilidad de establecer rutas, o caminos, por las cuales fluirá la comunicación entre el emisor y receptor tanto de ida como de vuelta.

4.2.2 Posibilidades de desarrollo

Aquí nos encontramos con una gran gama de potencialidades que ésta solución puede brindar a través de este proyecto. Se entiende que es posible entregar una serie de funcionalidades que van de facilitar una comunicación segura, como también pasar a un sistema de conexión de voz sobre IP, el cual se securiza por este medio; además se presenta la facilidad de integrar eventualmente todo los servicios de la escuela y/o instituto por medio de un sólo canal de comunicación seguro, el cual podría involucrar cualquier tipo de servicio, desde la transmisión de datos vía protocolo ftp hasta posibles modificaciones de base de datos locales.

³³ www.iptables.org

³⁴ www.redhat.com

Aún cuando la solución conlleva el que la transmisión de datos entre un punto y otro sea seguro, no media en el tema que todo lo que se genere en esta área confidencial esté seguro en su tránsito entre el emisor y el receptor, es así como el correo electrónico es un caso palpable, es por ello que se comprende esta omisión en favor del objetivo particular del proyecto, por lo cual éste tópico es dejado para ser solucionado posteriormente.

Lo más importante es considerar que cualquier software tiene diferentes formas de ser instalado en una plataforma Linux, ya sea haciendo uso de un archivo que al ser invocado desde una aplicación se instala o bien por medio de su compilación, al contarse con su código fuente, siguiendo las instrucciones que por lo general vienen con el software; sin embargo existe la problemática de que los llamados “paquetes” tienen relación con otros elementos del mismo tipo provocando que éstos deban estar presentes, o sea instalados, antes de instalar el software que se necesita. En el caso de los software que deben compilarse, ocurre que no vienen totalmente depurados y por lo tanto requieren algunas veces realizarles cambios, que aunque resultan menores, dificultan la normal instalación de estos. En el caso de los rpm, las dependencias con otros “paquetes” o rpm es lo que más problemas puede causar, para lo cual un buen conocimiento del sitio de la distribución de Linux con la cual se está trabajando, ftp.redhat.com, es siempre conveniente; para los que se deben compilar se requiere poseer un buen conocimiento de programación en lenguaje C, ya que éste, Linux, está basado en él. Con ello permitirá que actualizaciones, como por ejemplo cambios en una sentencia “for” o bien en la asignación de directorios para la referencia a archivos de cabecera sea trivial.

Una de los recursos más importantes para trabajar con Linux, es poseer una comunicación expedita con Internet o en su defecto poseer la distribución en cdrom. Una vez que se tiene esto lo que importa de ahí en adelante es establecer en base a los conocimientos con que se cuenta y la experiencia a la cuál se pueda tener acceso, ya sea en forma presencial o por medio de Internet, de cual sería el equipamiento ad-hoc para el

o los servicios que se desean implementar. Es por ello que la disponibilidad de hardware para la elaboración de pruebas es muy necesario, ya que con ello se disminuyen los problemas que pudieran suscitarse en el desarrollo de este proyecto al haber realizado pruebas preliminares; esto se aplica a cualquier proyecto que tenga relación con TI.

CONCLUSIONES

La TI evoluciona vertiginosamente, es así como se tiene que hace unos cuantos años atrás no se pensaba en la seguridad como algo que preocupara a quienes desarrollaban los protocolos de comunicación y menos los Sistemas Operativos; sin embargo hoy es un elemento fundamental para poder seguir existiendo en el mercado debido a que cualquier filtración de información podría provocar una debacle en la organización. Más aún si esta dice relación con entidades como CONICYT.

Es por ello que existiendo los medios y después de ver la solución propuesta se establece que las soluciones no necesariamente pasan por adquirir equipamiento propietario para solucionar éste tipo de problemática, sino tan solo los conocimientos suficientes para plasmarlos en una maquina con tecnología Intel y un Sistema Operativo de fuente abierta.

Al tener que trabajar con un lenguaje como C, al instalar los servicios necesarios para brindar el acceso seguro uno ha conocido más de cerca el como se interactúa con la maquina, no para llegar a nivel de la maquina, pero si lo suficientemente cerca, lo cual ha resultado ser muy enriquecedor.

Aunque las soluciones muestren que están probadas y funcionando, teóricamente, el experimentar con está, muestra la existencia de problemas en la instalación,. es por ello que mediante el uso de herramientas de depuración como lo es “strace”, se logra soslayar este tipo de dificultades.

Las comunicaciones son un elemento fundamental para el proyecto, es así que al enfrentarse a problemas de esta índole, resulta muy útil utilizar herramientas como “tcpdump”, la cual permite realizar un análisis del tráfico y con ello detectar las anomalías que pudieran afectar el buen funcionamiento de la solución.

Por último, es necesario consignar que la seguridad es un elemento que debe llevar toda aplicación; sin embargo ésta debe ir acompañada de una gran cantidad de conocimientos de comunicaciones, esto debido al principio que yace en que puedo

proteger una casa poniendo muros muy altos, pero luego uno se da cuenta que no existe la forma de poder entrar en ella.

BIBLIOGRAFÍA

[url 1] http://www.freeswan.org/freeswan_snaps/CURRENT-SNAP/doc/quickstart.html

Nota: En esta página se hace mención a un esquema de instalación rápida del producto FreeSwan.

[url 2] <http://www.poptop.org/PoPToP-RedHat-HOWTO.txt>

Nota: Breve explicación de como configurar el servicio VPN utilizando PPTP y que se llama PoPTop.

[gsc 00] Ma Nieves Gutiérrez, Ana Rosa Sancho y Amadeo Casas, *Estudio sobre las VPN (Redes Privadas Virtuales)*, 2000

Nota: En el escrito se realiza una descripción detallada de lo que es una red privada virtual, además de entregar información relevante a los estándares utilizados para establecer dicho servicio.

[spi 01] Santiago Pérez Iglesias, *Análisis del protocolo IPsec: el estándar de seguridad*, 2001

Nota: Es este escrito se trata en profundidad el protocolo para comunicaciones seguras más robusto que existe hoy en día.

ANEXOS

ANEXO 1: ESQUEMA DE INSTALACIÓN Y CONFIGURACIÓN LINUX

Instalación de distribución de Linux

- Se debe contar con los cdrom de instalación, que en su versión 7.3 son 3 discos.



Figura A1 - 1. Caja con distribución RedHat de Linux.

- De preferencia se debe bootear del primer cdrom e instalar en modalidad servidor; en caso de no ser posible se deben crear los disquetes de instalación, los cuales se generan con el programa rawrite en modalidad dos, éste viene en el primero de los discos compactos de la distribución y las imágenes necesarias para crearlos también se encuentran en él. Para una mejor apreciación del proceso se muestra a continuación un ejemplo:
 - C:\> d:
 - D:\> cd \dosutils
 - D:\dosutils> rawrite
 - Enter disk image source file name: ..\images\boot.img

- Enter target diskette drive: a:
 - Please insert a formatted diskette into drive A: and
 - press --ENTER-- : [Enter]
 - D:\dosutils>
- Por medio de este procedimiento se lleva a cabo tanto el particionamiento del disco en el cual se instalará la distribución de Linux, además de la instalación del software propiamente tal.
 - Durante el proceso se pedirá que se ingrese una contraseña para la cuenta que lleva por nombre “root”; ésta corresponde al que administra el sistema instalado. Se debe contemplar para efectos de seguridad una contraseña que cuente a lo menos con 8 caracteres mezcle números y letras.
 - Se reinicia el sistema.
 - Una vez reiniciado el sistema y haya llegado a pedir en pantalla un login, se debe ingresar la palabra root y la contraseña que se consideró la más adecuada durante el proceso de instalación. Esto se puede apreciar a continuación en el ejemplo siguiente.

Ejemplo

- Red Hat Linux release 7.3 (Valhalla)
- Kernel 2.4.18-10 on an i686
- login:

ANEXO 2: ESQUEMA DE INSTALACIÓN DE SERVICIOS VPN

Instalación de servicios VPN

Una vez instalada la plataforma se procede a la instalación del software que permitirá brindar el servicio de VPN, se comenzará con Vpnd. Para realizar dicha tarea se deberán realizar lo siguiente pasos:

- Como todo software para la plataforma Linux, aquí se puede instalar el “rpm” o bien a partir de los archivos fuentes compilar el software e instalarlo; se recomienda la primera forma, ya que resulta ser más transparente para quien debe instalarlo.
- Luego se genera la clave de sesión mediante el siguiente comando: `vpnd -m /etc/vpnd/vnpnd.key`, aquí lo primero es el comando, luego la opción `-m`, la cual significa que deje lo que generará en el directorio que lo precede; ésta se le hace llegar al cliente por algún medio como puede ser el correo electrónico o un disquete.
- A continuación tenemos cómo debería quedar el archivo de configuración del servicio VPN, el cual se encuentra en el directorio `/etc/vpnd` por omisión.

El contenido del archivo de configuración en el servidor, que se encuentra en el directorio `/etc/vpn` y se llama `vpnd.conf`, es el siguiente:

```
mode server

# Dirección IP y puerto del servidor

server a.b.c.d 2001

# Dirección IP y puerto del cliente

client w.x.y.z 2001

# Dirección IP privada del servidor
```

```
local a.b.c.d

# Dirección IP privada del cliente

remote w.x.y.z

# Opciones generales

autoroute Keepalive 10

noanswer 3

keyfile /etc/vpnd/vpnd.key

pidfile /var/run/vpnd.pid

keyttl 120

randomdev /dev/urandom

mtu 1600
```

Cambiando los valores a.b.c.d por el número ip del equipo servidor, w.x.y.z por la del cliente, a.b.c.d (local) por la dirección privada, pudiendo ser estas aquellas que comiencen con 192.168 o bien con 10.0, ya que así se han definido en Internet el rango de direcciones privadas o para ser utilizadas en intranets sin acceso a Internet. Por último se cambia la w.x.y.z (remota) por la dirección privada del cliente pudiendo utilizar cualquiera del rango antes mencionado.

Ahora bien en el caso del FreeSWan se contempla el siguiente procedimiento para su instalación. Al igual que el software anterior, la instalación de éste se puede realizar utilizando su versión en paquete (rpm), o bien mediante la compilación de sus archivos fuentes, procediendo a instalarlo de acuerdo con el procedimiento entregado por quienes desarrollaron el software. Hay que hacer notar que este paquete tiene una particularidad, que tiene relación con la versión a instalar, y se refiere a que debe ir a la

par con la versión de kernel de la distribución, por lo tanto para establecer cuál paquete utilizar se debe seguir el siguiente procedimiento:

- Establecer la versión del kernel que se encuentra activo; éste se obtiene ejecutando el comando “uname -a”, el cual entrega una salida como ésta

```
Linux lll.ucv.cl 2.4-18.10enterprise #1 SMP Fri Oct 26 13:15:53 EDT
2001 i686 unknown
```

De lo anterior establecemos que la versión del kernel es 2.4-18.10 y por lo tanto los paquetes en el caso que se deseen instalar vía rpm deberían seguir esta nomenclatura `freeswan-module-1.98b_2.4.18_10.i386.rpm` y `freeswan-1.98b_2.4.18_10.i386.rpm`.

- Si se desea instalar el software utilizando los archivos fuentes, el procedimiento será el siguiente:

- 1 Obtener desde el sitio oficial del producto el archivo de firma del software, el cual tiene por nombre `rpmsign.pgp`

2. Luego agregar éste a tus claves PGP así: `pgp -ka rpmsign.pgp`

3. Chequear la firma con el archivo que contiene los fuentes del software de ésta manera: `pgp freeswan-1.98b.tar.gz.sig freeswan-1.98b.tar.gz`

4. Al finalizar este proceso tiene que aparecer la siguiente leyenda: Good signature from user "Linux FreeS/WAN Software Team". Signature made 2002/06/26 21:04 GMT using 2047-bit key, key ID 46EAFCE1. Con esto aseguramos que el archivo es el que corresponde.

5. Estando en la máquina como superusuario, es decir habiendo ingresado con el login de root, desempaquetamos el archivo con extensión tar mediante la utilización del utilitario tar o unzip.

6. De preferencia se debe desempaquetar en el directorio `/usr/src`, ya que por omisión es donde deben residir los fuentes de los software que deseemos instalar; para ello utilizaremos el comando mv así:

- `mv freeswan-1.98b.tar.gz /usr/src`

Luego nos desplazaremos al directorio de la siguiente manera,

- `cd /usr/src`

Por último se procede a realizar la descompresión del archivo que contiene los fuentes del software de ésta manera:

- `tar -xzf freeswan-1.98b.tar.gz`

7. En la eventualidad que hubiesen parches que aplicar este contiene la forma de aplicarlo a la distribución de fuentes que uno tiene.

8. Por último uno debe cambiarse al directorio que se genera al descomprimir el archivo:

- `cd /usr/src/freeswan-1.98b`

Luego se procede a compilar los archivos fuentes mediante el uso del siguiente comando `make`, luego `make oldmod` para realizar la compilación de los modulos y al final un `make install` para instalar el software.

9. Para iniciar el servicio y probarlo, se debe primero ejecutar éste comando “`service ipsec start`”. Esto no requiere reiniciar la máquina.

10 Para probar que el software quedó satisfactoriamente instalado, se ejecuta el comando “`ipsec verify`”, el cual debiera enviar a pantalla lo siguiente:

Checking your system to see if IPsec got installed and started correctly

Version check and ipsec on-path [OK]

Checking for KLIPS support in kernel [OK]

Checking for RSA private key (/etc/ipsec.secrets) [OK]

Checking that pluto is running [OK]

En la eventualidad que la salida no fuera como se indica, existe una guía de solución de problemas en el sitio donde se obtuvieron los fuentes del software³⁵.

Por último tenemos el software PoPToP, que mediante el siguiente procedimiento se instala:

- Se debe contar con una versión de kernel superior a 2.2.12-20
- Se debe actualizar la versión del software ppp a 2.3.10-1, por medio de un paquete rpm, que en este caso sería ppp-2.3.10-1.i386.rpm.
- Obtener el paquete del software y los archivos de inicialización, los cuales se pueden encontrar en <http://poptop.lineo.com/releases> y llevan por nombre pptpd-1.0.0-1.i386.rpm y pptpd.init.
- Grabar el archive pptpd.init en el directorio /etc/rc.d/init.d, asegurándose de tener los permisos correspondientes.
- Se da ejecución al servicio por medio del siguiente comando:
`/usr/sbin/pptpd -d`
- Con anterioridad se debe configurar el archivo chap-secrets, el cual se ubica en el directorio /etc/ppp. Este debe verse de acuerdo al siguiente esquema:

```
1. # /etc/ppp/chap-secrets
```

```
2. #usernameservernamesecretipaddress
```

```
3. validname*validpass*
```

Para validar a los clientes Windows se debe usar esta nomenclatura: DOMAINNAME\\validname*validpass*; se hace notar que el DOMAINNAME es sensible al uso de mayúsculas y minúsculas.

³⁵ <http://www.fresswan.org>

- Editar el archivo `/etc/inittab` y comentar con un signo “#” la referencia al servicio `pptpd`, debido a que la aplicación que se instaló utilizará ese nombre.
- Hacer que el servidor vuelva a leer al archivo mediante el siguiente comando: `rereads /etc/inittab`
- Una vez que se ha establecido lo anterior, se deben cambiar las opciones del servicio en el archivo `options.pptp` que se ubica en el directorio `/etc/ppp/`; éste debe tener como mínimo las siguientes líneas dentro de éste archivo:

```
lock

debug

auth

+chap

proxyarp
```

- Luego se modifica el archivo `pptpd.conf` que se encuentra en el directorio `/etc`, este debiera lucir como se muestra a continuación:
 - `debug` #Esta opción se puede remover luego de estar seguro que el servicio está funcionando adecuadamente.
 - `option /etc/ppp/options.pptp`
 - `localip 192.168.1.80-89` direcciones IP privadas que no pueden ser vistas desde el exterior, pero si los equipos internos y los que establezcan una sesión con el servidor de enlace, llámese a esto en nuestro caso al nodo de la organización y a Internet.
 - `remoteip 200.20.45.33` # direccionamiento ip valido para interactuar con el exterior.

Hasta este punto se está trabajando sin encriptación; para lograr eso se debe seguir el siguiente procedimiento:

- Obtener la distribución con los archivos fuente desde `ftp://cs.anu.edu.au/pub/software/ppp/` y rescatar el archivo `ppp-2.3.11.tar.gz`.
- Parchar la distribución fuente con el archivo `ppp-2.3.11-openssl-0.9.5-mppe.patch.gz`, el cual se obtiene de `ftp://ftp.binarix.com/pub/ppp-mppe`; este parche soluciona el problema que existe con la modalidad `ppp_mppe`, la cual consiste en que luego de una resincronización un paquete se perdía.
- Además se debe obtener el archivo `ppp_mppe_compressed_data_fix.diff`, el cual se descarga desde `http://www.vibrationresearch.com/pptpd/`; con este parche solucionamos un problema de pérdida de paquetes por resincronización.
- Teniendo los tres archivos, el `ppp-2.3.11.tar.gz`, `ppp-2.3.11-openssl-0.9.5-mppe.patch.gz` y `ppp_mppe_compressed_data_fix.diff`, se copian al directorio `/usr/src` el cual habitualmente se utiliza para estos fines, descomprimos el primer archivo con el comando `tar`, de la siguiente manera: `tar -zxvf ppp-2.3.11.tar.gz`, luego lo hacemos con el archivo `ppp-2.3.11-openssl-0.9.5-mppe.patch.gz`, pero utilizando el comando `gunzip`, de esta forma `gunzip ppp-2.3.11-openssl-0.9.5-mppe.patch.gz`.
- Nos cambiamos de directorio de la siguiente forma: `cd /usr/src/ppp-2.3.11`
- Luego aplicamos el parche así `patch -p1 < ../ppp-2.3.11-openssl-0.9.5-mppe.patch`.

- Nos volvemos a cambiar de directorio a `/usr/src/ppp-2.3.11/linux` utilizando el comando `cd`.
- Y parchamos con el segundo archivo de parche de esta manera: `patch < ../../ppp_mppe_compressed_data_fix.diff`
- Retrocede 2 directorios [`cd ../../`]
- Nos desplazamos al directorio `/usr/src/ppp-2.3.11`
- Ejecutamos el programa `./configure`, luego `make`, posteriormente `make kernel` y por último `make install`.
- Ahora procedemos a construir los módulos, que son los que nos proveerán de la funcionalidad de tener VPN.
- Se desplaza al directorio `/usr/src/linux` y se ejecuta el siguiente comando: `make modules SUBDIRS=drivers/net`, luego se desplaza al directorio `drivers/net` y se copian los archivos `ppp.o`, `slhc.o`, `bsd_comp.o`, `ppp_deflate.o` y `ppp_mppe.o` al directorio `/lib/modules/2.2.12-20/net` a continuación se edita el archivo `/etc/conf.modules` (o bien `modules.conf` depende la versión del kernel), anexándose la siguientes líneas:
 1. `alias char-major-108 off # Este será diferente para kernels que posean una versión 2.3.x`
 2. `alias ppp-compress-18 ppp_mppe`
 3. `alias ppp-compress-21 bsd_comp`
 4. `alias ppp-compress-24 ppp_deflate`
 5. `alias ppp-compress-26 ppp_deflate`
- Se verifica que los módulos hayan sido cargados en memoria, con el comando `lsmod`

- En la eventualidad de no estar, se cargan con el comando: `depmod -a`
- Se prueba que están funcionando adecuadamente mediante el comando: `modprobe ppp`, para luego proceder a configurar el archivo `options.pptp` y seguir con los pasos que se mencionaron en un principio, eso si agregando lo siguiente:

1. `+chapms`
2. `+chapms-v2`
3. `mppe-40`
4. `mppe-128`
5. `mppe-stateless`
6. `auth`
7. `require-chap`
8. `+chap`
9. `name pptpd`

ANEXO 3: CONFIGURACIÓN DE CLIENTE WINDOWS EN AMBIENTE SEGURO

En el caso del cliente VPN, se explicará con detalle el que viene preinstalado en los equipos con windows, esto debido a que es la plataforma de estación de trabajo por excelencia.

Desde la versión 95 en adelante se encuentra disponible esta aplicación, la cual guarda algunas diferencias entre ellas. En este caso se mostrarán los pasos a seguir en un equipo con una versión de windows 2000 professional.

Instalar el adaptador privado virtual de la red en el pc cliente

- En el Escritorio del PC hacer clic en el botón **Inicio** para luego seleccionar la opción configuración y de allí conexión de redes y de accesos telefónicos, para por último seleccionar asistente para conexiones de red el cual presenta la siguiente pantalla:



Figura A3 - 1. Asistente de conexiones a redes.

- Pulsar con el botón siguiente y seleccionar el ítem destacado **Conectar a una red privada a través de Internet:**

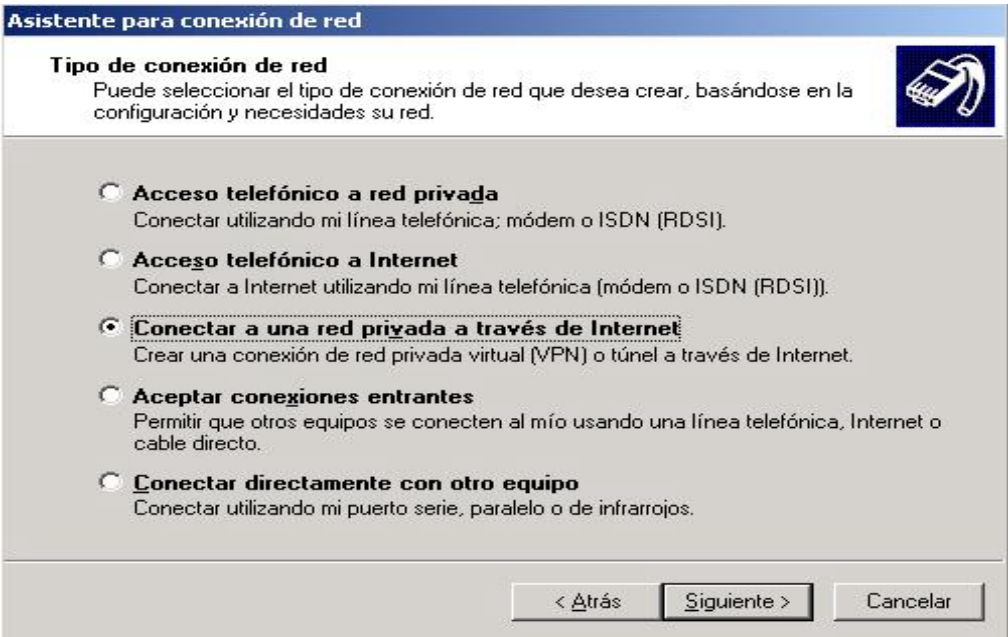


Figura A3 - 2. Selección del tipo de conexión de red.

- Entonces, se abrirá el **Diálogo de red pública:**

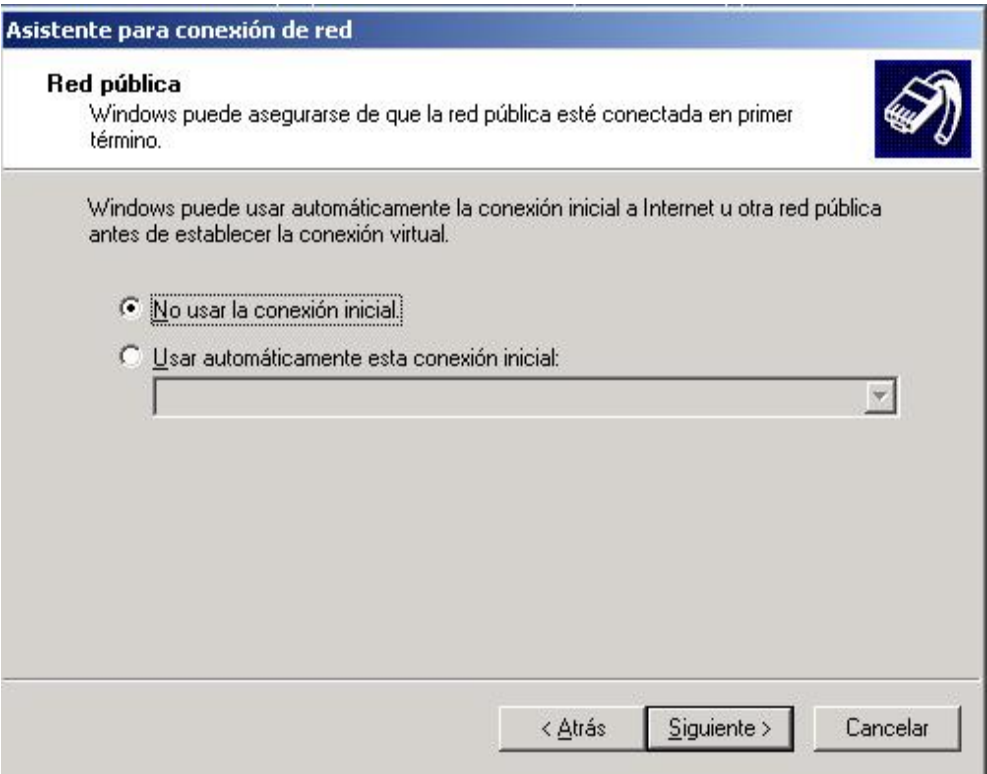


Figura A3 - 3. Selección de la red pública para el asistente de conexión.

- Una vez seleccionado la opción “no usar la conexión inicial”, se transita al cuadro de dialogo, donde se especifica la dirección IP o el nombre del equipo servidor de enlace VPN.

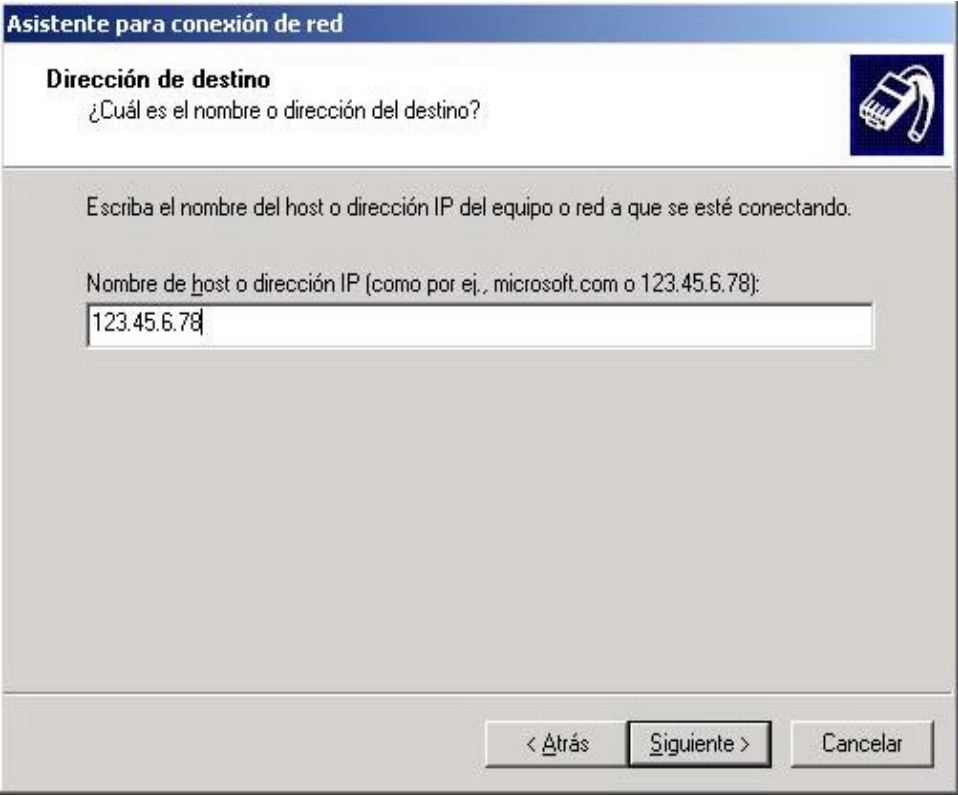


Figura A3 - 4. Selección de la dirección destino del servidor de enlace VPN.

- Se establece la disponibilidad de conexión.



Figura A3 - 5. Selección de la disponibilidad de conexión.

- Se establece si esta conexión será compartida a otros recursos de Internet.



Figura A3 - 6. Selección compartida de esta conexión.

- Finalización del asistente a conexión a red segura.



Figura A3 - 7. Finalización de la conexión a una red segura.

- Finalmente aparecerá en ítem de conexiones de red y de acceso telefónico el icono asociado a la conexión que se acaba de realizar.

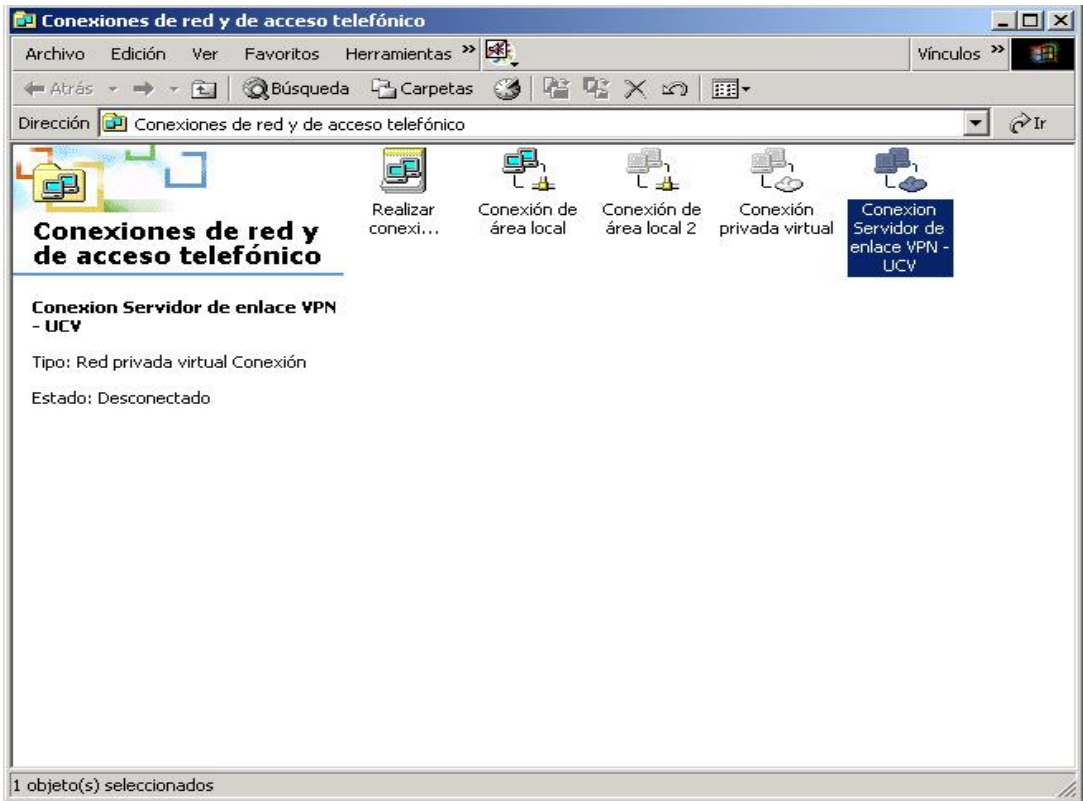


Figura A3 - 8. Ventana de acceso a la conexión segura.

- Establecimiento de la comunicación con el servidor VPN, el cual proveerá el acceso al área protegida.



Figura A3 - 9. Ventana de conexión por medio de la cual se accede al entorno protegido.

ANEXO 4: GLOSARIO

UIC : Unidad de Computación e Informática

TI : Tecnología de la Información

DSIC : Dirección de Servicios de Informática y Comunicaciones

TICS : Tecnologías de la Computación

TÚNEL: esquema de conexión de comunicación que se establece una vez que se ha negociado entre los dos extremos el inicio de la misma.

PPTP : Point to Point Tunneling Protocol

L2TP : Layer two Tunneling Protocol

IPSEC : Internet Protocol Security

ISO/OSI : International Organization for Standardization/Open Systems Interconnection

IETF : Fuerza de tarea de Ingeniería de Internet

PKI : Infraestructura de clave pública

HMAC : MAC con hash, donde MAC es Código de autenticación de mensaje.

ESP : Encapsulating Security Payload

IKE : Internet Key Exchange

DNS : Servicio de Resolución de Nombres

CA : Autoridad de Certificación

CRL : Lista de Certificados Revocados

LDAP : Lightweight Directory Access Protocol

SCEP : Simple Certificate Enrollment Protocol

PKCS : Public-Key Cryptography Standards

TOS : Type Of Service

VOIP : Voz sobre ip

B2B : negocio a negocio

VPN : Red Privada Virtual

QoS : Quality of Service (Calidad de Servicio)

Kernel : Corazón o parte fundamental del sistema operativo.

Paquete : Formato que presentan los software a ser instalados en la distribución RedHat

VAN : Valor Actual Neto

TIR : Tasa de Recuperación de la Inversión