TRABAJO ESPECIAL DE GRADO

IMPLANTACION DE UNA RED PRIVADA VIRTUAL (VPN) PARA EL ACCESO SEGURO Y CONTROLADO AL SISTEMA DE INFORMACIÓN DEL SECTOR ELECTRICO VENEZOLANO (SISE)

Presentado ante la Ilustre Universidad
Central de Venezuela para optar al Título
de Especialista en Comunicaciones y
Redes de Comunicación de Datos.

Autor: Ing. Pablo José Echenique Salas

Caracas, Noviembre de 2004

TRABAJO ESPECIAL DE GRADO

IMPLANTACION DE UNA RED PRIVADA VIRTUAL (VPN) PARA EL ACCESO SEGURO Y CONTROLADO AL SISTEMA DE INFORMACIÓN DEL SECTOR ELECTRICO VENEZOLANO (SISE)

TUTOR ACADEMICO: Msc. Vicenzo Mendillo
TUTOR INDUSTRIAL: Ing. Carlos Lamus

Presentado ante la Ilustre Universidad Central de Venezuela para optar al Título de Especialista en Comunicaciones y Redes de Comunicación de Datos.

Autor: Ing. Pablo José Echenique Salas

Caracas, Noviembre de 2004

Certifico que he leído este trabajo de Grado y que lo encuentro apropiado tanto en su contenido como en su formato y apariencia externa

Msc. Vicenzo Mendillo

Fecha

Trabajo de Grado aprobado en nombre de la Universidad por el siguiente Jurado:

_____

Coordinador

_____

_____

Dedicatoria

El éxito alcanzado en el desarrollo del presente Trabajo Especial de Grado está especialmente dedicado a mis padres, por haberme impulsado hacia el buen camino, con sus enseñanzas y lecciones, a ti abuelita por consentirme y entenderme, a ti Jesús por apoyarme y extender siempre tu mano en procura de mi bienestar.

A todos mis familiares y hermanos por estar a mi lado en todo momento, en especial a mis tías Leonor y Omaira que han sido factor de apoyo en los momentos difíciles de mi vida.

De igual forma extendiendo ésta dedicatoria a ti mi Dios, porque iluminastes el sendero del entendimiento y la sabiduría para salir airoso en ésta ardua lucha, por ello, me siento dichoso de tener tu apoyo.

Sientase todos, participes de éste triunfo.....

Reconocimientos

Agradezco a Dios en primer lugar por darme salud y llenarme de fuerzas para emprender y lograr éste arduo reto.

A Vicente Mendillo, quien en todo momento me prestó su ayuda y colaboración tanto en materia técnica y científica, así como, en la metodología y presentación del presente trabajo.

A mi Madre y Hermano, quienes con su presencia y colaboración fortalecieron mi Capacidad, Autoestima y Disposición al logro de los objetivos de la investigación.

A mis preciados amigos Alirio, Nasle y Joe, quienes me facilitaron recursos técnicos necesarios en el desarrollo del presente trabajo.

A la Alta Gerencia de FUNDELEC, por permitirme desarrollar la investigación en su sede utilizando recursos de la organización.

Más en general, y sin citar a nadie en concreto. A todos los que preguntaron una (y mil) veces cómo iba la cosa, a los que se interesaron por cuándo terminaba, a los que hacían lo que podían por presionar mi voluntad para avanzar, y a todos los que han comprendido la tardanza.

Gracias a todos.

Pablo J, Echenique S.

"No cabe duda que una tesis es un punto culminante en el mundo académico, pero también es cierto que no deja de ser un eslabón más en la cadena de la vida, y en esta vida ya son muchos los eslabones engarzados."

García Lorca

IMPLANTACION DE UNA RED PRIVADA VIRTUAL (VPN) PARA EL ACCESO SEGURO Y CONTROLADO AL SISTEMA DE INFORMACIÓN DEL SECTOR ELECTRICO VENEZOLANO (SISE)

Autor: Ing. Pablo José Echenique Salas
Año: 2.004

Resumen

El Trabajo de Grado presentado a continuación se centró en la Implantación de una Red Privada Virtual para acceder de modo seguro a la información contenida en el Sistema de Información del Sector Eléctrico Venezolano. A pesar que el SISE cuenta con una infraestructura tecnológica informática dispuesta para que las empresas eléctricas Venezolanas suministren la información solicitada y requerida, a efectos regulatorios en las distintas áreas de su operación dentro del servicio eléctrico, con el desarrollo de éste estudio se fortaleció dicho esquema evitando que la información viaje completamente descubierta a través de la Internet, es decir, desde la empresas eléctricas hacia FUNDELEC y viceversa, dado al establecimiento de conexiones seguras y uso de la tecnología de intercambio de claves públicas y certificados digitales.

Cabe destacar, que el esquema físico y lógico de Interconexión fue determinado por la creación de una red perimetral o DMZ, lo cual, puntualiza el ámbito de control y seguridad del SISE en modo producción y no se compromete las aplicaciones inherente a las áreas internas de la organización. Asimismo, se adoptó el uso de IPSec como tecnología para el establecimiento del túnel privado entre el usuario y el SISE, dado a su capacidad de integración con Windows 2000 y otras plataformas. Todo ello, acelerará el proceso de intercambio de información y por ende se dispongan de más herramientas para la reestructuración, organización y proyección nacional e internacional del Sector Eléctrico Venezolano.

Índice General

Lista de Tablas, Ilustraciones y Anexos

Glosario de Términos

TERMINO	DESCRIPCION
ACL	Access List Control / Lista control de acceso
Cifrado	Trama de datos codificada
Dial Up	Llamada telefónica
Distance Working	Trabajo a Distancia
DMZ	Zona desmilitarizada ó Red Perimetral
FUNDELEC	Fundación para el Desarrollo del Servicio Eléctrico
Hacker	Intruso que vulnera seguridad de sistemas en la Internet
IPSec	IP secure / IP Seguro
LAN	Local Area Network / Red de Area Local
OLAP	On-line Analytical Processing / Procesamiento analítico en Línea
PKI	Public Key Interchange / Intercambio de Clave Pública
SISE	Sistema de Información del Sector Eléctrico
SSL	Socket Secure Layer / Capa de Pila Segura
Telework	Teletrabajo
VPN	Virtual Private Network
WAN	Wide Area Network / Red de Area Extendida
Worm	Gusano

Introducción

En el ámbito empresarial de ésta era, el manejo y administración de los sistemas de información que soportan el proceso de toma de decisiones poseen un papel protagónico. Es por ello que en las últimas tres décadas se ha observado un desarrollo acelerado en las tecnologías de información y comunicaciones (*TIC)*, en función de proveer los mecanismos de acceso que permitan a los ejecutivos y demás personal de las empresas, obtener con facilidad resultados precisos de la gestión y establecer indicadores en los distintos aspectos del negocio.

Dada la necesidad de hacer disponible la información referida al negocio, así como los sistemas y aplicaciones que las contienen (sistemas contables, puntos de ventas, aplicaciones financieras, herramientas de control de proyectos, entre otros.), en la década de los 80's fue introducido y puesto en marcha el concepto de Redes de Area Local *LAN*. Precisamente con el propósito de distribuir y asignar actividades específicas en cada área, lo que redunde en la optimización de los procesos y la mejora de la competitividad de la empresa.

Desde entonces, la tendencia a compartir información, servicios y recursos dentro de una *LAN* ha sido una necesidad constante. En consecuencia y con la ayuda del desarrollo y crecimiento de la red de redes *Internet*, dicha necesidad se ve expresada no solamente dentro de las fronteras de la organización sino fuera de ella.

El ejemplo más clásico tiene lugar en la necesidad de un representante de ventas en consultar el precio, disponibilidad o descuentos disponibles para cierto producto, a la hora que éste se encuentre frente a un potencial cliente fuera de su oficina, o la conexión necesaria que debe existir entre la casa matriz productora de calzados y sus sucursales, para mantener actualizado el inventario general de la tienda y la emisión automática a la casa matriz de la orden de reposición y abastecimiento del inventario de dicha sucursal.

Todo esto ha hecho que el concepto de teletrabajo haya sido objeto de acelerado desarrollo, a través del establecimiento de las Redes Privadas Virtuales (en lo sucesivo *VPN*), donde el objetivo principal apunta a la desarrollo de una estrecha interconexión a través de una red WAN (*Internet, Frame Relay,* ATM) entre las organizaciones y sus clientes, empleados, proveedores, aliados comerciales, etc., y estos dispongan de los sistemas y servicios de información necesarios y autorizados directamente desde la fuente de los datos, para así desempeñar sus actividades predefinidas.

Es por ello, y vista la necesidad que existe en FUNDELEC de hacer disponible un conjunto de información contenida en el Sistema de Información del Sector Eléctrico (SISE), así como, proveer los mecanismos que permitan el acceso controlado y seguro al sistema, lo que constituyen los elementos básicos donde se sustenta la presente investigación. La cual, dará lugar al estudio y aplicación del concepto de la tecnología *VPN*, a fin de establecer una vía de comunicación e intercambio de la información requerido dentro del marco de la regulación que existe entre la Fundación para el Desarrollo del Servicio Eléctrico “FUNDELEC” y los agentes y empresas del sector eléctrico Venezolano.

Asimismo, la red privada virtual a implementarse en FUNDELEC puede constituirse en el mecanismo que controle la carga y alimentación automática del SISE a través de la Internet, garantizando la autenticidad del usuario, la confidencialidad de la información y la autenticidad del origen de los datos.

1.- El Problema

1.1.- Planteamiento del Problema

La Fundación para el Desarrollo del Servicio Eléctrico "FUNDELEC", en su carácter de centro de investigación y apoyo técnico al estado venezolano en materia de organización, regulación y desarrollo del sector eléctrico, requiere disponer de la información actualizada y oportuna del historial de la gestión técnica, económica y operativa de cada una de las empresas eléctricas que operan en el Sector Eléctrico Venezolano, en sus respectivas áreas de desempeño y soporte al servicio.

Por ello, en FUNDELEC se ha desarrollado el Sistema de Información del Sector Eléctrico *SISE*, el cual provee la infraestructura tecnológica informativa para que las empresas eléctricas suministren la información solicitada y requerida en las distintas áreas de la operación del servicio eléctrico tales como: Distribución, Subtransmisión, Generación, entre otras. Todas están representadas en el sistema bajo el concepto de modelo y están concebidos y desarrolladas precisamente para facilitar la recopilación, consulta y análisis de la data necesaria para el estudio de los distintos aspectos y variables (indicadores) susceptibles a supervisión y regulación en el servicio eléctrico.

Para llevar a cabo el registro y actualización en la base de datos del SISE, de la información solicitada a cada una de las empresas eléctricas de acuerdo a la(s) área(s) comercial en la cual ésta se desempeñe, fue establecido un mecanismo para la recepción de dicha información a través de la dirección electrónica sise@fundelec.org.ve. Dicho mecanismo, no establece la verificación y certificación de la fuente u origen de datos, mejor conocido como “Autenticidad de la Fuente”, es decir, cualquier persona pudiera comprometer la fidelidad de la información contenida en el Sistema enviando información con la misma estructura solicitada, pero con valores distorsionados.

Asimismo, dicha información pudiera ser interceptada en el tránsito al destino, ser modificada y nuevamente reenviada al SISE, y el sistema una vez recibida la información activar los procesos de actualización y carga de la base de datos predefinidos. Acción que es conocida como “Ataque del hombre en el medio” lo cual compromete la integridad de la información contenida en el sistema.

De igual manera, es posible que algunos de los responsables por parte de la empresas eléctricas designados para el envío periódico de la información requerida por el SISE, confronten problemas con su computador y éste sea infectado por un virus informático tipo worm, cuya característica principal es el envío sucesivo a todas las direcciones electrónicas de correo registradas en su aplicación de correo, donde pudiera estar incluida la predefinida para el SISE (sise@fundelec.org.ve). Lo que, convertiría al mecanismo de recepción del SISE en un sistema ocupado ó bien exigido en consecuencia de la recepción múltiple y constante de los mensajes emitidos por dicho virus. Esta situación guarda relación con el tipo de ataque Interrupción de servicio (*Denial of Service*) y compromete la disponibilidad y estabilidad del Sistema.

Todo lo anterior descrito constituye las limitaciones de operación a las que está expuesto el SISE en su fase de recolección y conformación de su base de datos, lo que constituye un aspecto de gran consideración dado a que el objetivo principal del SISE es “consolidar un gran repositorio de datos confiables y validos acerca de la gestión y operación de las empresas eléctricas”.

Asimismo, es de notar que el ámbito de interés para la consulta de la información contenida en el SISE, transciende mucho más allá de las fronteras de la organización (FUNDELEC). De igual manera, existe un conjunto de modelos de datos que contienen información de uso clasificado,

que sólo pueden ser consultados por los usuarios autorizados, por lo que, dicho esquema debe mantenerse tanto en el ámbito Interno (Intranet), como en el Externo (Internet).

Se prevé el uso de la Internet como el método de comunicación para los usuarios remotos que deseen acceder a la información disponible en el SISE, dado a su crecimiento y establecimiento como la vía más común para la publicación y distribución de información a nivel mundial. Sin embargo, son conocidos los múltiples riesgos y amenazas a los que está expuesto un sistema hoy día en la Internet, dentro de los cuales se destacan: (a) Acceso no autorizado; (b)Modificación y/o alteración de la fuente; (c) Copia ó plagio de información; (d)Destrucción y/o eliminación de la fuente; (e) Disminución y/o detención de servicios; entre otros.

De allí parte la necesidad de proveer un mecanismo de acceso controlado y seguro a los usuarios remotos que requieran consultar y/o analizar modelos de información que respondan a sus necesidades informativas y que se encuentren fuera del ámbito público y genérico de la información contenida en el SISE.

Por todas las consideraciones antes mencionadas, el desarrollo e implementación de una Red Privada Virtual en FUNDELEC con el fin de hacer disponible la información contenida en el Sistema de Información del Sector Eléctrico, se vislumbra como el camino a seguir para proveer una forma segura de intercambiar información, lo cual facilite la actividad regulatoria de la organización.

1.2.- Justificación de la Investigación

La Fundación para el Desarrollo del Servicio Eléctrico “FUNDELEC” en concordancia con su papel de apoyo al ente regulador del servicio eléctrico Venezolano “CNEE-MEM”, evalúa el comportamiento de las empresas eléctricas tales como: EDELCA, CADAFE, EDC, ENELVEN, ENELBAR, ELEVAL, SENECA, entre otras. Dicha evaluación tiene lugar en los aspectos más particulares y característicos en las referidas empresas, y dentro de los cuales se destacan:

- Revisión de estados financieros y situación administrativa de las empresas.
- Revisión del plan de inversiones para la expansión y mantenimiento de la infraestructura que provee el servicio vs. los niveles tarifarios.
- Evaluación de las características y descripción del parque eléctrico ó red eléctrica.
- Evaluación del comportamiento de la demanda eléctrica según tipos de suscriptor ó cliente.
- Planificación y simulación del escenario eléctrico para los próximos años.
- Supervisión en las áreas de atención al cliente y recuperación de fallas.

Todos estos aspectos son la base para que los analistas eléctricos, establezcan los criterios para elaborar las recomendaciones y ajustes que contribuyan con el eficiente y rentable funcionamiento de las empresas eléctricas, así como el ordenamiento del Sector Eléctrico Venezolano.

Sin lugar a duda esto representa una tarea muy ardua de efectuar, dada la cantidad y la diversidad en que se presentan las fuentes informativas, así como sus formatos (documento en papel, archivo digital, sistemas de propósito específico, etc.). Es por ello el nacimiento del Sistema de Información del Sector Eléctrico “SISE”, el cual provee a los usuarios, es

decir las empresas eléctricas, las herramientas para estandarizar la captura y recolección de la información requerida para fines regulatorios, así como su presentación y despliegue lo que facilita a los especialistas (empleados de la organización) y a los usuarios en general (agentes del sector) diseñar sus consultas y recuperar la información necesaria de acuerdo a sus necesidades e intereses.

Por tanto, los beneficios que FUNDELEC obtendría con el desarrollo del presente trabajo, se remontan al hecho de poder establecer una vía de comunicación segura, confiable y compatible con los estándares utilizados en Internet, entre las empresas eléctricas ←→ MEM-FUNDELEC y MEM-FUNDELEC ←→ Agentes del sector.

En el caso de la comunicación que debe darse entre las empresas eléctricas y FUNDELEC con el objeto que éstas suministren la información requerida para la actividad regulatoria, el SISE provee los mecanismos de recepción y clasificación de la información, sin embargo, con la implementación de una Red Privada Virtual *VPN* en FUNDELEC, este esquema se verá reforzado por la aplicación de las técnicas y conceptos de autenticación, encapsulamiento, administración de políticas de seguridad, conectividad, etc., lo que garantizará que la gran base de datos que constituye el SISE sea actualizada sólo por los usuarios remotos debidamente autorizados.

Asimismo, a través de la consecución del presente trabajo, se concretará lo relativo a la comunicación que debe darse desde FUNDELEC hacia los agentes del sector, en función de hacer disponible la información del Sector Eléctrico Venezolano. Todo ello con la implementación de una Red Privada Virtual *VPN* que establezca el medio de acceso al SISE para los usuarios remotos, y por ende dicho sistema comience aportar sus frutos en la reestructuración, organización y proyección nacional e internacional del Sector Eléctrico Venezolano.

1.3.- Objetivo General

Diseñar e implementar una Red Privada Virtual (VPN) para hacer disponible la información contenida en el sistema de información del Sector Eléctrico SISE, de modo seguro a los usuarios y agentes autorizados del Sector Eléctrico Venezolano.

1.3.1.- Objetivos Específicos

- Crear una zona desmilitarizada “Red Perimetral” que contenga al Sistema de Información del Sector Eléctrico SISE, como una plataforma de servicio informativa a los agentes y usuarios autorizados del sector eléctrico.

- Formular los métodos y protocolos para la negociación segura de claves cifradas, autenticación de usuarios, utilizando Internet Key Exchange.

- Diseñar e implantar las políticas del tráfico que cursará a través Firewall (Corta Fuego / Puerta de Seguridad), el cual será la frontera entre la Internet y la Red Perimetral.

- Garantizar la disponibilidad e interoperatividad de extremo a extremo de la Red Privada Virtual, verificando la compatibilidad y capacidad de integración de los distintos componentes y sistemas que la conformen.

1.4.- Alcance de la Investigación

Con el objeto de dar cumplimiento a los objetivos planteados en el presente trabajo, se orientará la investigación a la consecución de los siguientes aspectos:

- **Implantación de una Red Privada Virtual**

  A fin de establecer independencia entre los recursos disponibles en la red LAN de FUNDELEC y los servicios de información que contiene el SISE, se implementará una zona desmilitarizada *DMZ* que sólo contenga la infraestructura provista por el sistema de información del sector eléctrico y posea sus propias políticas de acceso y seguridad (ACL's).

  Dado a que el universo de posibles usuarios del SISE transciende mucho más allá de las fronteras de FUNDELEC, no es recomendable comprometer la infraestructura de la red Interna, por lo que la *DMZ* representará un pequeño sector aislado que será el centro de atención de los servicios relativos al SISE.

  No obstante, debe existir una conexión desde la Red Interna hacia la *DMZ* para permitir que los usuarios internos (FUNDELEC) puedan hacer uso del SISE, por lo que se establecerá una Relación de Confianza en un solo sentido (*One Way Trust Relationship*).

- **Implantación de la compuerta de seguridad (Firewall)**

  Con el objeto de establecer una puerta de seguridad al tráfico cursado entre la DMZ e Internet, se implementará en la *DMZ* un firewall que controle y procese las peticiones de conexión proveniente desde Internet.

Todo ello con el fin de controlar el tráfico cursado desde y hacia la DMZ, aplicando los criterios de autenticidad, integridad y control de acceso, con ayuda de las tecnologías presentes en el protocolo IPSec.

- **Establecimiento del método de cifrado y enmascaramiento de la Información que viajará a través de la *VPN*.**

  Como se ha descrito anteriormente, FUNDELEC requiere que los agentes del Sector Eléctrico Venezolano suministren con cierta periodicidad la información de carácter regulatorio, por lo que, a través del desarrollo del presente trabajo se establecerá el mecanismo de certificación y autenticación de las fuentes ó remitentes y los usuarios del SISE, a los fines de reforzar la segura recepción y disposición de la información que estará almacenada en el repositorio de datos del Sistema de Información del Sector Eléctrico.

  Por lo que, se propone implementar el uso de certificados digitales para la autenticación de las fuentes, en las distintas formas de recepción y despliegue, tales como: Correos electrónico, http, ftp, disquete, cd-rom, etc.)

- **Establecimientos de criterios para la disponibilidad e Interoperatividad de la Red Privada Virtual.**

  Con el objeto de garantizar la disponibilidad e interoperatividad de la Red Privada Virtual, lo cual se traduzca en la accesibilidad plena e independiente al ambiente operativo, arquitectura del computador, navegador, etc., en el presente trabajo se evaluarán los aspectos relativos a la calidad servicios *QoS* y compatibilidad de los elementos que componen la VPN de extremo a extremo, es decir la vía que se demarcará entre la DMZ de Fundelec y los usuarios remotos.

Para ilustrar de manera general el alcance del proyecto a continuación se presenta el esquema general de la Red Privada Virtual a implementarse en FUNDELEC

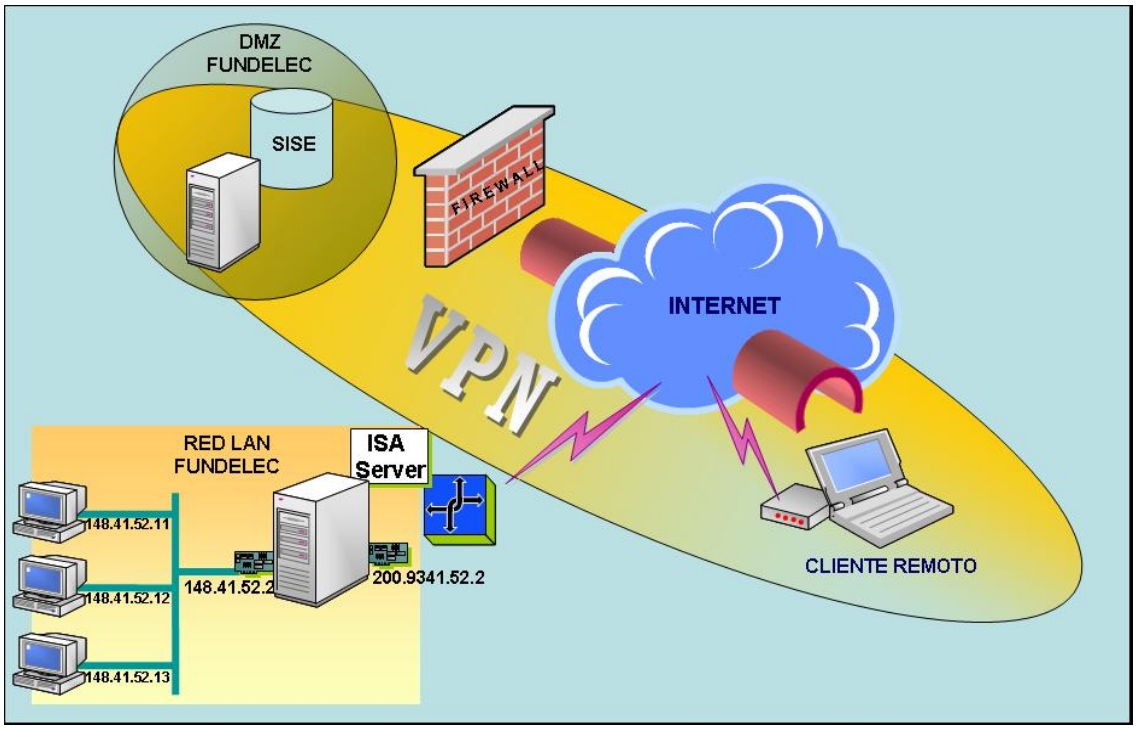


Figura 1. Esquema general de la Red Privada Virtual a implementarse en FUNDELEC

2.- Marco Referencial

2.1.- Antecedentes de la Investigación

La Fundación para el Desarrollo del Servicio Eléctrico "FUNDELEC", con el objeto de establecer un mecanismo de intercambio de la información necesaria y requerida para el control, regulación y supervisión del Sector Eléctrico Venezolano, ha dispuesto al personal de la organización de una dirección electrónica ó “Correo Electrónico”, lo cual facilita y acelera dicho fluido de información.

Tal implantación tuvo lugar en el año 1.999 donde su impacto y aporte fue determinante en término de reducir el tiempo de entrega y corrección de la información solicitada a las empresas eléctricas en ocasión del desarrollo del estudio de Pliegos Tarifarios 2.000 – 2.004.

Asimismo, con el desarrollo del Sistema de Información del Sector Eléctrico (SISE) en el año 2.002, el cual prevé consolidar una gran base de datos ó repositorio de información, se establece un único punto de entrada a través del uso de una dirección electrónica (sise@fundelec.org.ve) para la recepción de la información suministrada por las empresas eléctricas y posterior actualización de la base de datos en los distintos aspectos de la actividad eléctrica tales como: Características del Parque Eléctrico, Generación, Transmisión, Substransmisión, Comercialización, entre otras.

Dicho repositorio de información estará disponible a los usuarios autorizados en la red local de FUNDELEC “Intranet”, a través de las herramientas de consultas y análisis en línea “OLAP” que incorpora el SISE.

Sin embargo, el ámbito de interés para la consulta y acceso a dicho sistema va mucho más allá de las fronteras de FUNDELEC, dado a que el personal técnico lo requiere tanto dentro como fuera de la localidad de la organización.

Asimismo, existe un conjunto de usuarios asociados al sector eléctrico Venezolano tales como: MEM, CAVEINEL, OPSIS, entre otros, con interés y necesidad de acceder y consultar al SISE, a los fines de cotejar, validar y obtener información de acuerdo a su actividad ó área de acción dentro del referido sector.

Por ello, la importancia de incorporar a la infraestructura tecnológica del SISE un componente que habilite y controle las conexiones remotas y que garantice la integridad, confiabilidad y estabilidad del sistema.

Por lo que, revisando la infraestructura del SISE el cual está adaptado a las tecnologías Web (http, https), dado a que sus interfaces de consultas fueron desarrolladas en páginas Web dinámicas (asp), y evaluando la plataforma para la conexión a Internet existentes en FUNDELEC, es previsible que el establecimiento de una “Red Privada Virtual” como mecanismo de acceso a los usuarios remoto al sistema.

Todo ello, sobre la base de consolidación y crecimiento que ha tenido lugar en la última década en los servicios, ancho de banda y disponibilidad de la Internet, lo cual facilita hoy día el establecimiento de una “Red Privada Virtual” sobre protocolo IP.

Por tanto, a continuación se revisarán los basamentos teóricos de dicha tecnología, así como, todos los aspectos y criterios necesarios para entender y aplicarla de manera efectiva.

2.2.- Bases Teóricas

En el marco tecnológico en el que tiene lugar una Red Privada Virtual existen diversos componentes y configuraciones posibles de acuerdo al escenario y necesidad que exista, por lo que, dichos conceptos se revisarán a continuación con el objeto de establecer las Bases Teóricas donde se soportará la presente investigación.

2.2.1.-Un Marco para Entender una Red Privada Virtual

Una Red Privada Virtual, mejor conocida por sus siglas "VPN", es una red que utiliza recursos de transmisión y conmutación compartidos, de una red pública tal como la Internet, ATM y/o Frame, para disponer a usuarios remotos los recursos y servicios disponibles en una red corporación, utilizando métodos de seguridad y protección para salvaguardar tanto la plataforma corporativa como los datos intercambiados.

La esencia de ésta tecnología reside en que esa parte 'pública' no será accesible por ningún usuario no autorizados, lo que la constituye en una red "privada virtual", dado a que no es una red privada real.

Una VPN posee ciertas ventajas sobre una red "privada real", tal como que ésta puede establecerse de manera más efectiva y expedita en términos económicos, y así incorporar en la red corporativa sitios remotos más pequeños, los teletrabajadores y el personal móvil. Los ahorros se estiman aproximadamente entre un 20% y 40% para la interconexión de las sedes principales con sus sucursales, y un 60% u 80% para la conexión de los usuarios móviles.

Otros Aspectos importantes que se deben considerar, son los aspectos técnicos que la corporación requiere para establecer una conexión punto a punto entre sus sucursales y los usuarios móviles:

- Solicitar e instalar líneas telefónicas o troncales E1 a los proveedores de servicio.
- Comprar, instalar y configurar equipos de acceso remoto, rack de módems, etc.
- Instalar en los equipos portátiles software capacitados para establecer la interconexión. Monitorear los patrones de tráfico sobre los puertos en los equipos de acceso remoto.
- Suplir suficientes puertos de acceso en relación con el número de personal móvil utilizando el servicio.
- Mantenerse actualizado con los cambios tecnológicos del mercado.

En los últimos años se ha observado una fuerte tendencia al desarrollo redes virtuales privadas utilizando Internet, ya que así se reducen aún más los costos de implementación y se alcanza la conectividad global. Por ello, se habla de *intranet*, donde se utilizan tecnologías de Internet a lo largo de la organización y de *extranet*, donde se extiende fuera de las fronteras de la organización el acceso a clientes, socios, proveedores, etc.

A continuación se presenta una figura que muestra el esquema de conexión de una VPN a utilizando una linea dedicada Vs la implementación que utiliza la Internet.

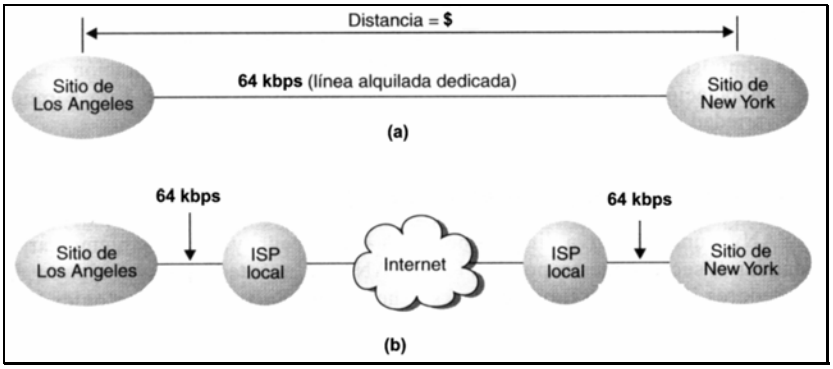


Figura 2. Comparación de Interconexión de una VPN

Como se observa en la gráfica anterior, utilizando líneas dedicada para el establecimiento de una VPN (a) existen las siguientes consideraciones:

- El costo de la linea dedicada depende de la distancia entre ambos extremos.
- El usuario cancela el costo total de la linea, a pesar de no haberla utilizado el 100%.
- Para cada nueva conexión (usuario) a la VPN debe contratarse una línea dedicada.

Asimismo se observa en la gráfica anterior, utilizando la Internet para establecer una VPN (b) existen los siguientes beneficios:

- El costo de conexión y establecimiento de la VPN no está asociado a la distancia entre los extremos.
- El usuario sólo cancela el costo necesario de conexión para el establecimiento de la VPN.
- Cada nueva conexión (usuario) a la VPN puede efectuarse sólo si dicho usuario dispone del acceso a Internet y los programas de seguridad y autenticación.

Los requisitos para establecer una VPN basadas en Internet se pueden agrupar en cinco áreas principales: compatibilidad, seguridad, disponibilidad e interoperabilidad.

a) Compatibilidad

Para establecer una VPN sobre Internet, debe ser compatible con el protocolo de Internet (IP). Resulta obvia esta consideración con el fin de poder asignar y, posteriormente, utilizar conjuntos de direcciones IP. Sin embargo, la mayoría de redes privadas emplean direcciones IP privadas o no-oficiales, provocando que únicamente unas pocas puedan ser empleadas en la interacción con Internet. La razón por la que sucede esto es simple: la

obtención de un bloque de direcciones IP oficiales suficientemente grande como para facilitar un *subnetting* resulta imposible. Las subredes simplifican la administración de direcciones así como la gestión de los routers y conmutadores, pero se desaprovechan direcciones muy preciadas.

Actualmente existen varias técnicas con las que poder obtener la compatibilidad deseada entre las redes privadas e Internet, por ejemplo la conversión a direcciones Internet mediante NAT (*Network Address Traslation*) y el empleo de túneles para encapsulamiento.

En la primera de estas técnicas, las direcciones Internet oficiales coexistirán con las redes IP privadas en el interior de la infraestructura de routers y conmutadores de las organizaciones. De este modo, un usuario con una dirección IP privada puede acceder al exterior por medio de un servidor de direcciones IP oficiales mediante la infraestructura local y sin necesidad de emplear ningún tipo de acción especial.

Con el túnel, la fuente encapsula los paquetes pertenecientes a otro protocolo en datagramas IP con el fin de poder atravesar la infraestructura de Internet. El proceso de encapsulación está basado en la adición de una cabecera IP al datagrama original, el cual representa la carga (*payload*). En el extremo remoto, el receptor desencapsula el datagrama IP (eliminando la cabecera IP) y entrega el datagrama original intacto. El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación.

El túnel envuelve, o encapsula, el paquete original dentro de un paquete nuevo. Este paquete nuevo puede contener nueva información de direccionamiento y enrutamiento, lo que le permite viajar por la red. Si el túnel se combina con la confidencialidad de datos, los datos del paquete original (así como el origen y el destino originales) no se muestran a quienes capturen el tráfico. La red puede ser cualquier conjunto de redes: una intranet privada o Internet. Cuando los paquetes encapsulados llegan a su destino, se quita la encapsulación y se utiliza el encabezado original del paquete para enrutar éste a su destino final.

El túnel es la ruta de información lógica a través de la cual viajan los paquetes encapsulados. Para los interlocutores de origen y de destino originales, el túnel suele ser transparente y aparece simplemente como otra conexión punto a punto en la ruta de acceso a la red. Los interlocutores desconocen los enrutadores, interruptores, servidores proxy u otras puertas de enlace de seguridad que pueda haber entre los extremos del túnel. Cuando el uso de túneles se combina con la confidencialidad de los datos, puede utilizarse para proporcionar redes privadas virtuales (VPN).

b) Seguridad

Es un aspecto de séria consideración cuando se implementa una Red Privada Virtual utilizando como canal de comunicación la Internet. Las comunicaciones ya no van a estar confinadas a circuitos privados, sino que van a viajar a través de Internet, que es considerada una red "demasiado pública" para realizar comunicaciones privadas. Aunque puede parecer poco probable que alguien monitoreando una línea con un sniffer[1] consiga capturar información y hacer uso de ella, la posibilidad existe, sin embargo y aplicando las correspondientes medidas de protección y seguridad, Internet puede convertirse en una red altamente privada y segura.

Para eso la encriptación es muy importante. Cuando la información está encriptada, se requiere una clave para desencriptarla. Los usuarios en cada extremo deben tener las claves adecuadas para encriptar y desencriptar los datos. Si se está configurando una conexión con una sucursal es fácil administrar este intercambio de claves. Sin embargo, si un usuario remoto accede a la red corporativa, se necesita un modo de verificar quién es (Identificación y Autenticación) y un modo de intercambiar las claves para la encriptación.

Las claves públicas basadas en certificados digitales son los que más de utilizan para este propósito.

[1] Instrumento utilizado para capturar tramas de información (paquetes) para uso ilícito

c) Disponibilidad

La disponibilidad viene motivada principalmente por dos variables: una accesibilidad plena e independiente del momento y del lugar, y un rendimiento óptimo que garantice la calidad de servicio ofrecida al usuario final.

La calidad de servicio (*QoS – Quality of Service*) hace referencia a la capacidad que dispone una red para asegurar un cierto grado de operación de extremo a extremo. La QoS puede venir dada como una cierta cantidad de ancho de banda o un retardo que no debe sobrepasarse, o bien como una combinación de ambas.

Actualmente, la entrega de datos en Internet es realizada de acuerdo al mejor esfuerzo (*best effort*), lo cual no garantiza la calidad de servicio demandada. No obstante y en un breve espacio de pocos años, Internet será capaz de suplir esta carencia ofreciendo un soporte para la QoS a través de un conjunto de protocolos emergentes entre los que cabe destacar DiffServ (*Differential Services*), RSVP (*Resource ReSerVation Protocol*) y RTP (*Real Time Protocol*). Pero por ahora, los proveedores sólo proporcionan la QoS de las VPNs haciendo uso del tráfico CIR (*Committed Information Rate*) en Frame Relay u otras técnicas.

d) Interoperabilidad

Las implementaciones de los tres primeros requisitos han provocado la aparición de un cuarto: la interoperabilidad. Los estándares sobre tunneling, autenticación, encriptación y modo de operación ya mencionados anteriormente son de reciente aparición o bien se encuentran en proceso de desarrollo. Por esta razón, previamente a la adquisición de una tecnología VPN, se debe prestar una cuidadosa atención a la interoperabilidad de extremo a extremo. Esta responsabilidad puede residir tanto en el usuario final como en el proveedor de red, dependiendo de la implementación deseada.

Una manera de asegurar una correcta interoperabilidad radica en la elección de una solución completa ofrecida por un mismo fabricante. En el caso de que dicho fabricante no sea capaz de satisfacer todos los requisitos, se deberán limitar los aspectos interoperacionales a un subconjunto que englobe aquellos que sean esenciales, además de utilizar únicamente aquel equipamiento que haya sido probado en laboratorios o bien sometido a pruebas.

En cualquiera de los casos, se deberán seleccionar fabricantes que se acoplen totalmente a los estándares VPN y adquirir únicamente aquel equipamiento que pueda ser actualizado tanto mediante software, firmware o módulos plug-in, con el fin de que puedan adecuarse a futuros estándares.

Una vez vista la relevancia que presentan estas cuatro áreas para las VPN, se procederá a realizar una breve descripción de los principales protocolos disponibles, los cuales permiten alcanzar en general unos resultados satisfactorios, principalmente en las áreas de seguridad y compatibilidad.

2.2.2.-**C**omponentes de una **R**ed **P**rivada **V**irtual

La efectividad y confiabilidad en la implantación de una Red Privada Virtual viene determinada por los siguientes componentes:

a) Firewall (Corta Fuego)

Un Firewall es un importante componente de seguridad para cualquier usuario que utilice la Internet. Se encuentra disponible en el mercado mediante productos de Hardware y Software, y evita que usuarios no autorizados envien ó reciban datos a una red corporativa conectada a Internet, mediante el uso de reglas de acceso, permitiendo ó rechazando comunicaciones desde subredes y/o direcciones específicas a traves de ciertos protocolos.

Sin embargo un Firewall no protege por sí mismo la red corporativo de las amenazas de ataque presente en la Internet, dado que información importante como: a)nombres de usuarios; b) contraseñas; direcciones de servidores, entre otros, son visibles para los *hackers*. Por lo que en una VPN se habilita un tunel privado, a través del uso de algoritmos de encriptamiento, lo que posibilita el uso de un medio público y compartido como la Internet para transmisión de datos seguros.

b) Tunel

Es el componente que permite que una Red Privada Virtual sea "Virtualmente Privada". A pesar que éste se establezca a través de un medio público éste no se establece sobre la Internet, éste se establece directamente desde una sucursal hasta una red corporativa privada. A pesar que el término "Tunel" describe una ruta predeterminada sobre la Internet, éste no es el caso. Al igual que cualquier tráfico que cursa en la web los paquetes de un tunel VPN debe tomar varias rutas en su trayecto entre los dos extremos.

El componente tunel en una VPN se confiere al hecho de que sólo el transmisor y el destinatario puedan ver y entender los algoritmos de encriptamiento y así tener acceso a los datos del paquete.

La tecnología de Tunel ó *tunneling* encripta y encapsula su propio protocolos de red dentro del protocolo (IP), permitiendo de esta manera enrutar, conmutar, habilitar filtros y desarrollar filtros para el control de costos, de igual manera como se emplean en los enlaces WAN tradicionales. Por ello no es sólo la transmisión de VPN transparente a los usuarios, sino que es virtualmente transparente a las operaciones de administración de la propia red corporativa.

c) Encriptamiento

Un criptosistema o sistema de cifrado es un método de alterar mensajes de tal forma que sólo personas que conozcan esa alteración, puedan conocer el mensaje de origen. Criptografía es el arte de crear criptosistemas. Criptoanálisis es el arte de romper criptosistemas, es decir ver el mensaje original a través de las modificaciones aplicadas sobre este sin ser la persona receptora del mensaje.

El mensaje original es conocido como "texto puro" o “texto en claro” y el mensaje modificado se conoce como "texto cifrado". Encriptar es el proceso de crear "texto cifrado" a partir de "texto puro". Desencriptar es crear, por medio de cualquier proceso, "texto puro" a partir de "texto cifrado"

Un criptosistema está compuesto normalmente por una colección de algoritmos.

La teconólgia VPN apoyada en las técnicas de criptogría, encripta la información de la siguiente forma: en ambos extremos del tunel VPN se coloca un *Gateway* ó traductor en hardware ó software, en el extremo trasmisor dicho gateway encripta la información dentro de un “Cipher-Text” antes de enviar la información encriptada a través de la Internet. El gateway receptor restaura la información encriptada a un “Clear-Text”.

En el nacimiento de la tecnología VPN las compañias mantenían en secreto los algoritmos de encriptamiento, sin embargo, éstos fueron descubiertos y utilizados por los hackers, por lo que toda la información que viajaba encriptada con dichos algoritmos se convirtió vulnerable. Por lo que, la industria comenzó a publicar el mejor algoritmo conocido y probado, como el Data Encryption Standart (DES), dado a que el componente seguro a partir de ese momento pasó a ser la clave.

El Estandar de Encriptaminto de Datos “La Data Encryption Standard” (DES) utiliza claves simétrica de 56-bit para encriptar datos en bloques de

64-bit. La clave de 56 bit provee 72,057,594,037,927,900 combinaciones posibles, Lo que pareciera ser lo suficientemente robusto dado que tomaría cerca de 20 años para descifrarlo, sin embargo, la organización de piratas en la Internet “Hackers” lo ha vulnerado en tan sólo 12 segundos.

DES ha venido desarrollando desde entonces el algoritmo 3DES (“Triple-DES”) sistema que encripta la información multiple veces.

Criptografía Simétrica

En un criptosistema clásico, tenemos el mensaje P (de plaintext en inglés), una función de encriptación E(k) y una función de desencriptación D(k) que utilizan una clave k de tal forma que:

$$D(k)\,[E(k)\,[P]\,] = P$$

Es la forma más clásica de criptografía. Con este tipo de criptografía A y B comparten una clave secreta k que utilizan para encriptar y desencriptar mensajes. Esto requiere un acuerdo previo entre A y B mediante un canal seguro para acordar y comunicar dicha clave secreta.

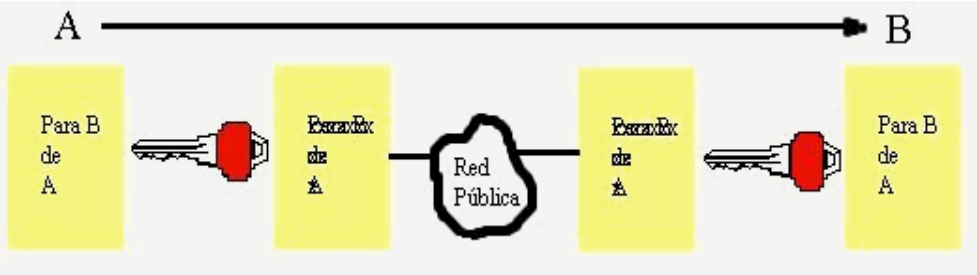


Figura 10. Esquema general de Criptografía Simétrica

Existen sistemas para comunicarse de forma segura a través de redes públicas usando claves simétricas; el más notable es Kerberos. Sin embargo estos sistemas no soportan bien comunidades grandes de

usuarios, pierden seguridad y necesitan de medidas extras, como almacenar la clave simétrica en un servidor seguro centralizado.

Criptografía Asimétrica ó Claves Pública

En contraste con la criptografía simétrica, la criptografía de clave pública es relativamente joven. Fue concebida por Diffie and Hellman en 1976 y en 1977 Rivest, Shamir y Adelman inventaron el criptosistema RSA, la primera realización de un sistema de clave pública.

Siguiendo la nomenclatura de la clave simétrica anterior diríamos que:

$$D(k')\ [E(k)\ [P]\ ] = P$$

La criptografía de clave pública se basa en la utilización de dos claves k y k', en contraste con la criptografía simétrica que sólo utiliza k. La particularidad del sistema de encriptación de clave pública se fundamenta en la relación entre estas dos claves. El resultado de encriptar un texto con una de las claves sólo es recuperable desencriptando con su pareja y viceversa. Una de las claves la guarda el usuario manteniéndola en 0secreto (clave privada) y distribuye libremente la otra (clave pública).

La propiedad básica de un sistema de encriptación de clave pública es que dada una clave de encriptación k es técnicamente imposible calcular la clave de desencriptación k'. Esta propiedad permite a B públicar su clave k. Cualquiera puede utilizar esta clave para encriptar un mensaje que sólo la clave privada k' de B puede desencriptar. Decimos así que B posee el par de claves.

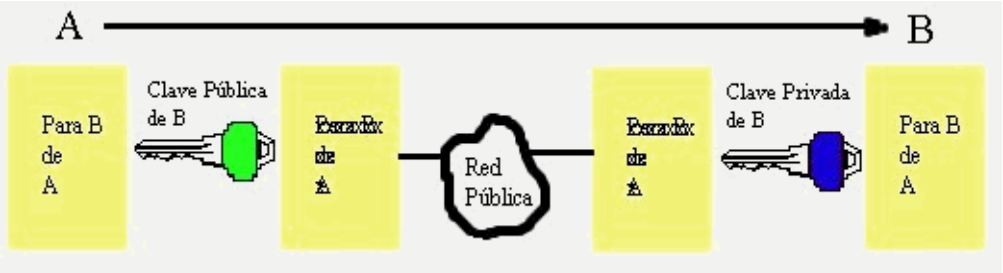


Figura 11. Esquema general de Criptografía Asimétrica

El proceso para encriptar un mensaje con un sistema de clave pública es computacionalmente mucho más pesado que hacer lo mismo con un sistema de clave simétrica. Esto ha llevado a que en la práctica el proceso de encriptación se realice mediante una clave simétrica y después encriptar la propia clave simétrica con un sistema de clave pública como RSA. Así decimos que el sistema de clave pública transporta la llave simétrica.

Ya que la clave simétrica K es más corta que el mensaje a encriptar, esta técnica resulta significantemente más rápida que hacer lo mismo con un sistema de clave pública.

$$D(k') [E(k) [K]] = K$$

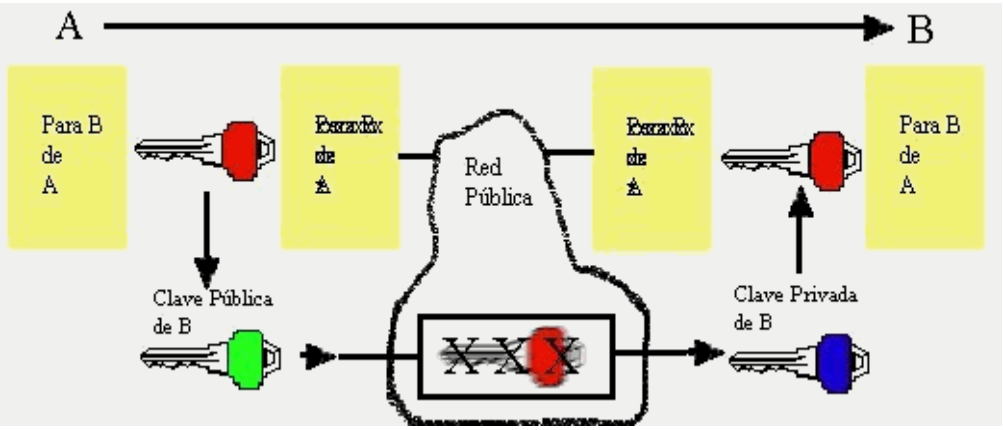


Figura 12. Esquema detallado de Criptografía Asimétrica

d) Autenticación

Por autenticación se entiende cualquier método que permita comprobar de manera segura alguna característica sobre un objeto. Dicha característica puede ser su origen, su integridad, su identidad, etc. A continuación se consideran tres grandes tipos dentro de los métodos de autenticación:

Autenticación de mensaje. Es aquel donde se desea garantizar la procedencia de un mensaje conocido, de forma que podamos asegurarnos de que no es una falsicación. Este mecanismo se conoce habitualmente como firrma digital.

Autenticación de usuario mediante contraseña. En este caso se trata de garantizar la presencia de un usuario legal en el sistema. El usuario debería poseer una contraseña secreta que le permita identificarse.

Este sistema de autenticación basa su funcionamiento en una información secreta conocida únicamente por el usuario, que le permite identificarse positivamente frente al sistema. Supondremosque el usuario se encuentra en un terminal seguro, es ecir, libre de posibles ataques del exterior. Distinguiremos entonces dos casos claramente diferenciados:

a) El sistema se comunica con el usuario, pero éste no puede entrar en él. El usuario carece de acceso a los archivos del sistema y no tiene posibilidad ejecutar aplicaciones en él, únicamente puede llevar a cabo una serie de operaciones muy restringidas.

b) El sistema permite al usuario entrar. Este es el caso de los sistemas operativos como UNIX, que ofrecen la posibilidad a los usuarios operar con el sistema desde terminales remotos. Normalmente el usuario tiene acceso más o menos restringido a los archivos del sistema y puede ejecutar programas.

Autenticación de dispositivo. Se trata de garantizar la presencia de un dispositivo válido. Este dispositivo puede estar solo o tratarse de una llave electrónica que sustituye a la contraseña para identificar a un usuario.

Cabe destacar que la autenticación de usuario por medio de alguna característica biométrica, como pueden ser las huellas digitales, la retina, el iris, la voz, etc. puede reducirse a un problema de autenticación de dispositivo, solo que el dispositivo en este caso es el propio usuario.

Los algoritmos MAC pueden ser empleados para autenticar dispositivos, siempre que éstos permitan llevar a cabo las operaciones adecuadas en su interior, a la vez que impiden acceder físicamente a la clave que llevan almacenada.

Un ejemplo de este mecanismo de autenticación lo tenemos en las tarjetas SIM que emplean los teléfonos celulares GSM. Dichas tarjetas llevan implementado un algoritmo MAC, denominado $COMP128_2$, que genera un valor a partir del mensaje y una clave k almacenada en un lugar de la memoria que no se puede leer desde el exterior. En cada tarjeta se graba una única clave, de la que se guarda una copia en lugar seguro. Si la compañía quiere identificar una tarjeta simplemente genera un bloque de bits aleatorio X y calcula su resumen $E_k(X)$ asociado. Posteriormente se envía X a la tarjeta para que realice el mismo cálculo y devuelva su propio resultado. Si ambos coinciden, la tarjeta será considerada auténtica. Esta técnica se conoce como autenticación por desafío.

Firmas Digitales Funciones Resumen

Mediante la aplicación de criptografía asimétrica se permite autentificar información, es decir, puede asegurar que un mensaje *m* proviene de un emisor A y no de cualquier otro.

En general, las funciones resumen se basan en la idea de funciones de compresión, que dan como resultado bloques de longitud *n* a partir de bloques de longitud *m*. Estas funciones se encadenan de forma iterativa,

haciendo que la entrada en el paso *i* sea función del i-ésimo bloque del mensaje y de la salida del paso *i*. En general, se suele incluir en alguno de los bloques del mensaje *m*, información sobre la longitud total del mensaje. De esta forma se reducen las probabilidades de que dos mensajes con diferentes longitudes den el mismo valor en su resumen.

e) Protocolos

PPTP (Point-to-Point Tunneling Protocol): Es un protocolo de red creado por Microsoft que permite la realización de transferencias seguras desde clientes remotos a servidores emplazados en redes privadas, empleando para ello tanto líneas telefónicas conmutadas como Internet.

En el escenario típico de PPTP, el cliente establecerá una conexión a través de una linea telefónica ***dial-up*** con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP.

Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos del cliente externo y transmitiéndolos al correspondiente destino en la red privada.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido. PPTP soporta los protocolos de red IP, IPX, y NetBEUI. Se utiliza una versión modificada del Generic Routing Encapsulation (GRE) para encapsular los paquetes PPP como datos para el túnel, de forma que estos puedan viajar cifrados y comprimidos.

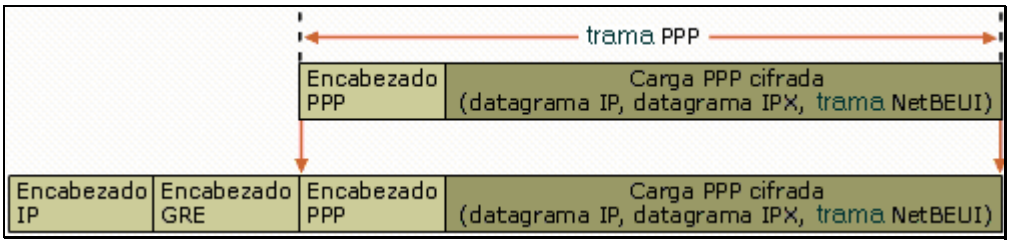


Figura 3. Estructura de un paquete PPTP

L2F (Layer 2 Forwarding): Desarrollado por Cisco Systems, tiene como objetivo proporcionar un mecanismo de tunneling para el transporte de tramas a nivel de enlace (HDLC, PPP, SLIP, etc.). El proceso de tunneling involucra tres protocolos diferentes: Protocolo pasajero, protocolo encapsulador, y protocolo portador.

El protocolo pasajero representa el protocolo de nivel superior que debe encapsularse (PPP, SLIP, etc). A continuación, el protocolo encapsulador indica el protocolo que será empleado para la creación, mantenimiento y destrucción del túnel de comunicación. En este caso, el protocolo encapsulador será L2F. Por último, el protocolo portador será el encargado de realizar el transporte de todo el conjunto.

Por lo general, este protocolo suele ser IP, dadas sus capacidades de enrutamiento, su acople a los diferentes medios y su estandarización dentro del ámbito de Internet.

Entre las principales ventajas que ofrece el protocolo L2F, cabe destacar el soporte multiprotocolo, la multiplexación de múltiples sesiones remotas (minimizando el número de túneles abiertos en un momento dado), y la gestión dinámica de los túneles, en la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario. Además, por cada túnel L2F establecido, el proceso de seguridad genera una clave aleatoria como medida de prevención ante posibles ataques basados en falsificación de la fuente (*spoofing*). A su vez, en el interior de los túneles, cada una de las sesiones

multiplexadas mantiene un número de secuencia para evitar problemas debidos a la duplicidad de paquetes.

L2TP (Layer 2 Tunneling Protocol): Este protocolo de túnel de capa 2 es el resultado de la combinación de los protocolos L2F y PPTP. Permite la creación de túneles a través de una gran variedad de tipos de redes (IP, SONET, ATM) para el transporte de tráfico PPP.

Los túneles L2TP pueden llevarse a cabo tanto en redes públicas IP como en redes privadas. Esto provoca que tanto los paquetes de control como los paquetes de datos sean vulnerables frente a posibles ataques como *snooping,* negación de servicio, modificaciones, o incluso interceptación de los procesos de negociación de la encriptación (ECP) y de la compresión (CCP) con el fin de provocar la supresión de los mecanismos de confidencialidad o en su caso, obtener el acceso a las contraseñas de los usuarios.

Para evitar todas estas posibles situaciones, el protocolo de seguridad debe proporcionar autenticación así como mecanismos para asegurar la integridad y la protección de los paquetes de control, además de la confidencialidad de todos los paquetes. Para poder alcanzar este nivel, es que usualmente se utiliza L2TP conjuntamente con IPSec.

SSL (Secure Socket Layer): La Capa de conectores seguros es un protocolo que suministra un canal seguro. Con SSL, el cliente y el servidor utilizan una cierta técnica para acordar el nivel de seguridad que quieren usar durante la sesión. La identificación ocurre sobre un canal seguro y toda la información se transmite sobre las sesiones encriptadas.

SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 o IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de

sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 o SHA se pueden usar como algoritmos de resumen digital (hash). Esta posibilidad de elegir entre tan amplia variedad de algoritmos dota a SSL de una gran flexibilidad criptográfica.

Durante el protocolo SSL, el cliente y el servidor intercambian una serie de mensajes para negociar las características de seguridad. Este protocolo sigue las siguientes fases (de manera muy resumida):

La fase *Hola*, usada para ponerse de acuerdo sobre el conjunto de algoritmos para mantener la confidencialidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles. Normalmente se utilizarán los más fuertes que se puedan acordar entre las dos partes. En función de las posibilidades criptográficas del navegador, el servidor elegirá un conjunto u otro de algoritmos con una cierta longitud de claves.

La fase de *autenticación*, en la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3 (sólo si la aplicación exige la autenticación de cliente).

La fase de *creación de clave*, en la que el cliente envía al servidor una clave de sesión a partir de la cual ambos extremos cifrarán los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado previamente. El navegador envía cifrada esta clave usando la clave pública del servidor, que extrajo de su certificado.

Por último, la fase *Fin*, en la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente

establecido. Una vez finalizada esta fase, ya se puede comenzar la sesión segura.

De ahí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores) a través del cual se intercambiará cifrada la información relevante, como el URL y los contenidos del documento solicitado, los contenidos de cualquier formulario enviado desde el navegador, las cookies enviadas desde el navegador al servidor y viceversa y los contenidos de las cabeceras HTTP.

IPSec (IP Secure): Representa un conjunto de mecanismos de seguridad de alta calidad basado en claves criptográficas. Proporciona un canal seguro para los datos a través de la red, ofreciendo para ello un control de acceso, así como una integridad en los datos transmitidos, además de mecanismos de autenticación y confidencialidad. IPSec opera sobre la capa 3 de red.

Los servicios IPSec son llevados a cabo mediante el uso de dos protocolos de seguridad: *Authentication Header (AH)* y *Encapsulating Security Protocol (ESP)*, así como mediante un conjunto de protocolos necesarios para la gestión de claves criptográficas, llamado IKE (*Internet Key Exchange*).

El protocolo AH proporciona únicamente mecanismos de autenticación. Los datos de autenticación AH son insertados entre el encabezado IP y los datos referentes al paquete de nivel superior (TCP, UDP, ICMP), tal como se muestra en la siguiente figura.

Figura 4. Un paquete IPSec con el encabezado AH

ESP ofrece confidencialidad (además de proporcionar autenticación, integridad y protección contra réplica) para la carga IP. ESP hace uso de una amplia variedad de algoritmos de encriptación entre los cuales cabe destacar DES, 3DES, CAST128 y *Blowfish*. Por ejemplo, Alicia en el equipo A envía datos a Bernardo en el equipo B. La carga IP está cifrada y firmada para garantizar su integridad. Al recibirse, una vez completado el proceso de comprobación de la integridad, se descifra la carga de datos del paquete. Bernardo puede estar seguro de que fue Alicia quien le envió la información, de que la información no ha sufrido cambios y de que nadie más ha podido leerla.

ESP se identifica en el encabezado IP con el Id. de protocolo IP 50. Como se muestra en la figura siguiente, el encabezado ESP se coloca delante de la carga IP, y tras ella se incluye un finalizador ESP y un finalizador de autenticación ESP.

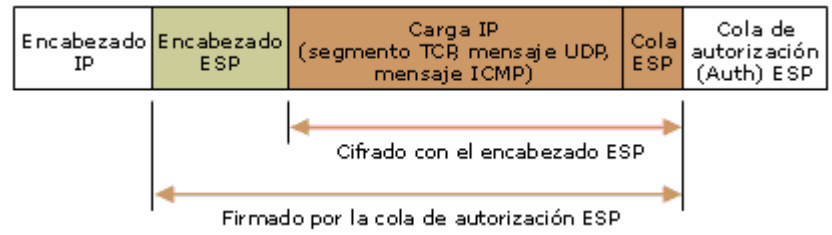


Figura 5. Un paquete IPSec com el encabezado y cola ESP

La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué información del mismo está protegida por confidencialidad. El encabezado IP no se firma y no está necesariamente protegido frente a modificaciones. Para proporcionar integridad de datos y autenticación al encabezado IP, puede utilizarse ESP conjuntamente con AH.

El encabezado ESP contiene los campos siguientes:

1.-Índice de parámetros de seguridad: Identifica la asociación de seguridad correcta para la comunicación cuando se utiliza junto con la dirección de destino y el protocolo de seguridad (AH o ESP). El receptor

utiliza este valor para determinar la asociación de seguridad con la que se debe identificar este paquete.

2.-Número de secuencia: Proporciona protección contra la réplica del paquete. El número de secuencia es un número de 32 bits que aumenta de forma incremental (a partir de 1) e indica el número de paquetes enviados a través de la asociación de seguridad de modo rápido para una comunicación dada. El número de secuencia no se puede repetir mientras perdure la asociación de seguridad de modo rápido. El receptor comprueba este campo para asegurarse de que no ha recibido ya un paquete para una asociación de seguridad con este número. Si se recibió alguno, se rechazará este paquete.

La cola ESP contiene los campos siguientes:

1.-Relleno: Es un valor entre 0 y 255 bytes y asegura que la carga cifrada junto con los bytes de relleno se ajuste a los límites de bytes que requieren los algoritmos de cifrado.

2.-Longitud de relleno: Indica la longitud en bytes del campo Relleno. El receptor utiliza este campo para quitar los bytes de relleno una vez descifrada la carga cifrada que los contiene.

3.-Siguiente encabezado: Identifica el tipo de datos de la carga, por ejemplo TCP o UDP.

La cola de autenticación ESP contiene el valor de comprobación de integridad (ICV), también conocido como código de autenticación de mensaje, que se utiliza para comprobar la autenticación del mensaje y su integridad. El receptor calcula el valor de ICV y lo compara con este valor (calculado por el remitente) para comprobar la integridad. El ICV se calcula para el encabezado ESP, los datos de la carga y el finalizador ESP.

El protocolo IPSec que acabamos de describir se conoce como el modo transporte . Existe también el modo túnel, donde se añade una nueva cabecera IP que puede contener direcciones distintas, tales como las direcciones de los firewalls. La cabecera IP interna transporta las direcciones fuente y destino.

El modo túnel protege los paquetes IP completos, pues los trata como una carga AH o ESP. Todo el paquete IP se encapsula con un encabezado AH o ESP y un encabezado IP adicional. Las direcciones IP del encabezado IP externo son los extremos del túnel, y las direcciones IP del encabezado IP encapsulado son las direcciones últimas de origen y de destino.

Como se muestra en la siguiente figura, el modo de túnel AH encapsula un paquete IP con un encabezado AH e IP y firma todo el paquete para asegurar su integridad y autenticación.

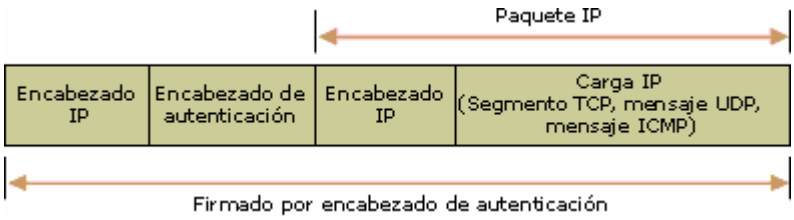


Figura 6. Un datagrama IPSec-AH en modo túnel

El modo túnel ESP encapsula un paquete IP con un encabezado ESP e IP y un finalizador de autenticación ESP. La parte firmada del paquete indica dónde se firmó el paquete para confirmar su integridad y autenticación. La parte cifrada del paquete indica qué información del mismo está protegida por confidencialidad.

Debido al nuevo encabezado agregado al paquete para el túnel, todo lo que sigue al encabezado ESP está firmado (excepto el finalizador de autenticación ESP), ya que ahora se encuentra encapsulado en el paquete enviado por el túnel.

El encabezado original se coloca después del encabezado ESP. El paquete entero se anexará con un finalizador ESP antes del cifrado. Todo lo que sigue al encabezado ESP, salvo el finalizador de autenticación ESP, se cifra.

Esto incluye el encabezado original, que ahora se considera parte de los datos del paquete.

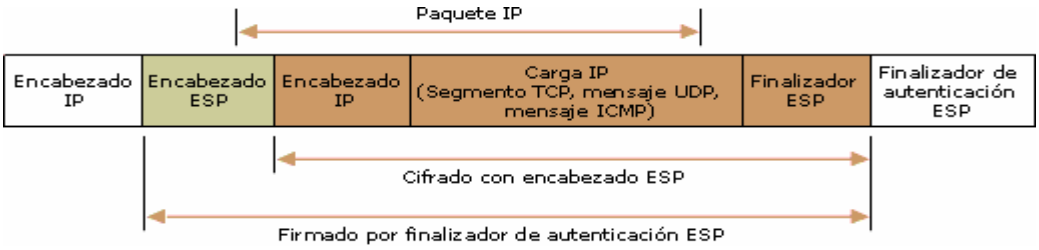


Figura 7. Un paquete IPSec-ESP en modo túnel

Toda la carga ESP se encapsula dentro del nuevo encabezado de túnel, el cual no se cifra. La información del nuevo encabezado de túnel sólo se utiliza para enrutar el paquete desde el origen hasta el destino. Si el paquete se envía a través de una red pública, se enrutará hacia la dirección IP del servidor de túnel de la intranet receptora.

En la mayoría de los casos, el paquete irá destinado a un equipo de una intranet. El servidor de túnel descifra el paquete, descarta el encabezado ESP y utiliza el encabezado IP original para enrutar el paquete hacia el equipo de la intranet.

ESP y AH pueden combinarse al utilizar túneles para lograr tanto la confidencialidad del paquete IP enviado por el túnel como la integridad y la autenticación de todo el paquete.

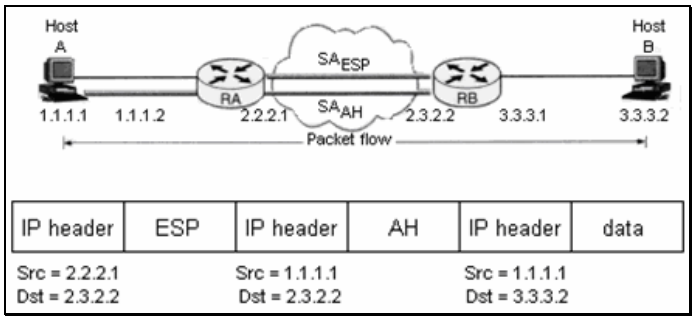


Figura 8. Combinación de ESP y AH

Los túneles IPSec se utilizan principalmente para la interoperabilidad con otros enrutadores, puertas de enlace o sistemas finales que no admiten conexiones L2TP/IPSec o PPTP.

El modo túnel de IPSec se admite como característica avanzada y sólo se utiliza en túneles entre puertas de enlace (también conocidos como túneles entre enrutadores) y para configuraciones de servidor a servidor o de servidor a puerta de enlace. Los túneles IPSec no se admiten para casos de VPN de acceso remoto. Para las conexiones VPN de acceso remoto debe utilizarse L2TP/IPSec o PPTP.

f)IKE (Internet Key Exchange)

Antes de que se pueda intercambiar información protegida, debe establecerse un acuerdo de seguridad entre los dos equipos. En ese acuerdo de seguridad, denominado asociación de seguridad (SA), los dos equipos establecen el modo de intercambiar y proteger la información, como se muestra en la ilustración siguiente.

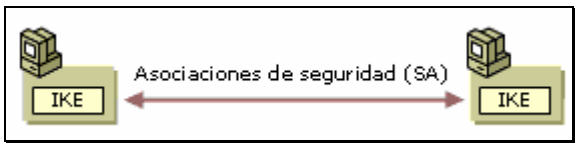


Figura 9. Concepto de la asociación de seguridad

Con el fin de establecer este acuerdo entre los dos equipos, IETF ha establecido un método estándar de asociación de seguridad y resolución de intercambio de claves denominado Intercambio de claves de Internet (IKE: *Internet Key Exchange*), que es una variante de ISAKMP/Oakley (*Internet Security Association and Key Management Protocol/Oakley Key Determination Protocol*). Este protocolo presenta tres características principales:

- Asegura que la comunicación IPSec y el intercambio de claves se lleve a cabo entre partes autenticadas.
- Negocia los protocolos, algoritmos, y claves que serán utilizados en la comunicación IPSec.
- Proporciona un método seguro para actualizar y renegociar asociaciones una vez que éstas han expirado.

Una asociación de seguridad (SA) es la combinación de una clave negociada, un protocolo de seguridad y el índice de parámetros de seguridad (SPI), que conjuntamente definen el método de seguridad utilizado para proteger la comunicación desde el remitente hasta el receptor. El SPI es un valor único e identificable de la SA utilizado para distinguir entre las múltiples asociaciones de seguridad que existen en el equipo receptor. Por ejemplo, pueden existir varias asociaciones si un equipo mantiene comunicaciones seguras con varios equipos a la vez.

Esta situación es habitual cuando el equipo es un servidor de archivos o un servidor de acceso remoto que atiende a varios clientes. En estos casos, el equipo receptor utiliza el SPI para determinar qué SA se utilizará para procesar los paquetes de entrada.

IKE funciona con dos fases. En la primera, los dos extremos crean una asociación bidireccional, estableciendo con ello un canal seguro entre ellos. Ya en la segunda fase, este canal será empleado para realizar la

negociación de las asociaciones IPSec. La confidencialidad y la autenticación se aseguran durante cada una de las fases mediante el uso del cifrado y los algoritmos de autenticación acordados entre los dos equipos durante las negociaciones de seguridad. Al estar las tareas divididas entre las dos fases se agiliza la creación de claves.

Los siguientes son brevemente los pasos de que constan las 2 fases de IKE.

Fase I o negociación de modo principal

1. Negociación de directivas: Los cuatro parámetros obligatorios siguientes se negocian como parte de la SA de modo principal son: Algoritmo de cifrado (DES o 3DES), algoritmo de integridad (MD5 o SHA1), Grupo Diffie-Hellman que se utilizará para el material base de generación de claves (768 bits, 1024 bits o 2048 bits), el método de autenticación (Kerberos V5, certificado o autenticación por claves compartidas previamente)

2. Intercambio Diffie-Hellman: Las claves reales no se intercambian en ningún momento. Sólo se intercambia la información básica que requiere el algoritmo de determinación de la clave Diffie-Hellman para generar la clave secreta compartida. Después de este intercambio, el servicio IKE de cada equipo genera la clave principal utilizada para proteger la autenticación.

3. Autenticación: Para impedir un ataque por usuario interpuesto, los equipos intentan autenticar el intercambio de claves Diffie-Hellman. Si se produce un error en la autenticación, no se continuará con la comunicación. Para autenticar las identidades se utiliza la clave principal junto con los algoritmos y métodos de negociación. Los algoritmos de hash y cifrado se aplican a toda la carga de identidad mediante las claves generadas a partir del intercambio Diffie-Hellman del segundo paso. La carga incluye el tipo de identidad (para autenticación), puerto y protocolo.

IPSec utiliza los siguientes tipos de identidad para autenticación: para autenticación de certificados, el nombre completo de certificado y el nombre general; para Kerberos V5 y autenticación por clave compartida previamente, direcciones IPv4, el nombre de dominio completo (FQDN) del equipo y FQDN para el usuario. La carga de identidad queda protegida frente a modificaciones e interpretaciones, independientemente del método de autenticación empleado.

El remitente presenta una oferta para establecer una posible asociación de seguridad con el receptor. El interlocutor de respuesta no puede modificar la oferta. En caso de que se modifique la oferta, el interlocutor inicial rechazará el mensaje del interlocutor que responde. El interlocutor que responde envía una respuesta para aceptar la oferta o bien una respuesta con alternativas.

Los mensajes enviados durante esta fase tienen un ciclo de reintento automático que se repite cinco veces. Si se recibe una respuesta antes de que termine el ciclo de reintento, comienza la negociación de SA estándar. Si la directiva IPSec lo permite, después de un intervalo breve comenzarán las comunicaciones no seguras. Si se inician comunicaciones no seguras, después de cinco minutos de tiempo de inactividad (durante el cual no se envían mensajes), la próxima vez que se envíen mensajes se intenta la negociación de comunicación segura. Si se envían mensajes continuamente, la comunicación sigue siendo no segura durante la duración establecida para la directiva de modo principal. Una vez transcurrido el tiempo de la directiva, se intenta efectuar una nueva negociación de comunicación segura.

No hay ningún límite preestablecido en cuanto al número de intercambios que pueden tener lugar. El número de SA que se pueden establecer sólo está limitado por los recursos del sistema. Al estimar el número de asociaciones de seguridad que pueden establecerse sin disminuir significativamente el rendimiento del equipo, tenga en cuenta la capacidad de procesamiento de la CPU y RAM del equipo, la duración de la

asociación de seguridad y la cantidad de tráfico que se envía a través de las asociaciones de seguridad.

Fase II o SA de modo rápido

1. Se negocia la directiva: Los equipos con IPSec intercambian la siguiente información para proteger la transferencia de datos: Protocolo IPSec (AH o ESP), algoritmo de hash para la integridad y autenticación (MD5 o SHA1), algoritmo para el cifrado, si se solicita (3DES o DES). Finalmente se llega a un acuerdo y se establecen dos SA. Una SA para la comunicación entrante y la otra para la comunicación saliente.

2. El material de clave de sesión se actualiza o se intercambia: IKE actualiza el material de generación claves, y se generan nuevas claves compartidas para la integridad de los datos, la autenticación y el cifrado (si se ha negociado). Si es necesario volver a generar las claves, se produce un segundo intercambio Diffie-Hellman (como se describe en la negociación de modo principal) o se actualiza la clave Diffie-Hellman original.

3. Las SA y las claves, junto con el SPI, se pasan al controlador de IPSec.

La segunda negociación de la configuración de seguridad y el material de claves (con el fin de proteger los datos) está protegida por la SA de modo principal. Mientras que la primera fase protege la identidad, la segunda fase proporciona protección mediante la actualización del material de las claves antes de enviar los datos. IKE puede dar cabida a una carga de intercambio de claves para realizar un intercambio Diffie-Hellman adicional si es necesario volver a generar las claves; es decir, si está habilitada la confidencialidad directa perfecta (PFS, Perfect Forward Secrecy) de clave de sesión. De lo contrario, IKE actualiza el material de las claves obtenido en el intercambio Diffie-Hellman del modo principal.

El modo rápido produce un par de asociaciones de seguridad, cada una de ellas con su propio SPI y su clave. Una SA se utiliza para la comunicación entrante y la otra para la comunicación saliente.

El uso de una única SA de modo principal para varias negociaciones de SA de modo rápido aumenta la velocidad del proceso. Mientras la SA de modo principal no caduque, no es necesario volver a negociar o a autenticar. El número de negociaciones de SA de modo rápido que pueden realizarse viene determinado por la configuración de la directiva IPSec.

La SA de modo principal se almacena en caché para permitir múltiples negociaciones de SA de modo rápido (salvo en el caso de que esté habilitada PFS de clave de sesión). Cuando se llega a una cierta duración de la clave principal o de sesión, se vuelve a negociar la SA. Además, la clave se actualiza o se vuelve a generar.

Cuando transcurre el periodo predeterminado de tiempo de espera para la SA de modo principal, o cuando se alcanza la duración de la clave principal o de sesión, se envía un mensaje de eliminación al interlocutor que responde. El mensaje de eliminación de IKE indica al interlocutor que responde que la SA de modo principal ha caducado. De este modo se impide la creación de nuevas SA de modo rápido a partir de la SA de modo principal caducada. IKE no hace caducar la SA de modo rápido, ya que sólo el controlador de IPSec contiene el número de segundos o bytes que han transcurrido hasta alcanzar la duración.

Es necesario tener precaución al establecer duraciones muy diferentes para las claves principales y de sesión. Por ejemplo, si se establece una duración de clave principal de ocho horas y una duración de clave de sesión de dos horas, una SA de modo rápido podría continuar establecida casi dos horas después de que la SA de modo principal hubiera caducado. Esta situación se produciría cuando la SA de modo rápido se generara poco antes de caducar la SA de modo principal.

Generalmente se recomienda mantener la configuración predeterminada de IKE (por ejemplo, PFS de clave principal y duración de claves) y los métodos de seguridad predeterminados para evitar una sobrecarga administrativa. De esta manera se proporciona un nivel estándar (medio) de seguridad. Si su planeamiento requiere un nivel de seguridad más alto, puede considerar la posibilidad de cambiar los métodos de seguridad predeterminados.

2.2.3.-**T**ipos de **R**edes **P**rivadas **V**irtual

El marco de posibilidad para la implantación de una Red Privada Virtual es cada día más amplio dado al gran crecimiento de la red de redes "Internet", y con ello se sustenta con el hecho del incremento de la capacidad de transmitir mayor cantidad de información en menor tiempo. Sin embargo, la configuración de una VPN no sólo depende del medio de transmisión que ésta utilice, sino en la manera que sus diversos componentes sean dispuestos y concebidos para cumplir su función específica.

A continuación se reseñan las configuraciones más comunes en una implementación de una Red Privada Virtual:

2.2.3.1 Acceso Remoto antes de la Red Privada Virtual

Como se observa en la siguiente figura cuando se configura el acceso remoto antes de la Red Privada Virtual para establecer sesiones VPN, se utiliza la red pública de telefonía, donde el cliente "PC" hace una llamada a través del "MODEM" y se conecta directamente al servidor de acceso remoto "REMOTE ACCESS SERVER", el cual da acceso a la Red Corporativa "LAN", después de cumplido todo el proceso de Identificación y Autenticación.

Cabe destacar, que dicha conexión no superará los 56Kbps para la transmisión de los paquetes en ambos sentidos.

Figura 10. Acceso Remoto antes de la VPN

Para conectar usuarios móviles ó remotos a la red empresarial tradicionalmente han venido utilizando servicios de telefonía ó ISDN conmutadas.

El ejemplo típico son aquellos usuarios que no disponen de conexiones permanentes a la red corporativa han venido utilizando el servicio de "Marcado Telefónico". Sin embargo, la elevada tarifa para llamadas de larga distancia, ha hecho de ésta solución muy costosa.

Otro costo considerable está constituido en el "Servidor de Acceso Remoto", el cual actúa como un sitio central de conexiones, así como lo relativo al personal de soporte técnico necesario su configuración mantenimiento.

2.2.3.2 Acceso Remoto después de la Red Privada Virtual

Como se observa en la siguiente figura cuando se configura el acceso remoto después de la Red Privada Virtual para establecer sesiones VPN, se utiliza la red pública de telefonía, donde el cliente "PC" hace una llamada a través del "MODEM" y un proveedor de servicio local "ISP" y se conecta vía Internet al servidor a la puerta de enlace VPN "Firewall" de la corporación, el cual provee finalmente el acceso a los recursos corporativos al cliente una vez cumplidas todas las reglas y políticas de acceso.

Adicionalmente dicho esquema permite establecer conexiones muchas rápido (500Kbps ó superior) con el uso de tecnología DSL ó cable que hoy día proveen diversos “ISP” alrededor del mundo.

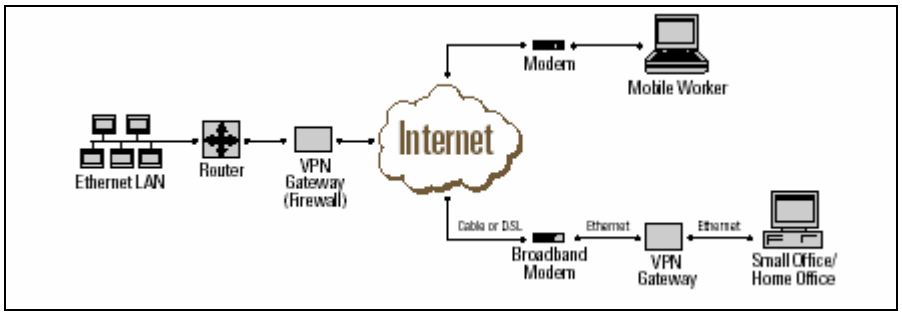


Figura 11. Acceso Remoto después de la VPN

En esta configuración es posible sustituir el tradicional “MODEM” por el uso de tecnología DSL ó cable provista por diversos “ISP” alrededor del mundo, lo cual, permite establecer conexiones muchas rápidas (500Kbps ó superior) y disminuir sustancialmente el costo de conexión para cada Estación ó Cliente.

2.2.3.3 Conectividad Sitio a Sitio antes de la VPN

Como se observa en la siguiente figura ambos extremos de la VPN se encuentra conectados por una nube “Frame Relay” ó una “Línea Dedicada”, lo cual está supeditado a las reglas y políticas de acceso configurados en los enrutadores “Router” que incluidos en la conexión, los cuales provee el acceso a los recursos dispuestos tanto en la sedes principal como en la sucursales conectadas.

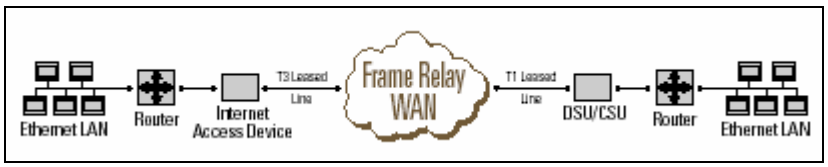


Figura 12. Conectividad Sitio a Sitio Antes la VPN

En el mundo comercial en el cual vivimos requiere en muchos casos que las compañías mantengan una estrecha comunicación con todas sus sucursales tanto regionalmente como internacionalmente. Este concepto se ha venido desarrollando mediante el uso de servicios de líneas dedicadas ó marcado telefónico (local / Internacional), como el caso de los usuarios remotos descritos previamente

Como se observa en la figura anterior la conexión entre toda la Empresa, requiere se instale un router VPN y el arrendamiento de una línea dedicada en cada una de las sucursales y básicamente se establece el túnel sobre una nube “Frame Relay”.

2.2.3.4 Conectividad Sitio a Sitio Después de la VPN

Como se Observa en la siguiente figura el esquema de conectividad Sitio a Sitio después de la VPN, utiliza la Internet como medio de transmisión de la información y se sustituye Backbone WAN (nube Frame Relay) presentado en el esquema “Conectividad Sitio a Sitio antes de la VPN”. Esto representa una gran ventaja dado a que se disminuye notablemente los costos de alquiler y mantenimiento del enlace.

Una transmitida la información a través de la Internet el VPN Gateway la recibe para analizar, descencriptar y comprobar su autenticidad e integridad de acuerdo las reglas y políticas de acceso establecidas a nivel corporativo.

Una vez finalizado el proceso de autenticación se establece la sesión a través de un túnel privado y seguro el cual provee el acceso al usuario remoto (sucursal) a los recursos disponibles en la red corporativa.

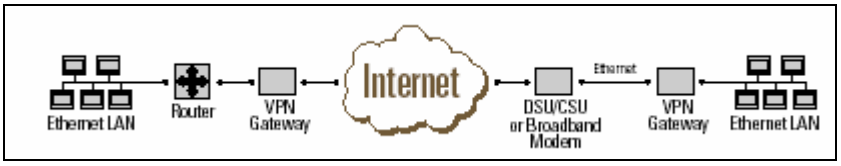


Figura 13. Conectividad Sitio a Sitio Después la VPN

3.- Marco Metodológico

3.1.- Diseño de la Investigación

Dado el contexto y características donde se enmarca ésta investigación, es importante explorar el objeto en estudio mediante la evaluación y diagnostico en forma directa de los aspectos que intervienen en la necesidad de disponer la información contenida en el Sistema de Información del Sector Eléctrico, a los fines de identificar y analizar todos los factores que inciden en la problemática planteada.

En tal sentido se adoptará la modalidad de **Proyecto Factible**, la cual es definido por la UPEL (1998), como:

"El Proyecto Factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimiento o necesidades de organizaciones o grupos sociales". (p.7).

De lo anterior se infiere que según el diseño de investigación adoptado, los resultados que se obtendrán en el presente estudio conducirán a la implantación de un modelo viable (Dado a su factibilidad Técnica y Económica) que facilite el tratamiento de la información que se maneja en los proyectos de carácter técnicos en desarrollo dentro de la Fundación para el Desarrollo del Servicio Eléctrico.

3.2.- Tipo de Investigación

Dada la importancia de determinar los efectos que causan la incidencia de las variables que intervienen en la necesidad de disponer de la información contenida en el SISE a los usuarios autorizados de manera segura y confiable a través de la Internet, se adoptará el tipo de investigación Explicativo, el cual es definido por Hernández, Fernández y otros, (1998)

como: “Aquella investigación que va más allá de la descripción de conceptos o fenómenos del establecimiento de relaciones entre conceptos; está dirigida a responder las causas de los eventos físicos o sociales”. (p.66).

De la definición anterior se infiere, que ésta investigación conducirá a la interpretación de la necesidad de disponer la información contenida en el SISE de forma segura y privada, donde sólo puedan accederla aquellos usuarios predefinidos y autorizados por el administrador del sistema, así como la atención y estudio de los agentes externos que distorsionan, comprometen y atentan en la comunicación que se da de extremo a extremo en la implantación de una Red Privada Virtual, tales como:

a) Ataque del Hombre en el medio: Lo cual compromete la integridad de la información contenida en el sistema

b) Denegación del Servicio: Lo compromete la disponibilidad y estabilidad dado el alto nivel de solicitud de respuesta exigido al sistema.

c) Certificación de las fuentes de datos: Aseguramiento de la autenticidad de los nodos que integran la Red Privada Virtual.

Los elementos citados previamente se estudiarán en función de impulsar al logro efectivo de las metas preestablecidas y brindar resultados de manera ágil y efectiva, a los requerimientos recibidos del entorno de la organización, para apoyar al ejecutivo nacional en la toma de decisiones.

3.3.- **M**etodología **E**mpleada para el **D**iseño y **D**esarrollo de la **VPN**

Dadas las características y objetivos planteados en esta investigación, es necesario definir un patrón metodológico que indique las fases ó pasos a seguir, en la búsqueda del alcance de dichos objetivos. En tal sentido el autor consideró seleccionar según la técnica de Eclecticismo, una metodología mixta con la recomendación de los autores Ruixi Yuan, W. Timothy Strayer, en su publicación "Virtual Private Networks: Technologies and Solutions" y lo sugerido por Casey Wilson y Peter Doak, en su libro "Creating and Implementing Virtual Private Networks".

Dado a que la VPN prevista para implantar en Fundelec prevé conexiones de Empresas Eléctricas y Fundelec (G2E) las cuales estarán enmarcadas bajo el método "Conectividad Sitio a Sitio" y las que tengan lugar entre Usuario del Sector Eléctrico y Fundelec, suscritas en el método "Acceso Remoto".

Lo cual hace que la Red Privada Virtual a implantarse disponga de ambos métodos de conexión, lo que soporte la consecución de los objetivos de la presente investigación.

A continuación un cuadro resumen de la metodología propuesta por el Autor:

Fase	Descripción
1	Evaluación de la Plataforma Informática de FUNDELEC
2	Desarrollo de las políticas de seguridad y acceso de la VPN
3	Determinación de la estrategia para implantación de la VPN
4	Diseño y Desarrollo de la Infraestructura para conexiones segura en VPN
5	Validación y prueba del esquema
6	Entrenamiento para los usuarios remotos del sistema

Tabla 1. Metodología Propuesta por el Autor

3.3.1.- Fase (1): Evaluación de la Plataforma Informática

En ésta fase se evaluarán los diversos componentes que conforman la Red LAN de FUNDELEC, para su efectiva integración y/o adecuación a los distintos esquemas de implantación de una Red Privada Virtual, así como determinar aquellos componentes no presentes en la configuración actual de la RED, para cada uno de los tipos de VPN de conformidad con lo descrito en las “Bases Teóricas” de ésta investigación.

3.3.2.-Fase (2): Desarrollo de las Políticas de Seguridad y Acceso a la VPN

En ésta fase se definirán las Políticas de Seguridad y Acceso a los recursos y servicios disponibles en el “Sistema de Información del Sector Eléctrico”, en función de consolidar los aspectos susceptibles de control y/o restricción dentro de la Red Privada Virtual, lo cual se exprese en una matriz de acceso que permita configurar los perfiles para los distintos tipos de usuarios del sistema.

Dicha configuración permitirá establecer y garantizar lo siguiente

1) Disponibilidad de la conectividad a la Red Privada Virtual.
2) Comprobación de la autenticidad de la identidad del usuario cuando establece una sesión.
3) Los recursos informativos existentes en el SISE estarán limitados según el perfiles establecidos para el usuario.

3.3.3.-Fase (3): Determinación de la Estrategia para la Implantación de la VPN

De acuerdo a la necesidad que poseen los distintos agentes del sector eléctrico Venezolano de acceder a la información contenida en el SISE y evaluando las opciones y tecnologías existentes para la Implantación de una VPN, en éste capítulo se determinará la estrategia para el diseño e

implantación de la “Red Privada Virtual” en FUNDELEC, y así permitir el acceso a los recursos información contenidos del SISE de manera remota y segura.

Todo ello se ajustará en función a las posibilidades técnicas y económicas que posea FUNDELEC, lo cual quedará expresado en una matriz de evaluación y de decisiones.

3.3.4.-Fase (4): Diseño y Desarrollo de la infraestructura tecnológica para conexiones seguras en una VPN

En ésta fase se llevará a cabo el trabajo de “Ingeniería de Detalle” propiamente dicho, es decir, de acuerdo a la estrategia de implantación adoptada se efectuará un “diseño concepto” de la Red Privada Virtual y se adicionarán, instalaran y ajustarán todos aquellas herramientas (hardware y software) previstos en el diseño.

Obteniendo así una primera versión de la VPN, donde se tengan lugar las pruebas y validación previstas en la siguiente fase.

3.3.5.-Fase (5): Instalación y Pruebas del esquema

Fase de comprobación del funcionamiento operativo y estratégico de la Red Privada Virtual que permite acceder los recursos del SISE. Lo cual queda expresado en términos de su disponibilidad, seguridad e integración.

3.3.6.-Fase (6): Entrenamiento para los Usuarios Remotos del Sistema

El entrenamiento es el factor fundamental para el apropiado uso de la Red Privada Virtual, por ello en la presente fase se inducirán a todos aquellos agentes asociados con el SISE para transferirles de manera efectiva los conocimientos necesarios para que puedan hacer uso de la VPN.

4.- Resultados

4.1.- Evaluación de la Plataforma Informática

En función de conocer la estructura física y lógica, de la Red LAN de FUNDELEC a continuación se describen cada uno de sus componentes:

a) Servidores y Estaciones de Trabajo

Está compuesta por 4 servidores configurados con el Active Directory de Windows'2000 para establecer las políticas de acceso y seguridad a cada unos de los recursos disponibles, tales como: 1)Areas de Disco; 2)Aplicaciones; 3)Impresoras; 4)Acceso a Internet, entre otros.

Asimismo, existen 70 Estaciones de Trabajo que en su mayoría operan bajo los sistemas operativos Windows XP y 2000. Contando éstas con las características y capacidades técnicas (Hardware) para desempeñarse optimamente con dichos sistemas.

b) FireWalls y Routers

Para establecer la conexión a la Internet se ha venido contratando desde el año 2000 los servicios de Cantv Banda Ancha ABA de 1.536Mbps, lo cual incorpora un Modem Router Cisco 677, el cual es el enlace entre la Red LAN y la Internet.

Adicionalmente FUNDELEC dispone de un enlace suministrado por el Ministerio de Energía y Minas para el acceso a Internet, cuyo proveedor es Genesis, y se ha establecido según conexión Interna como se observa en el siguiente gráfico.

Asimismo, en Fundelec se Implementó ISA Server, con el objeto de proteger de los ataques y acceso no autorizado a la información contenida en la Red LAN, así como, controla el tráfico entrante y saliente hacia la Internet.

A continuación se muestra el diagrama lógico de interconexión de la Red LAN de FUNDELEC.

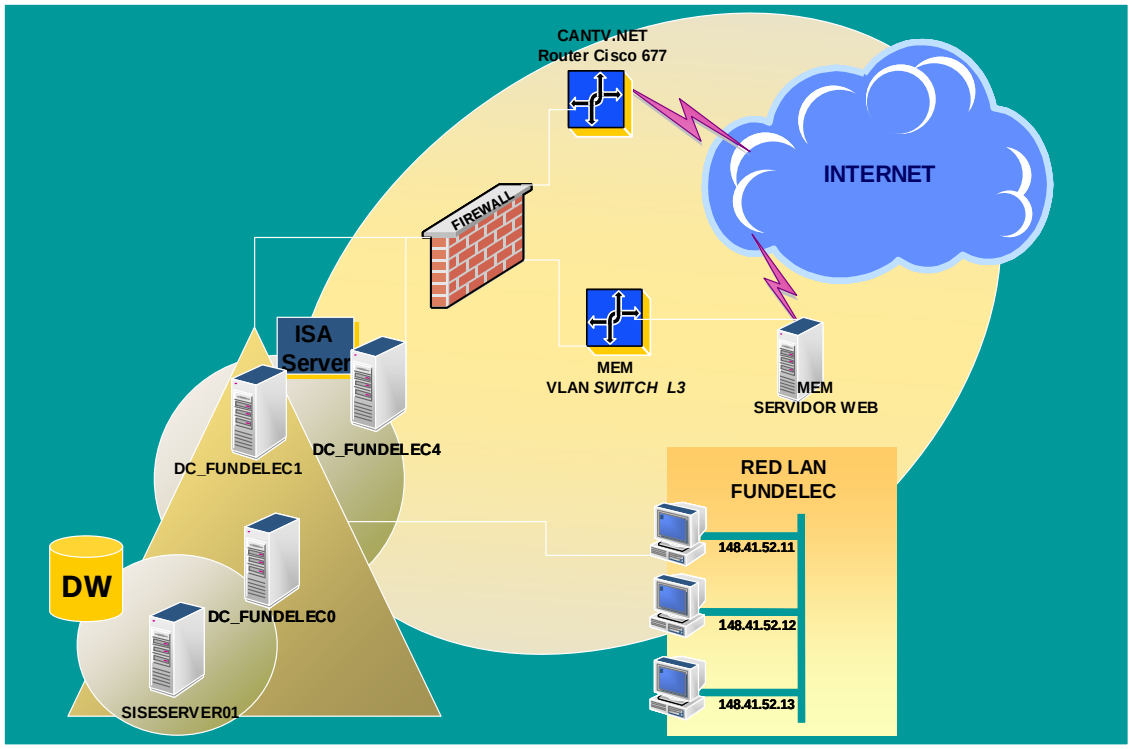


Figura 14. Diagrama General de la Plataforma Informática

Como se aprecia en el Diagrama General de la Plataforma Informática de FUNDELEC, el Servidor “Siseserver01” donde se encuentra alojado el SISE es parte del mismo dominio “interfundelec.org”, dicha configuración es riesgosa y compromete la seguridad de la RED en un esquema de acceso remoto, dado que, no sólo habría que controlar el acceso al servidor del SISE sino a todos aquellos que componen el dominio interfundelec.org.

Asimismo, es de notar que sólo existe una implementación del SISE en operación, es decir, que el mismo servidor de desarrollo del sistema ejecuta funciones producción y consultas, lo que trae como consecuencia los siguientes riesgos:

1.- Los usuarios remotos pudieran acceder a módulos y consultas aún no depuradas ni validadas y obtener información no precisa o actualizada.

2.- El sistema está de cara a los desarrolladores y usuarios en simultaneo, lo cual implica, que con cierto daño ó ataque que sufra el SISE ambos esquemas se vean afectados.

De igual forma, cabe destacar el hecho que todo el tráfico cursado desde la Internet ó hacia ella, se efectúa de manera simple y clara, es decir, “texto en claro”, lo que abre la brecha de posibilidades para que la información contenida en el SISE, la cual, es accedida por un usuario autorizado, sea obtenida y por personas no autorizadas una vez que cruza la frontera de la plataforma informática de FUNDELEC, y entra en la red pública ó Internet.

Adicionalmente, en el esquema General de la Plataforma Informática no se observa un método alterno para el acceso de los usuarios remotos hacia el SISE, sino sólo vía Web, Claro está que la presencia de la Internet cada día es mayor en cada uno de los lugares de nuestro país y en el mundo, sin embargo, para aquellos usuarios que no dispongan de dicho servicio debe preverse una solución que sea técnicamente factible y que no implique grandes inversiones para dicho usuario, tal como lo es, la conexión a través de una línea telefónica ó DialUp, lo cual permita conectar el cliente a la red privada virtual.

4.2.- Desarrollo de las Políticas de Acceso y Seguridad a la VPN

4.2.1.-De los Usuarios

1.- El acceso a la Información contenida en el SISE que FUNDELEC considere de carácter privado y/o exclusiva estará disponible sólo a aquellos usuarios autorizado a través de la Red Privada Virtual.

2.- Los usuarios remotos con privilegios exclusivos para acceder al SISE deben poseer una identificación electrónica (certificado) como instrumento de autenticidad antes el sistema. Dicha Identificación será unipersonal ó unifuncional y no se permitirá su transferencia.

3.- Cada usuario tendrán un perfil de acceso que le permitirá acceder sólo a las áreas de información, módulos y consultas preestablecidas, de acuerdo a su función e interés dentro del sistema.

4.- Los Certificados Digitales tendrán una vigencia de uso según la consideración y aprobación de la Junta coordinadora para el desarrollo del SISE.

5.- Toda información suministrada por el Sistema al Usuario Remoto es de uso exclusivo y privado, por lo que, queda sin efecto su divulgación, promoción y publicación.

4.2.2.-De la Plataforma Informática del SISE

1.- La Infraestructura informática que soporta a la Red Privada Virtual debe proveer los mecanismos para que cada usuario obtenga, instale y configure su identificación electrónica antes el sistema.

2.- Todas las Empresas Eléctricas deben ser provista con un área de almacenamiento privado y exclusivo dentro de la Red Privada Virtual para el envío periódico de la información requerida por el SISE.

3.- La infraestructura informática para atender a los usuarios remotos deben estar fuera del ámbito de la Red Lan (interfundelec.org), lo cual, reduce el establecimiento del control del acceso y la seguridad sólo a los recursos informativos contenidos en el SISE.

4.- La Plataforma para la conexión al SISE vía VPN debe ofrecer métodos alternos, para aquellos casos que el usuario no posea por razones excepcionales ó naturales acceso a la Internet.

5.- La Red Privada Virtual debe ofrecer disponibilidad e interoperatividad con los protocolos TCP/IP, PPTP y L2TP a los fines de ser compatibles con los estándares de comunicación utilizados en la Internet.

4.3.- Determinación de la Estrategia para la Implantación de la VPN

Para establecer la estrategia de implantación de la Red Privada Virtual, la cual dará acceso a los usuarios remotos del SISE, es importante determinar el tipo de red virtual a configurar (sección 2.2.3 de ésta investigación) y la cual será designada en lo sucesivo como “Estructura Física de Conexión de la VPN”. Asimismo, debe efectuarse lo propio con los métodos de conexión descritos en la sección 2.2.2 (componentes de una red privada virtual) y en lo adelante reseñados como “Métodos de conexión a la Red Privada Virtual”.

Por lo que, la estrategia que orientará el desarrollo e implantación de la VPN, considera no sólo las herramientas disponibles en cada uno de las áreas y funciones dentro de la Red Interna de FUNDELEC, sino la posibilidad de adquisición de nuevos componentes en un momento dado, los cuales, fortalezcan el esquema desarrollado.

Por lo cual, a continuación de estudiarán los aspectos “Estructura Física de Conexión de la VPN” y “Métodos de conexión a la Red Privada Virtual” y las distintas alternativas e implicaciones en cada uno de sus componentes.

4.3.1.-Estructura Física de la Red Privada Virtual

De acuerdo a los tipos de Redes Virtuales presentados en la sección 2.2.3, a continuación se presenta una tabla comparativa entre ambos esquemas.

Tipo VPN	Riesgos y Vulnerabilidades	Requerimientos	Disponible
Conexiones VPN directo a la LAN	Todos los componentes de la red LAN están comprometidos y confinados a la seguridad de la VPN, así como el SISE en desarrollo	- (1) Servidor VPN	NO
		- (1) FireWall	SI
		- (1) Servidor RAS (Telefónico)	NO
Conexiones VPN directo al área de Red Perimetral (dmz)	Sólo la Red Perimetral está sujeta al establecimiento de control y seguridad	- (1) Servidor SISE (Prod)	NO
		- (1) Servidor VPN	NO
		- (1) FireWall	SI
		- (1) Servidor RAS (Telefónico)	NO

Tabla 2. Comparación de los esquemas de conexión de una VPN

Como se observa en la tabla anterior, el esquema de conexiones VPN directo al área de Red Perimetral ó DMZ, confiere solamente acceso a los recursos informativos contenidos en el servidor del SISE (producción), obteniendo de esta manera dos ventajas significativas:

1.- Los usuarios remotos podrán acceder a una versión validada y revisada del SISE.

2.- La Plataforma Informática de FUNDELEC no estará expuesta a usuarios que sean autorizado para el uso del SISE, pero no así para el acceso a aplicaciones e información inherente sólo a las áreas internas de la organización.

4.3.2.-Métodos de Conexión a la Red Privada Virtual

La selección del tipo de tecnología a utilizarse para establecer el túnel Cliente-Servidor, es el aspecto más importante en el desarrollo de una VPN, dado que de ello depende la capacidad, flexibilidad y seguridad de dicha Red.

A continuación se presenta una tabla comparativa de los aspectos más importante de los protocolos IPsec y SSL:

Protocolos / Características	SSL (Socket Secure Layer)	IPSec (IP Secure)
Maneja Tecnología PKI	SI	SI
Longitud de Clave	128bits	128bits
Presencia en Modelo (OSI)	Capa 6 (Aplicaciones)	Todas las Capas
Acceso Subredes con control de Acceso Requerido	NO	SI
Compatibilidad con Árbol de Directorio	NO	LDAP, Kerberos
Típica Implementación	Bancaria	Corporativa Militar Gubernamental
Clientes a Conectarse	No Controlado	Conocidos e Identificados
Instalación en la del Cliente	Automático	SemiAutomático

Tabla 3. Comparación entre los Protocolos SSL Vs. IPSec

Como se muestra en la tabla anterior IPSec y SSL poseen características similares en el manejo de claves públicas. Sin embargo existen diferencias según la aplicabilidad que éstos tienen en distintos escenario.

En el caso del acceso requerido por los usuarios remotos a las consultas disponibles en el SISE, donde es necesario la autorización y autenticación para el establecimiento de la sesión, pareciera necesaria la implementación de IPSec, dado a su integración a través de los protocolos LDAP y Kerberos, con el árbol de directorio (Base de Datos de Usuarios) de Windows 2000 sistema donde está desarrollado el SISE. Así como, los sistemas operativos estándares para la línea de servidores tales como: Windows 2003, Linux, FreeSBD, entre otros.

Dado a que el SISE basa su control de acceso y seguridad interna en los distintos componentes que lo integran (Base de Datos, Servicios OLAP, Index Server, IIS5.0, entre otros), a través del uso de las Listas de Control de Acceso (ACL's). Lo que permite establecer Grupos de Usuarios para el acceso a consultas específicas a cada perfil de usuario.

Por lo que, dicho esquema puede ser extensivo a las conexiones remotas efectuadas vía Red Privada Virtual, si se transfieren los datos del autenticación del usuario a través de LDAP ó Kerbero a las ACL's de Windows 2000.

Asimismo, es de notar que se estima un universo de usuarios remotos controlados, es decir, sólo aquellos usuarios que Fundelec autorice para el uso del sistema podrán accederlo, por lo que, su instalación en el lado del cliente no debe ser un obstáculo para la implementación.

4.4.- Diseño y Desarrollo de la Infraestructura Tecnológica para Conexiones Segura en una VPN

De acuerdo a lo analizado en la sección anterior la estructura física de conexión se desarrollará bajo el contexto de “Conexiones VPN directo al área de Red Perimetral (dmz)”, dado a la independencia que suministra dicho esquema con respecto al control de acceso y seguridad de la red interna de Fundelec. Asimismo, dicho esquema permitirá establecer un servidor para el SISE en ambiente de producción tanto para los usuarios remotos como los usuarios internos.

En cuanto al método de Conexión a la Red Privada Virtual, se seleccionó el protocolo IPSec para el establecimiento del túnel en cada sesión de usuario, dado a su integración con el Active Directory, componente que controla el acceso y la seguridad de Windows 2000 y por ende la del SISE.

A continuación se muestra Diseño General de la VPN para FUNDELEC

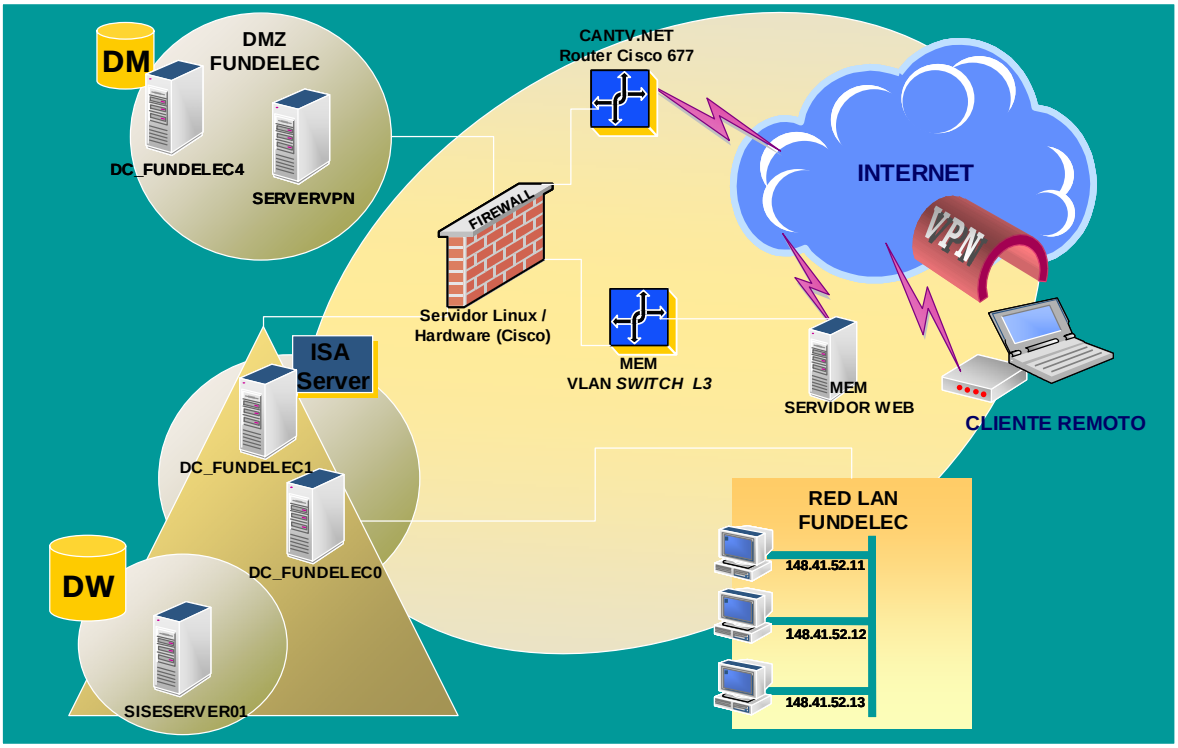


Figura 15. Diagrama General de la VPN a implantarse en FUNDELEC

4.4.1.-Diseño detallado de la Infraestructura para la Implantación de la VPN

A continuación se presentan cada uno de los componentes de Hardware y Software requeridos y disponibles en Fundelec para implantación de la Red Privada Virtual en Fundelec.

	Componente	Disponible	1era Opción	2da Opción
Hardware	- Servidor SISE (Producción)	NO	Estación de Trabajo (1)	Servidor Nuevo de alta capacidad
	- Servidor VPN	NO	Estación de Trabajo (2)	FireWall (Cisco, 3Com, otros)
	- FireWall	SI		
	- Servidor RAS (Telefónico)	NO	Estación de Trabajo (2)	
Software y Aplicaciones	- Tecnología de Cifrado y Enmascaramiento	NO	PKI	
	- Características del algoritmo de encriptamiento	NO	128Bits	
	- Protocolo para establecimiento del túnel	NO	IPSec	
	- Software del Cliente	NO	Conocidos e Identificados (Instalación Semi-Automática)	

a) Servidor SISE (Producción)

Para establecer el servidor del SISE en modo producción (DC_FUNDELEC4) se dispondrá de una estación de trabajo PIII 450MHz, con 256MB RAM y 40GB de capacidad en disco, quedando así instalado y configurado todo el software requerido para la ejecución del sistema. Todo ello dentro de la red perimetral bajo la subred (148.41.53.0/24).

b) Servidor VPN

Para el desarrollo y activación de los mecanismos PKI (Intercambio de Claves Pública), así como el FireWall de la Red Perimetral se dispondrá de una estación de trabajo (SERVERVPN) con la capacidad requerida por Windows 2000. Asimismo se utilizarán los servicios “Servidor de Certificado” y “Servidor de Enrutamiento y Acceso” de dicho sistema operativo.

c) FireWall

Ya existe una implementación en modalidad software con ISA Server de Microsoft en el servidor DC_FUNDELEC1, sólo se adicionarán los filtros necesarios para el establecimiento de la VPN con los protocolos PPTP y L2TP.

d) Servidor RAS (Acceso Telefónico)

Se configurará en el servidor (SERVERVPN) el servicio de acceso telefónico de Windows 2000 para permitir conexiones vía MODEM a la Red Privada Virtual que dará acceso privado y seguro al SISE.

e) Software y Aplicaciones

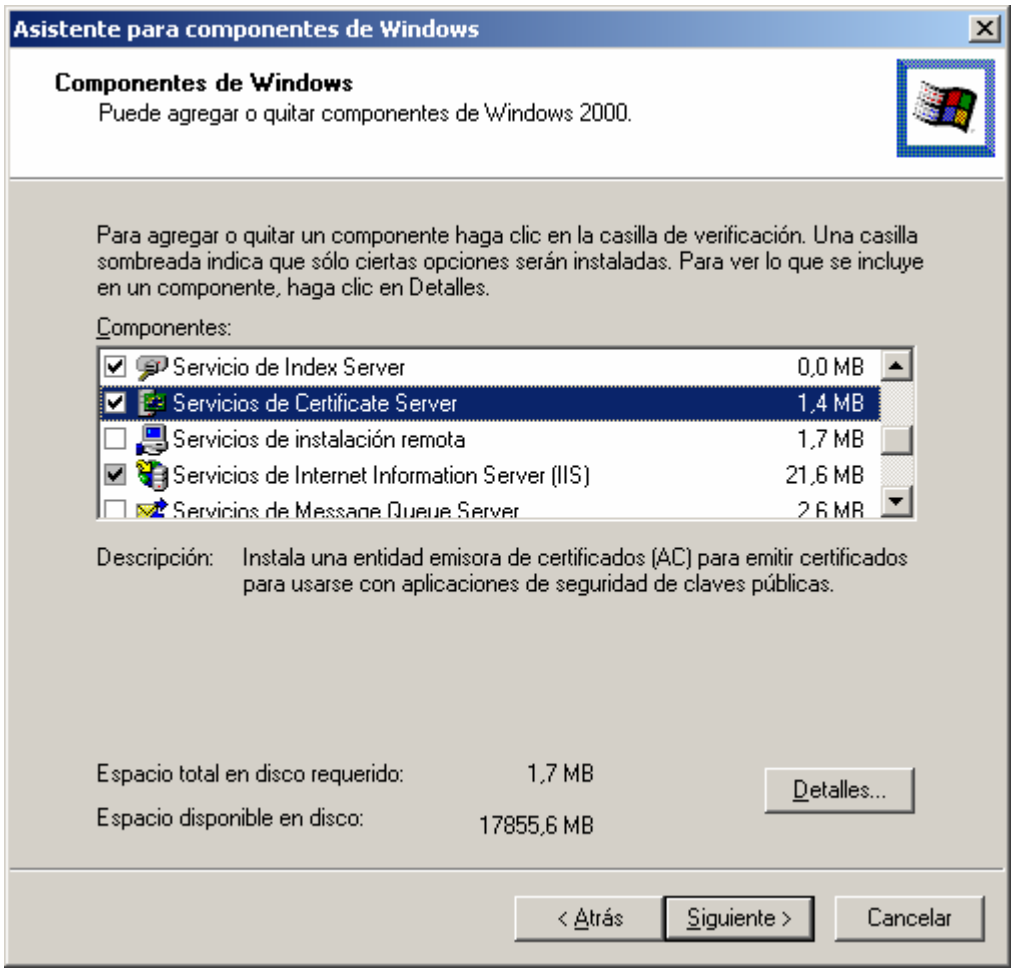
En cuanto al software y aplicaciones a utilizarse en el desarrollo de la Red Privada Virtual para brindar acceso seguro y privado al SISE, se estableció el método de conexión con la tecnología PKI (Claves Públicas), con claves de 128bits de encriptación.

Asimismo, motivado a su integración con el árbol de directorio de Windows 2000, se seleccionó el protocolo IPSec para el establecimiento del túnel de la VPN, lo cual extenderá las políticas de seguridad existentes en la red perimetral a los usuarios y conexiones remotas.

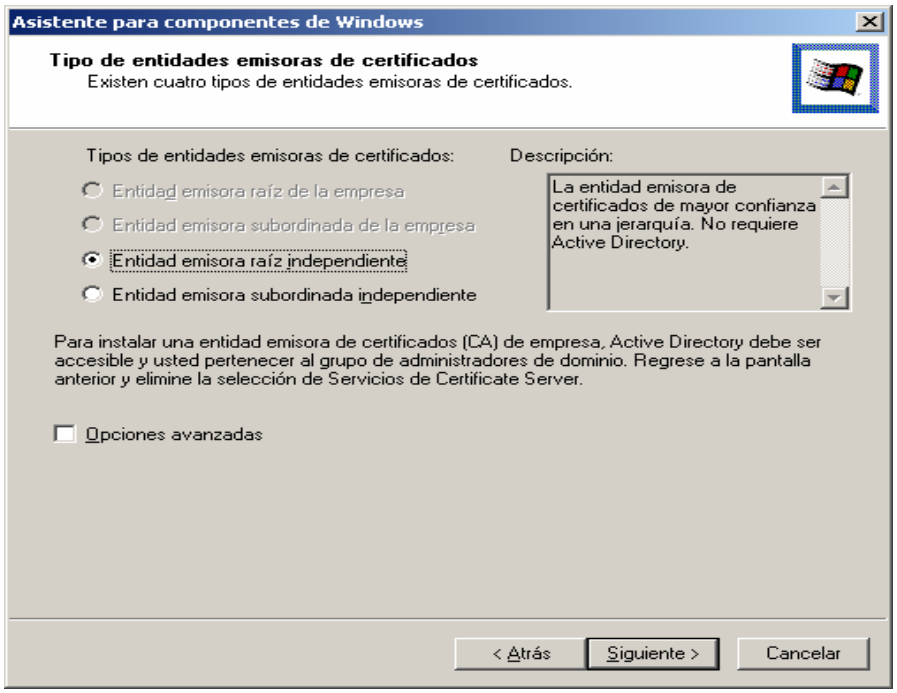
4.5.- Instalación y Pruebas del Esquema

Para configurar el Servidor VPN en Windows 2000 se instaló el "Servicio de Certificado", como se muestra a continuación.

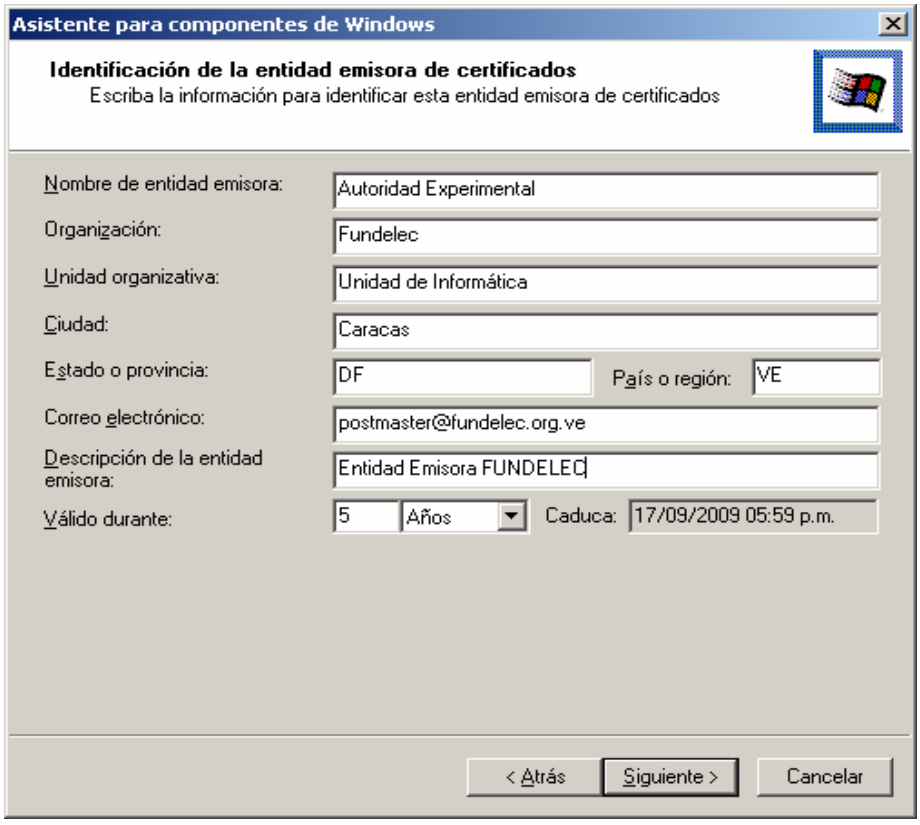
Paso 1: Instalación del Servicio de Certificado



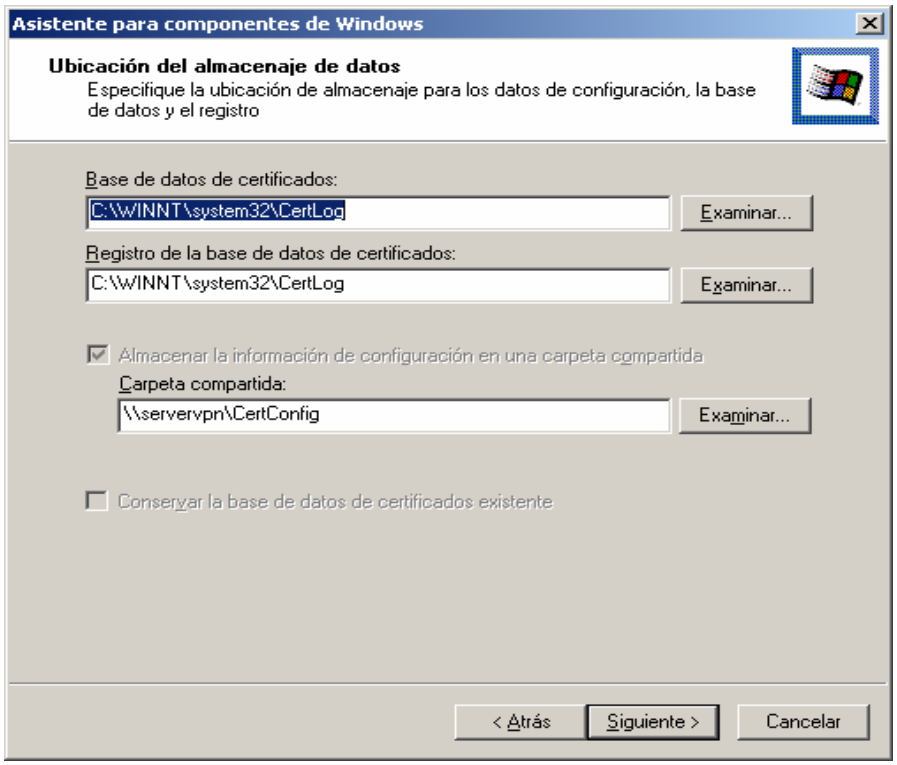
Paso 2: Instalación del Servicio de Certificado (Tipo de entidades)



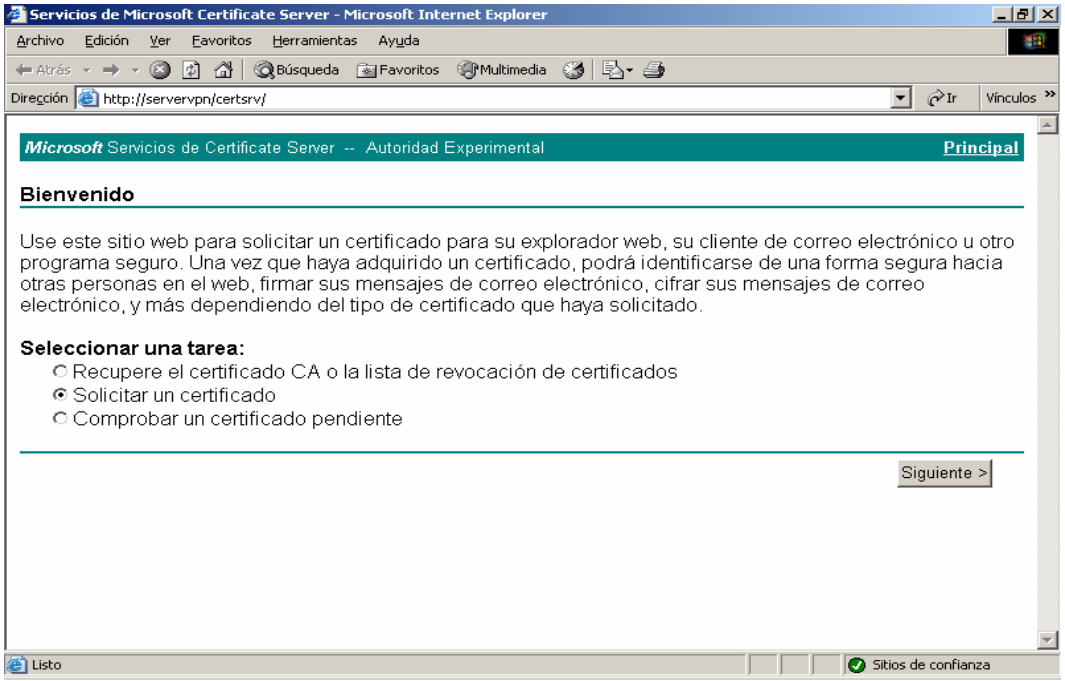
Paso 3: Instalación del Servicio de Certificado (Identificación de la entidad)



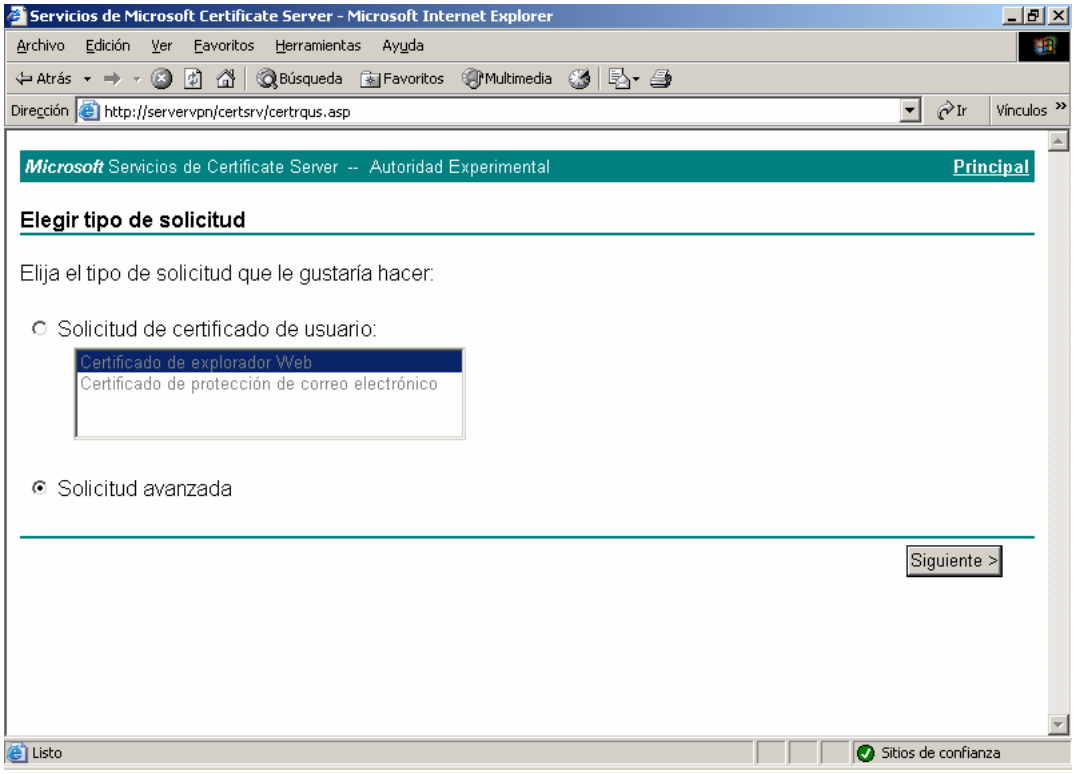
Paso 4: Instalación del Servicio de Certificado (Ubicación del Almacenaje de Datos)



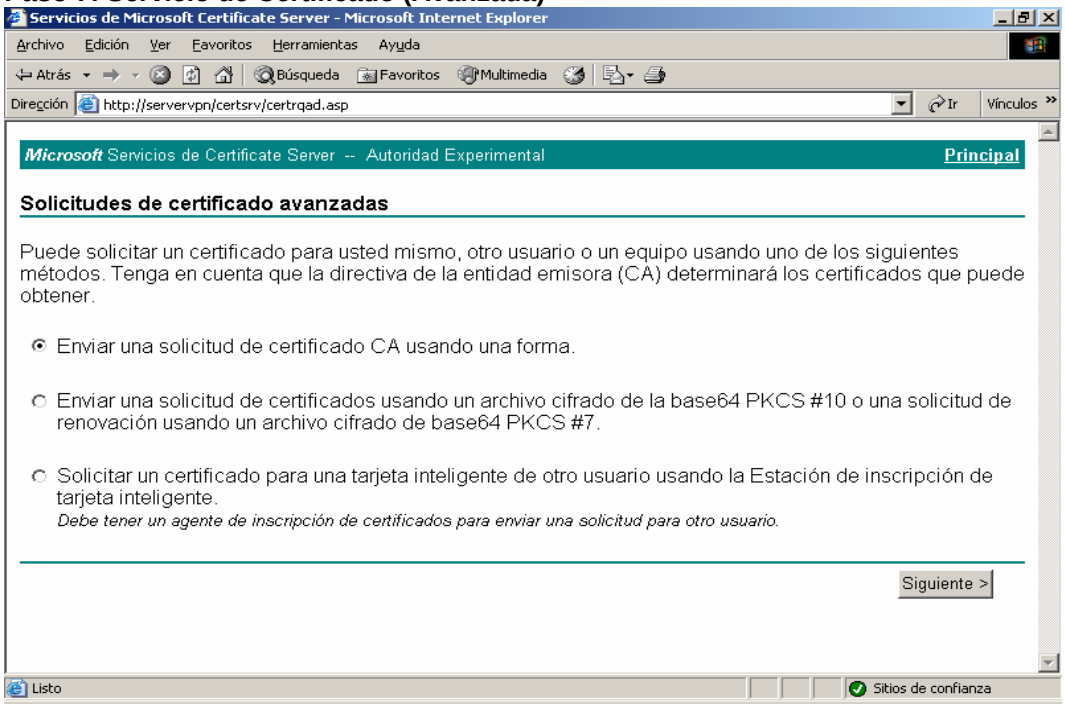
Paso 5: Servicio de Certificado (Servicio Web)



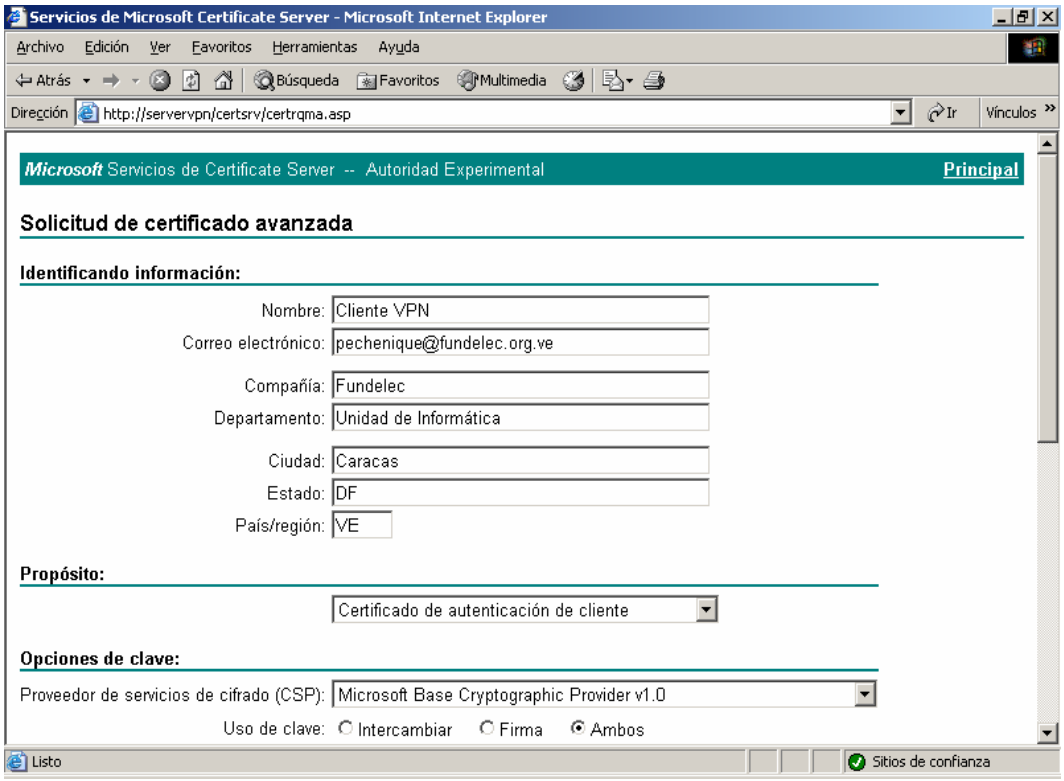
Paso 6: Servicio de Certificado (Tipo de Solicitud)



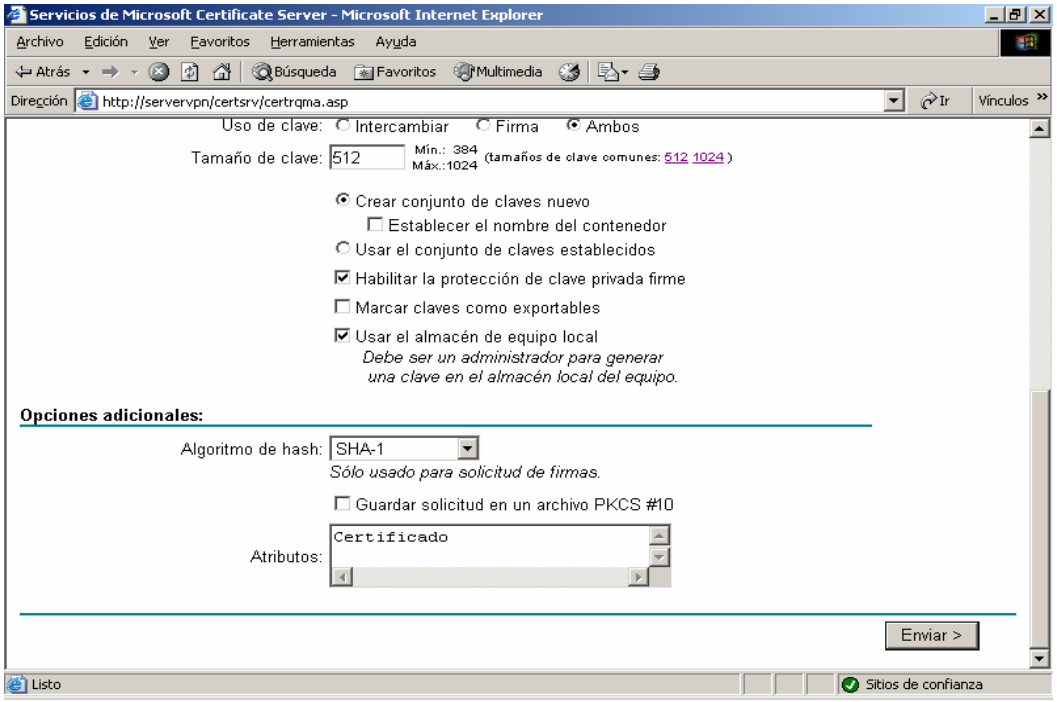
Paso 7: Servicio de Certificado (Avanzada)



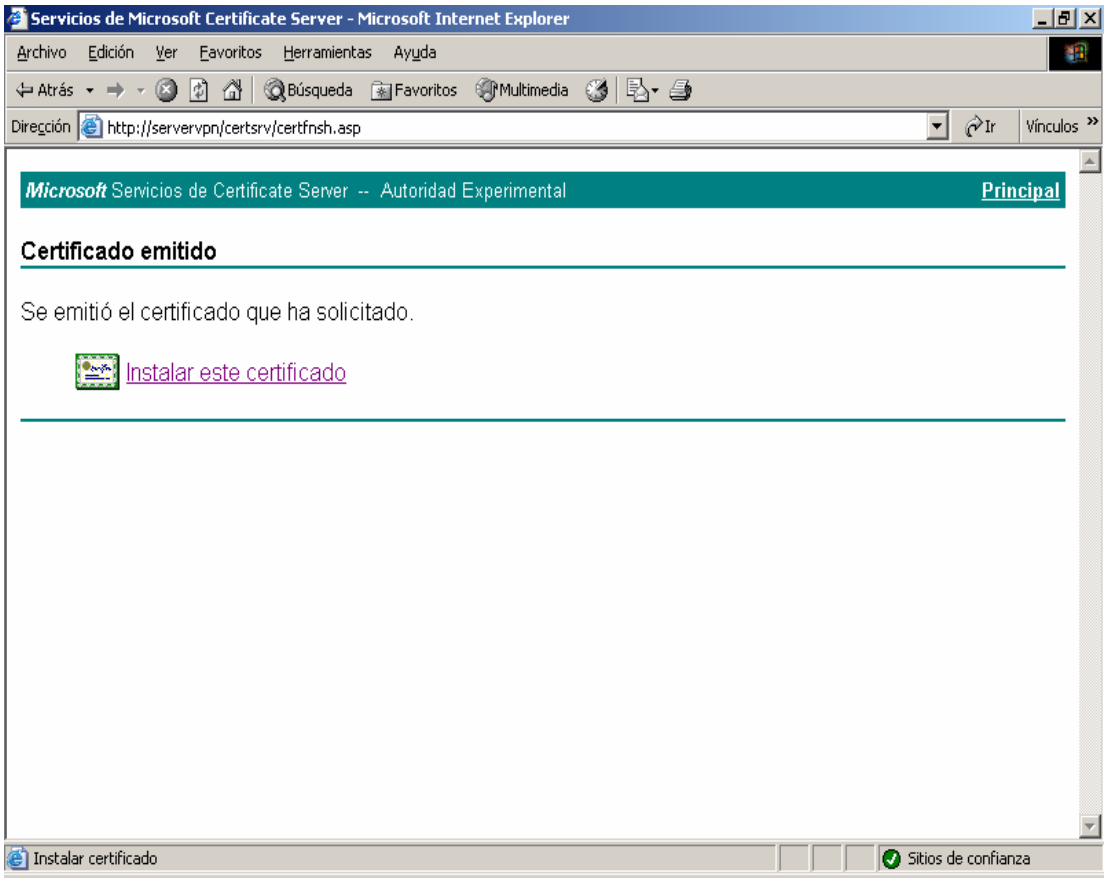
Paso 8: Servicio de Certificado (Avanzada 1)



Paso 9: Servicio de Certificado (Avanzada 2)

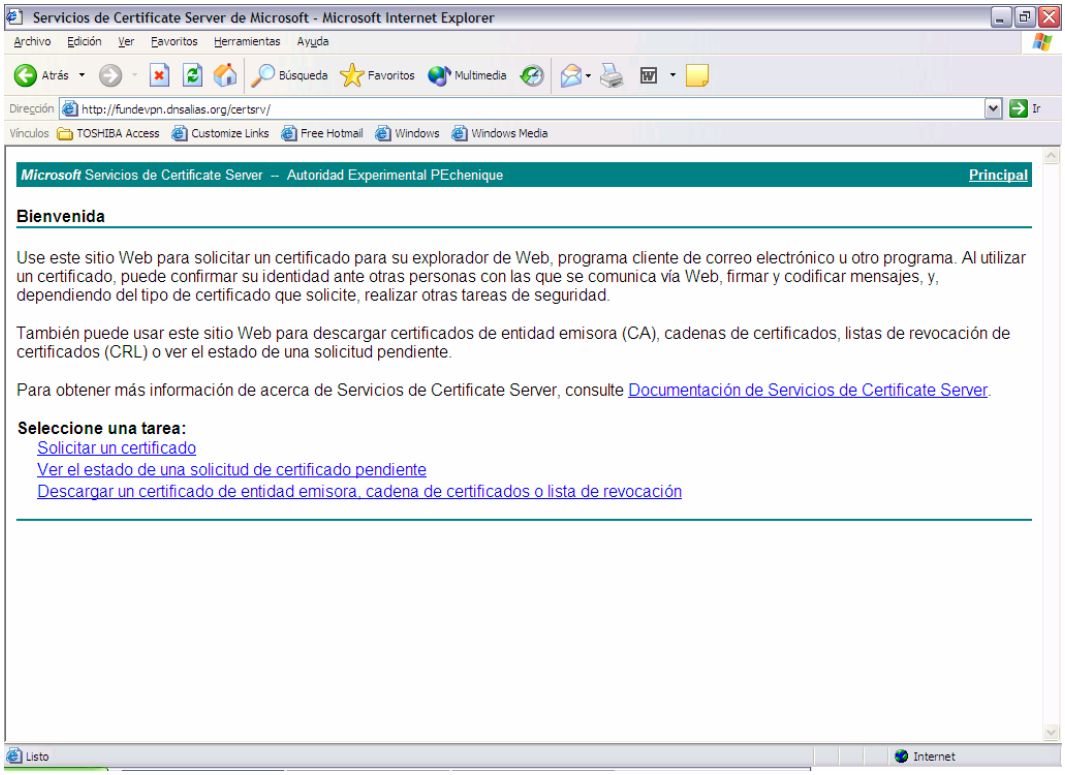


Paso 10: Servicio de Certificado (Certificado Emitido)

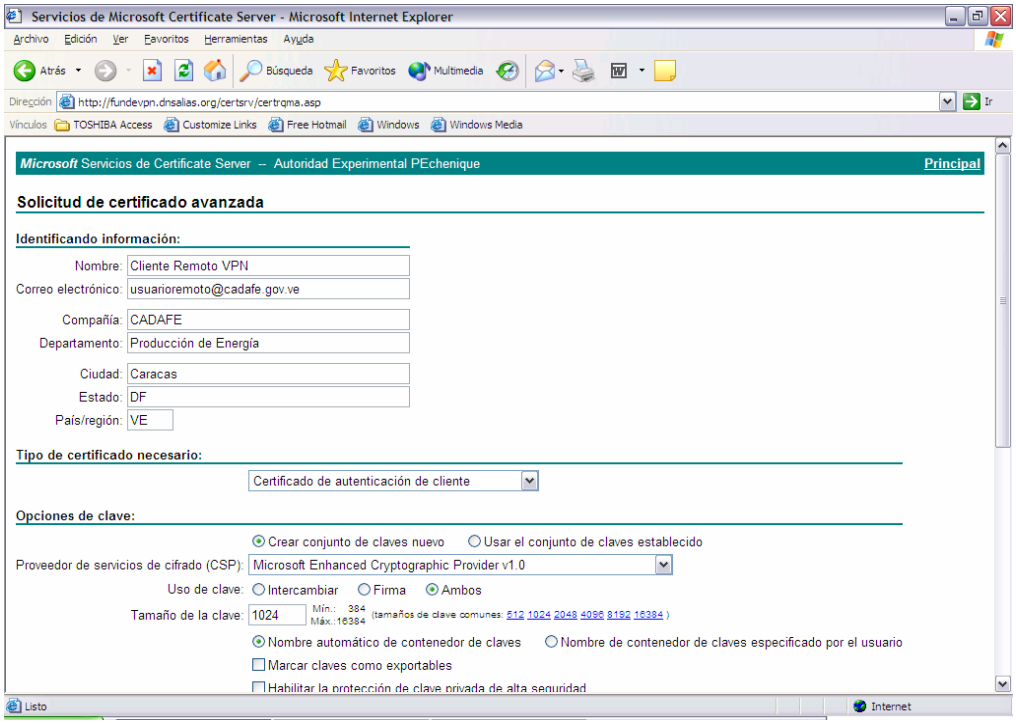


Para instalar los certificados digitales para servidores en el servidor se descargó desde el sitio fundevpn.dnsalias.org, a través del siguiente proceso:

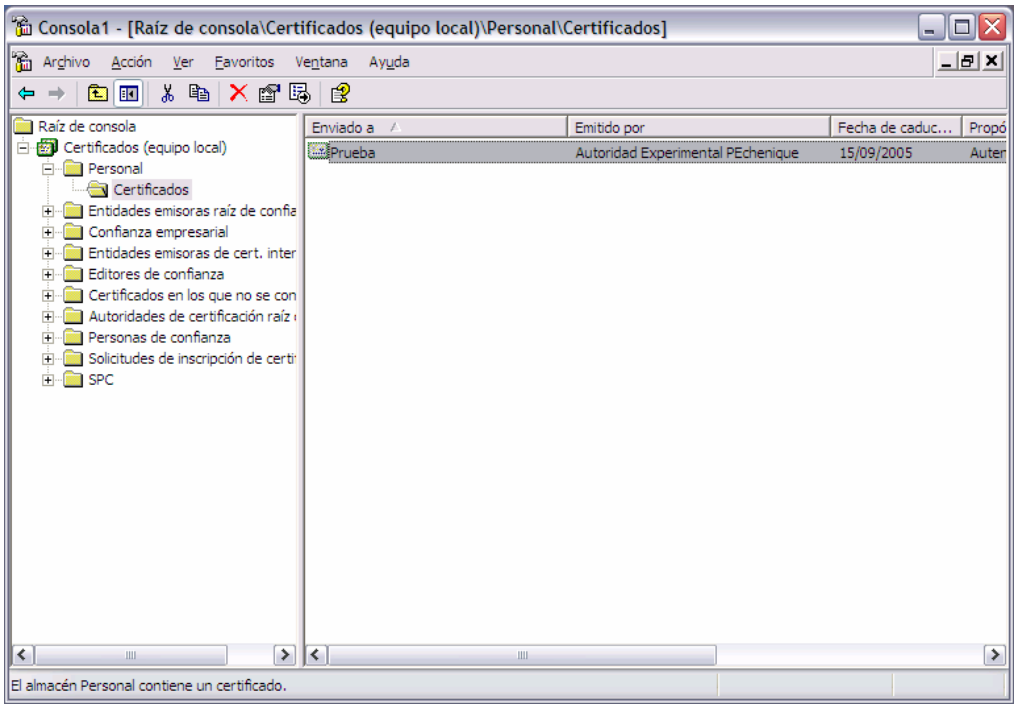
Paso 1: Descargar el certificado desde el Sitio Privado (fundevpn.dnsalias.org)



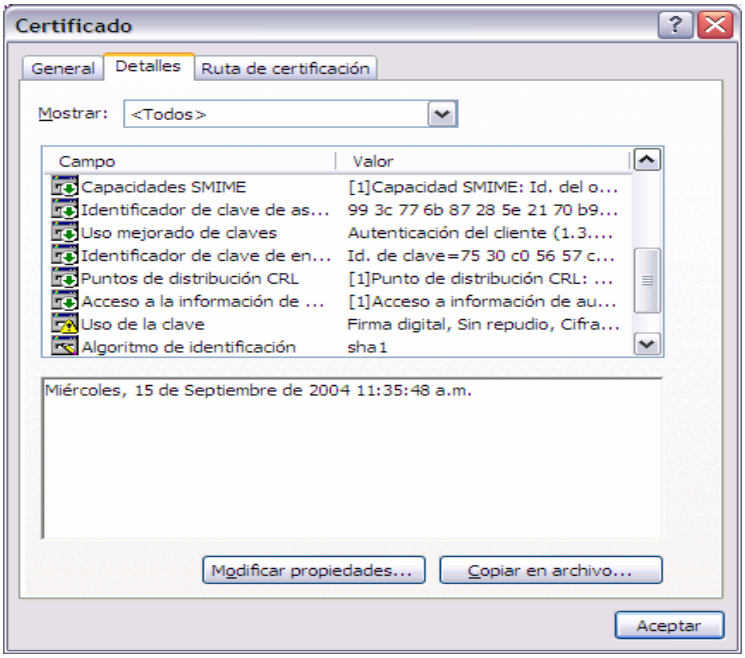
Paso 2: Formulario de Registro para el Certificado (fundevpn.dnsalias.org)



Paso 3: Certificado Instalado en el Cliente (fundevpn.dnsalias.org)

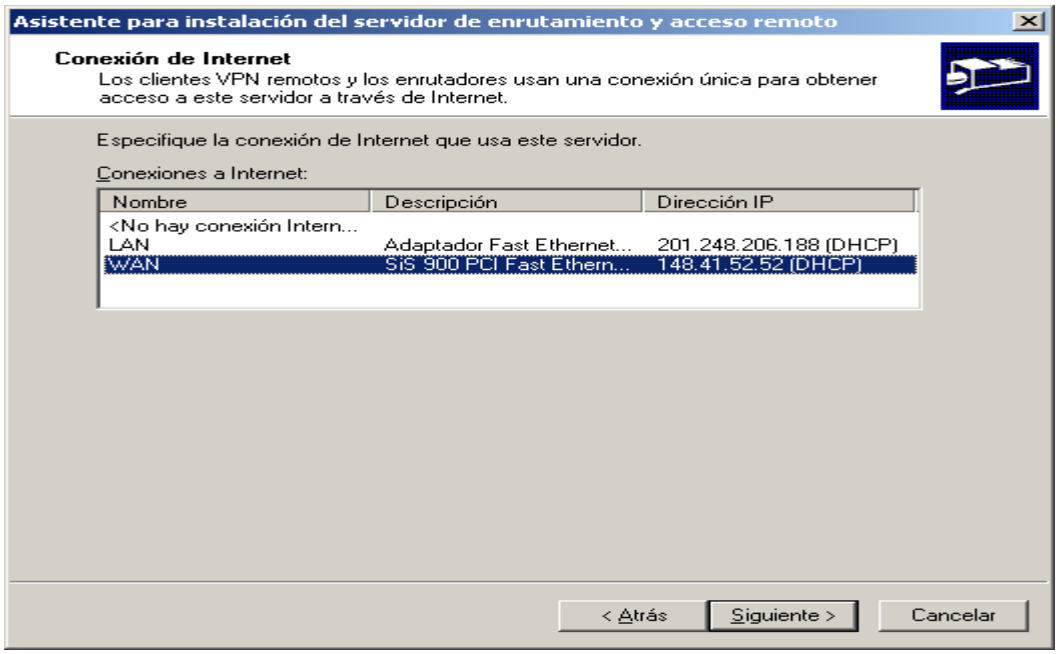


Paso 4: Características del Certificado Instalado en el Cliente (fundevpn.dnsalias.org)

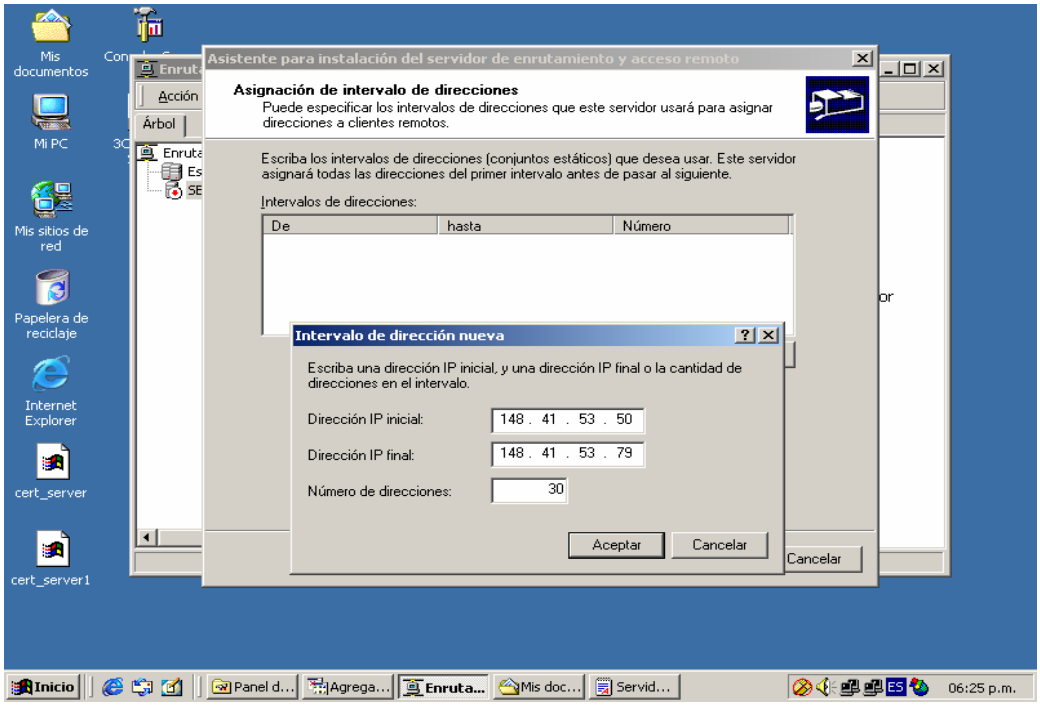


Una vez instalado el certificado en el servidor se procedió a habilitar el servicio de Enrutamiento y Acceso.

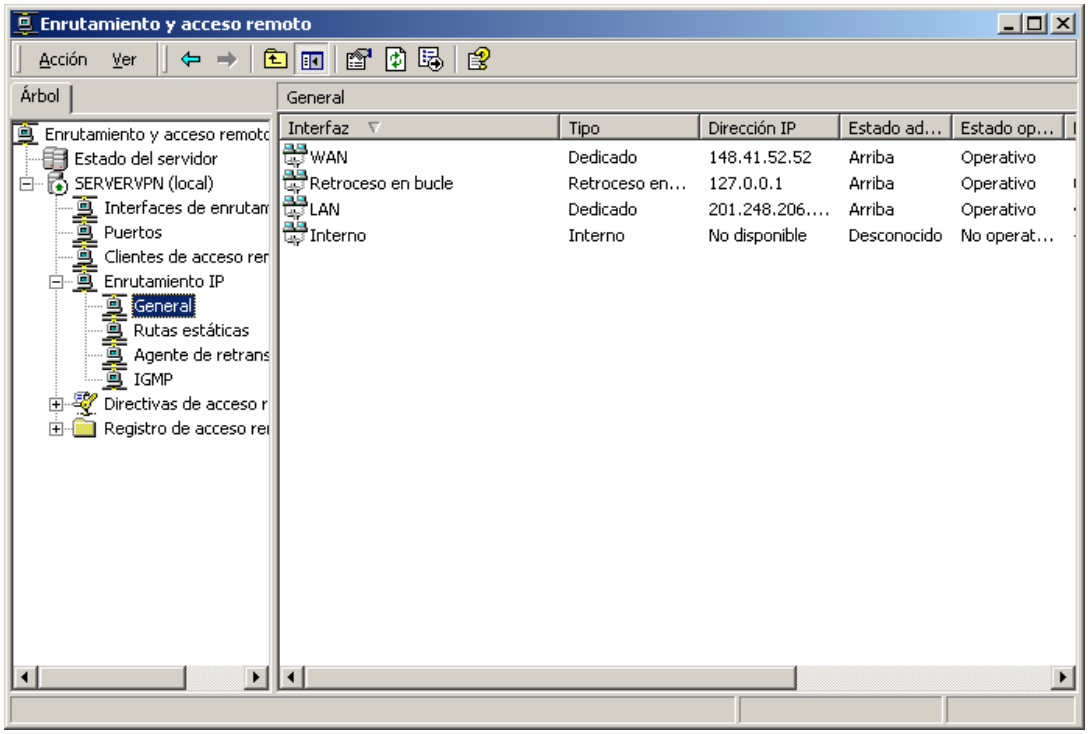
Paso 1: Instalación de Servidor Enrutamiento y Acceso



Paso 2: (Definición de la SubRed)

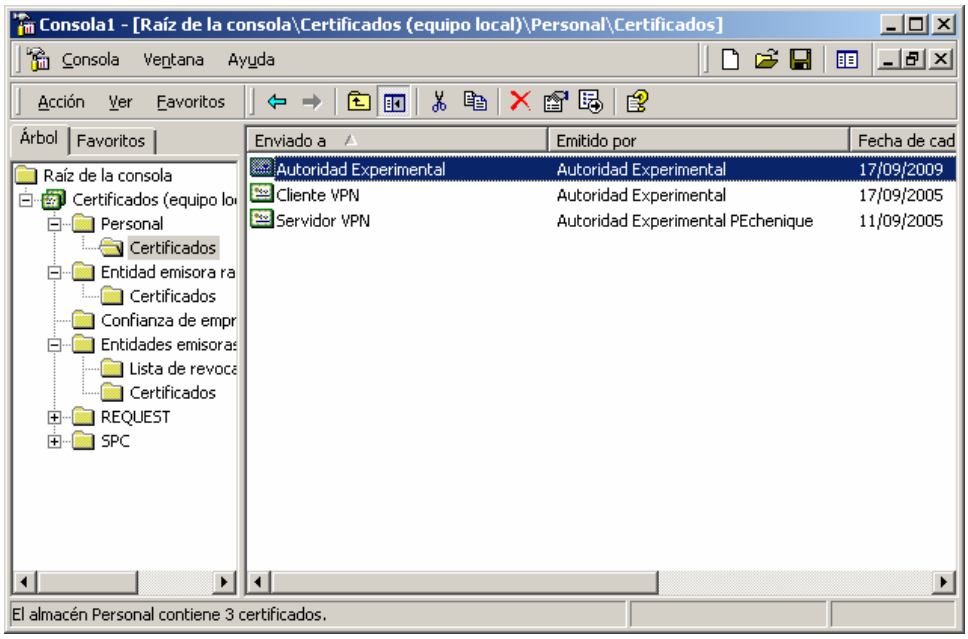


Paso 3: (Servicio de Enrutamiento y Acceso Instalado)

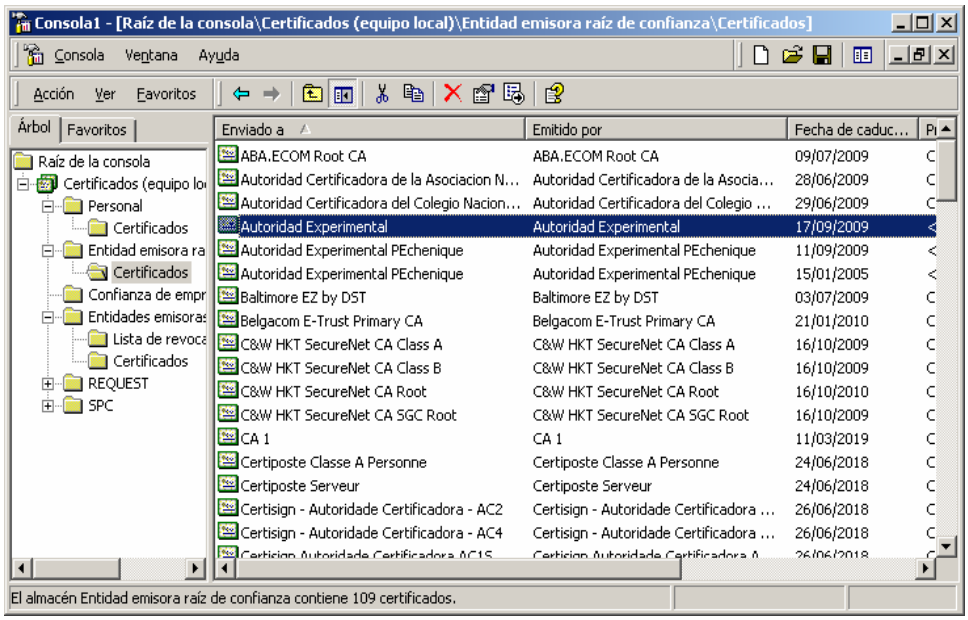


Finalizado el proceso de instalación del lado del servidor se procedió a instalar en el lado del cliente el software necesario para la VPN.

Paso 1: Verificación del Certificado (1)

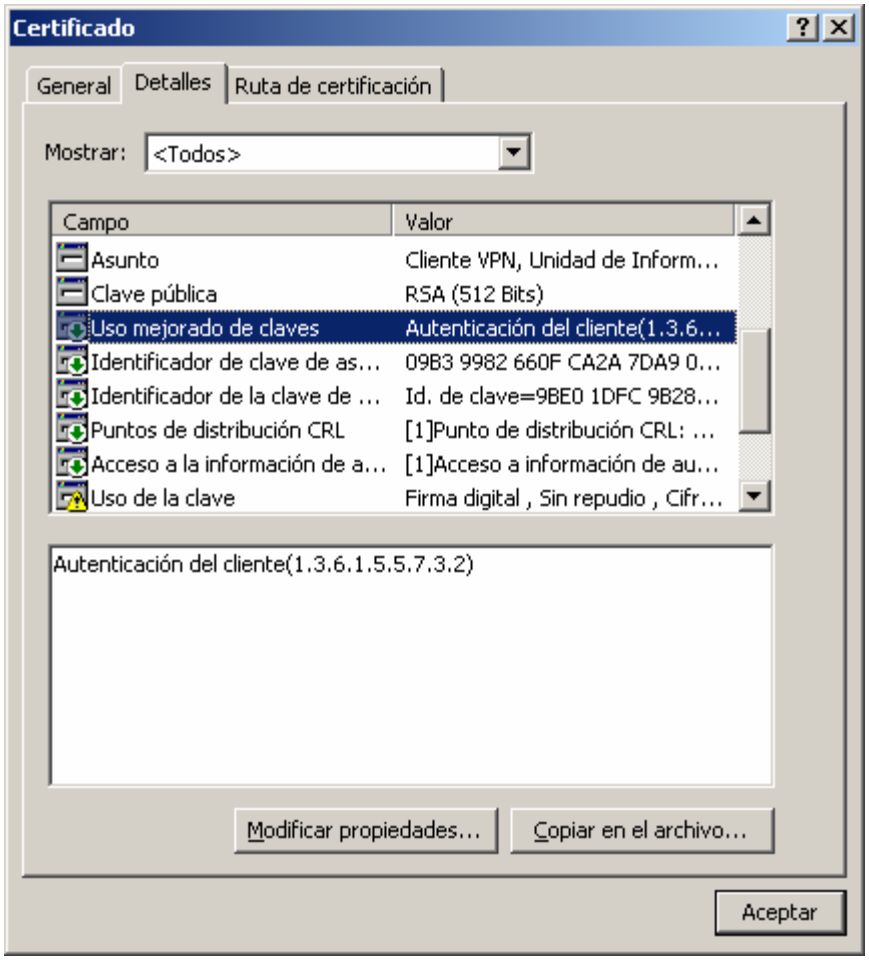


Paso 2: Verificación del Certificado (2)



Nota: Cabe destacar que la entidad emisora “Autoridad Experimental” debe quedar inscrita bajo la estructura Certificados(Equipo Local) \ Entidad Emisora Raíz \ Certificados, para que funcione la conexión vía IPSec.

Paso 3: Verificación del Certificado (3)

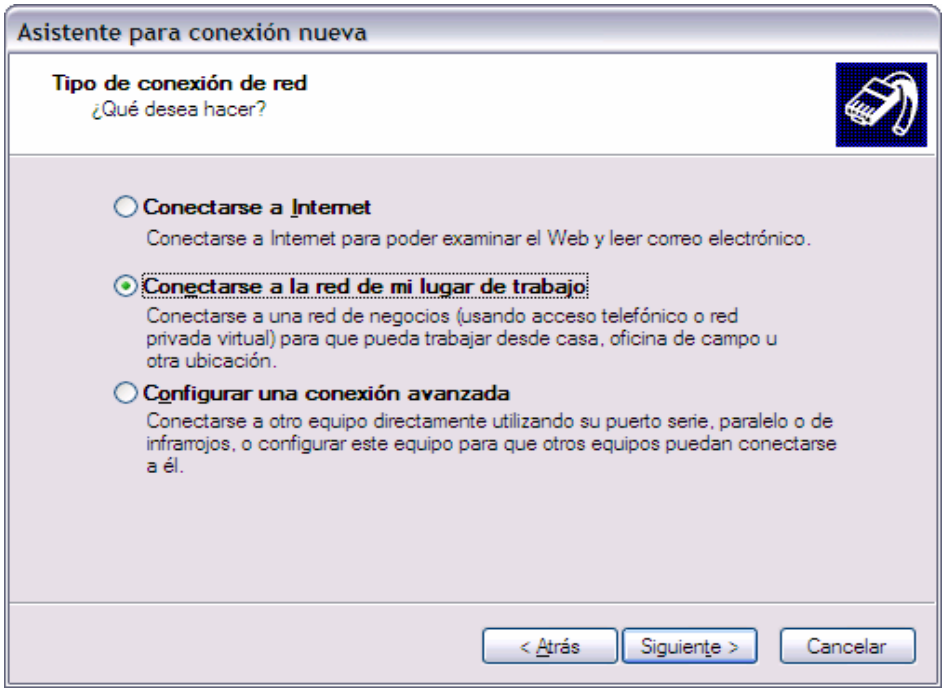


Completados todos los pasos anteriores ya están integrados todos los componentes a la infraestructura informática de FUNDELEC, para establecer la Red Privada Virtual que dará acceso al SISE.

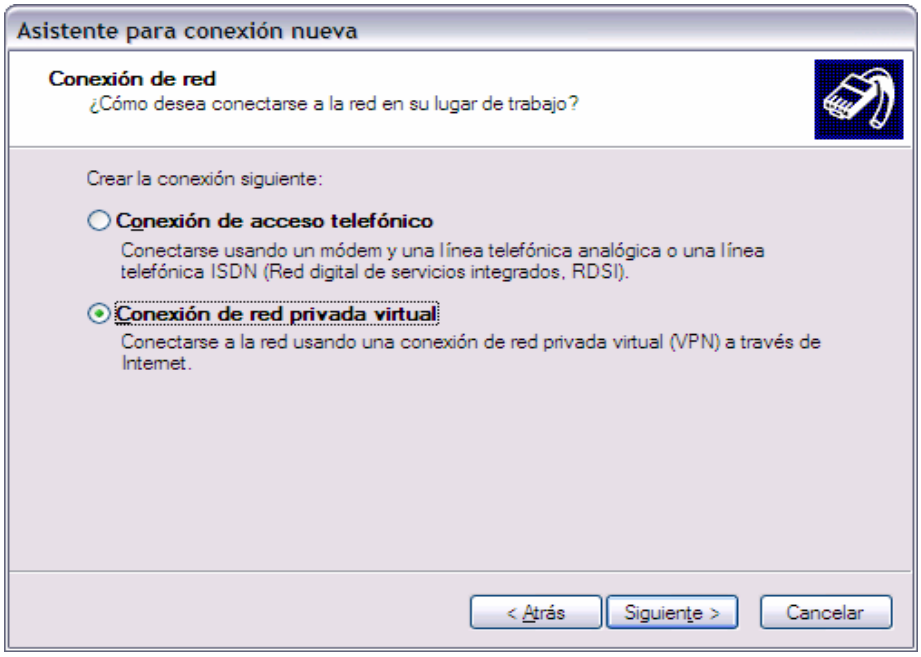
Quedando a sí constituida la red perimetral contentiva del servidor VPN “SERVERVPN” y el servidor de producción para el SISE “DC_FUNDELEC4”, lo que garantizará a los usuarios remotos la obtención de la información validada y comprobada por FUNDELEC.

4.6.- Entrenamiento para los Usuarios remotos del Sistema

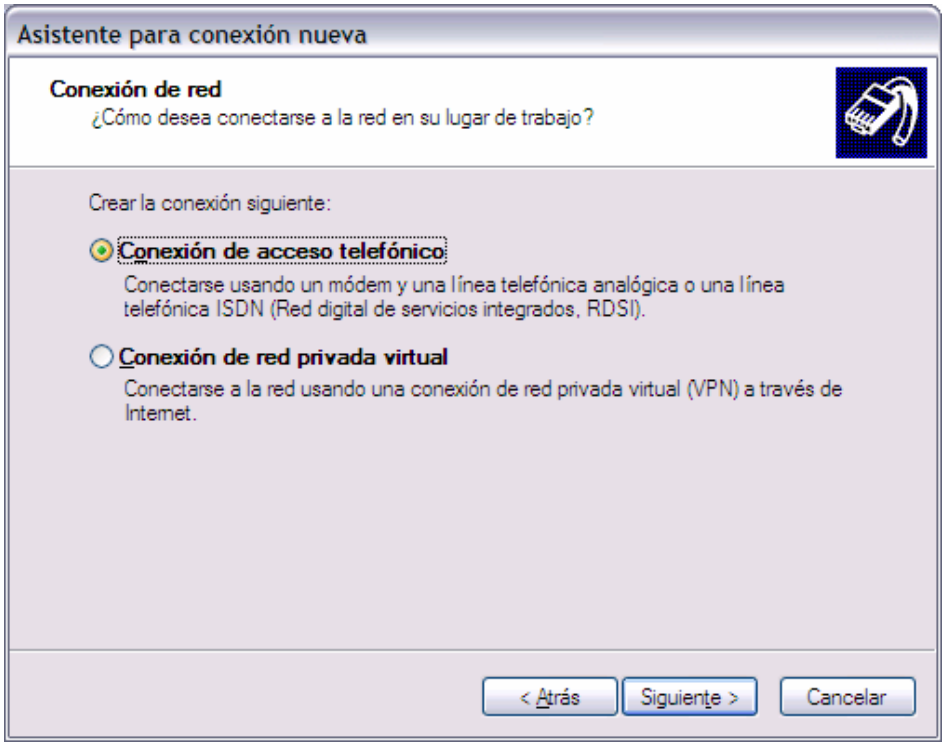
Paso 1: Creación de la Conexión Telefónica – A Través de Internet



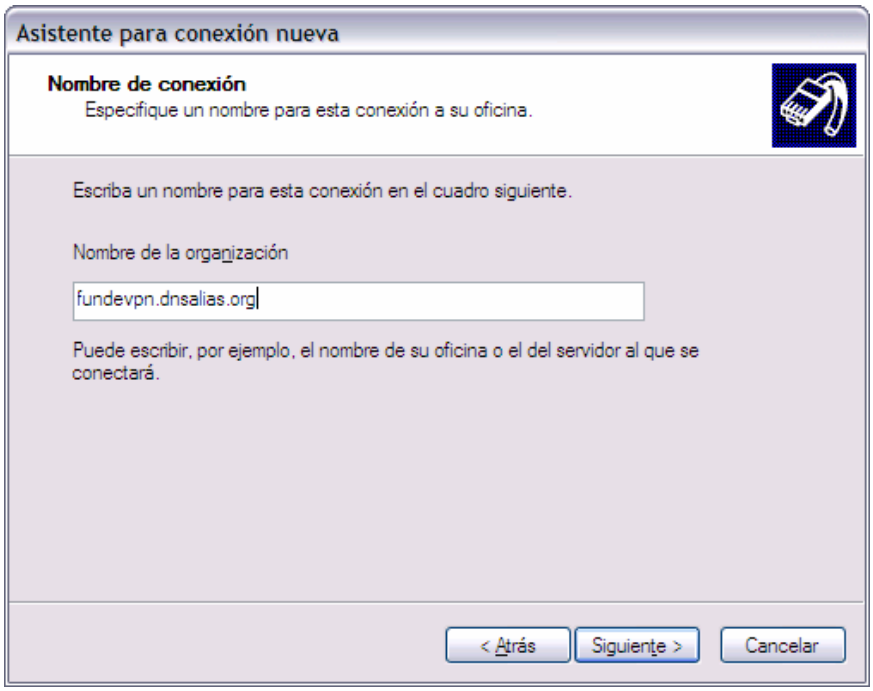
Paso 2: Creación de la Conexión Telefónica – A Través de Internet



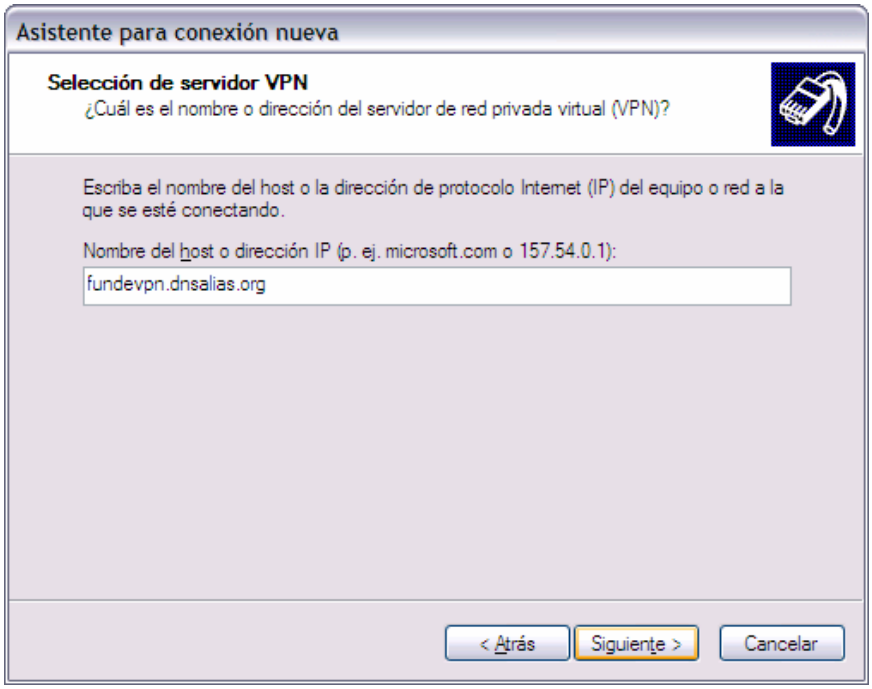
Paso 2: Creación de la Conexión Telefónica – A Través de Llamada Telefónica



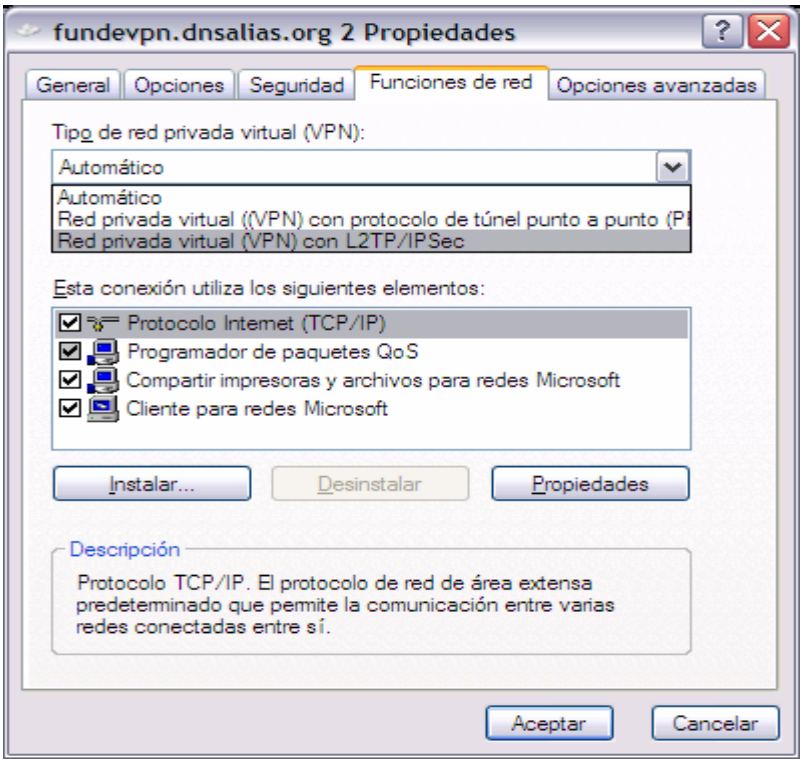
Paso 3: Creación de la Conexión Telefónica – A Través de Llamada Telefónica



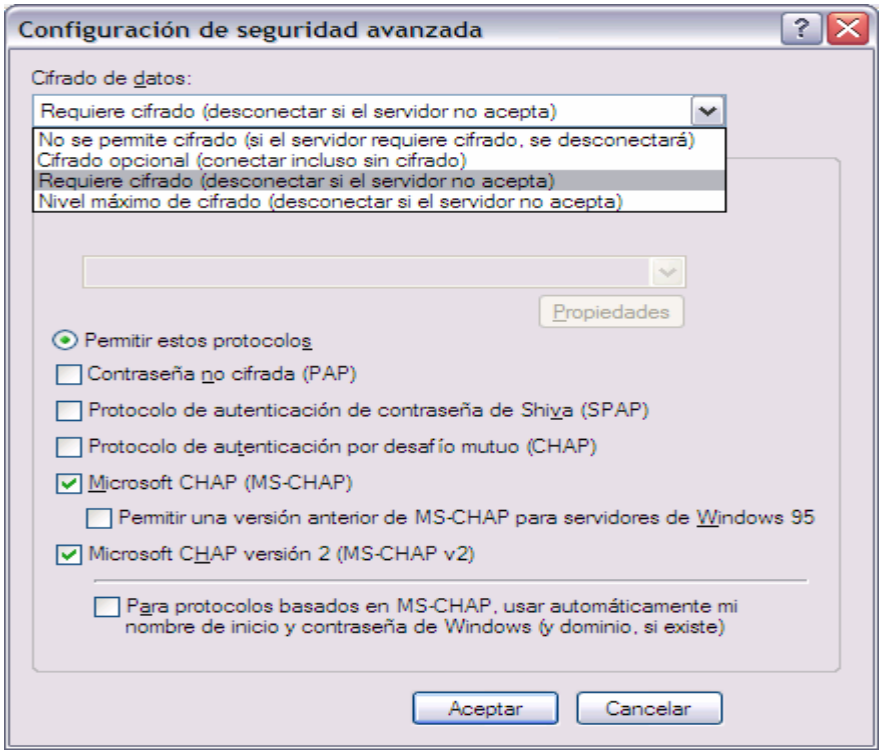
Paso 4: Creación de la Conexión Telefónica – Dirección del Servidor



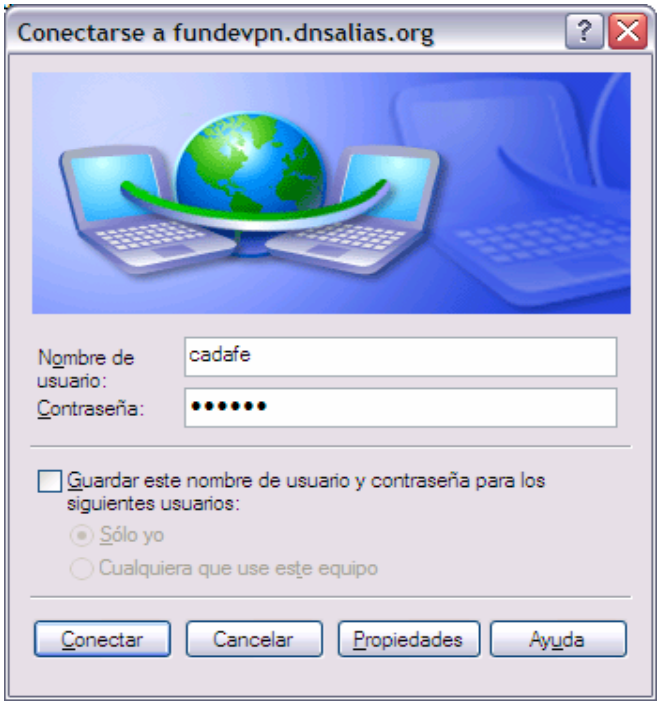
Paso 5: Creación de la Conexión Telefónica – Establecimiento de VPN con L2TP/IPSec



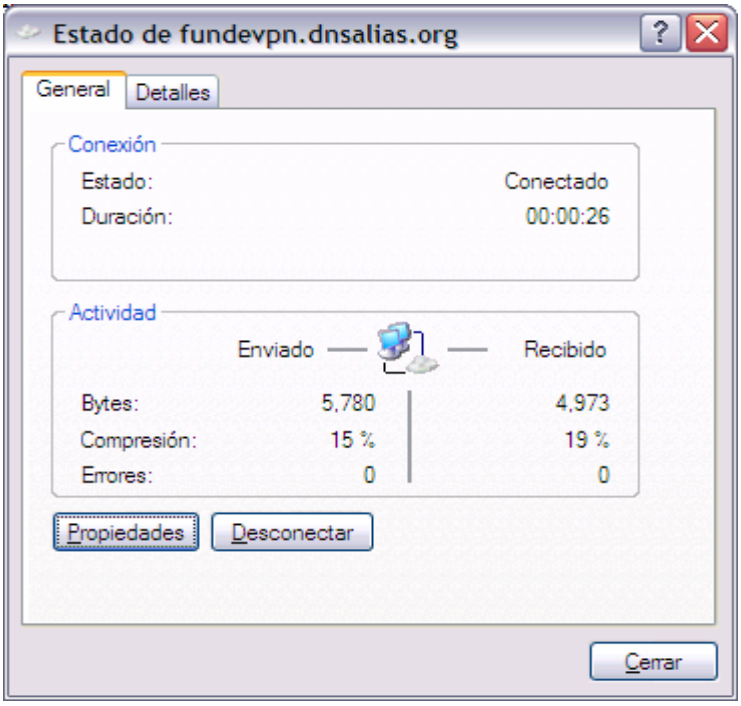
Paso 6: Creación de la Conexión Telefónica – Requerir certificados



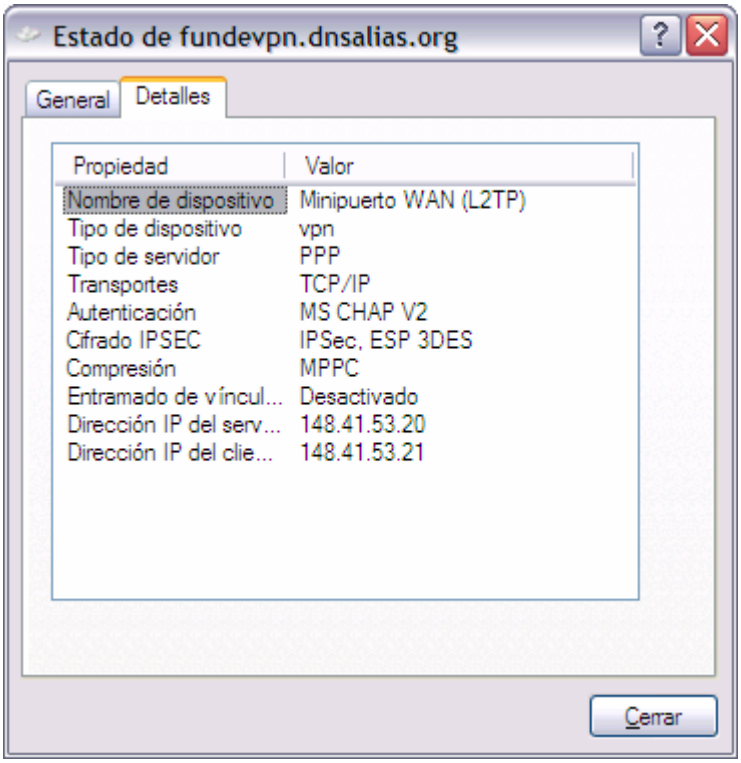
Paso 7: Establecimiento de Sesión – Usuario Cadafe



Paso 8: Establecimiento de Sesión – Usuario Cadafe



Paso 9: Establecimiento de Sesión – Usuario Cadafe



5.- Conclusiones

A lo largo del desarrollo del presente Trabajo Especial de Grado se ha estudiado la necesidad de disponer de la información contenida en el SISE a aquellos usuarios que se encuentran fuera de la sede de operaciones de FUNDELEC, y así, proveerles los mecanismos para la recolección, actualización y consulta de los indicadores, y características descriptivas de las áreas de operación de las Empresas Eléctricas Venezolanas, tales como: Generación, Distribución, Substransmisión, Comercialización, entre otras.

Todo ello, conforme a las políticas y restricciones de acceso establecidas para cada perfil de usuario de acuerdo al nivel de accesibilidad que tenga lugar a cada uno de los componentes operacionales del SISE.

Por tanto, se sustentó el desarrollo de la presente investigación, con base a el creciente uso y presencia mundial de implementaciones de Redes Privadas Virtuales (VPN's) como medio seguro para compartir información y recursos informativos (Bases de datos, aplicaciones, servidor de correo, entre otros) a través de la Internet.

En cuanto a la estrategia de implementación de la "Red Privada Virtual para el acceso seguro y controlado al SISE", el esquema físico y lógico de Interconexión fue determinado por la creación de una red perimetral ó DMZ, con el uso de un nuevo servidor, lo cual específica el ámbito de control y seguridad del SISE en modo producción, donde se obtienen los siguientes beneficios:

1.- Los usuarios remotos sólo podrán acceder a una versión validada y revisada del SISE.

2.- La Plataforma Informática de FUNDELEC no estará expuesta a usuarios que sean autorizado para el uso del SISE, pero no así para el acceso a

aplicaciones e información inherente sólo a las áreas internas de la organización.

En lo referente al método de Conexión de la Red Privada Virtual, lo cual determina el protocolo estándar para las conexiones remotas, se seleccionó el uso de “IPsec”, de acuerdo a la capacidad de integración con el árbol de directorio (Base de Datos de Usuarios) de Windows 2000 sistema donde está desarrollado el SISE.

De igual manera, IPSec es compatibile con los sistemas operativos estándares para la línea de servidores tales como: Linux, FreeSBD, Windows 2003, entre otros. Todo ello a través de los protocolos LDAP y Kerberos. Lo que hace de ésta solución portable y expandible en las plataformas mencionadas

Dado, a que el SISE a diferencia de los sistemas de información convencionales, es una implementación de un conjunto de herramientas que operan de forma aislada y cuyo único punto de interconexión es el sistema operativo del servidor, la forma más adecuada de transferir la información del usuario remotos para llevar a cabo el proceso de identificación, autenticación y autorización, es transportando dicha información desde el token “Etiqueta” de la conexión al sistema operativo y luego el sistema operativo reporta a cada elemento del sise el usuario activo.

Por tanto, la selección de IPSec como método para el establecimiento del túnel para la transferencia segura de información desde ó hacia el SISE, constituyó el factor fundamental para el desarrollo de la matriz de acceso y seguridad (ACL’s) de los usuarios en cada uno de los módulos de operación que integran al SISE, tales como: a) Base de Datos; b) Cubos OLAP; c) Index Server; d) Árbol de directorios; lo que permite establecer de forma centralizada grupos de usuarios para conceder el acceso a consultas y/o módulos específicos a cada perfil.

Dicho esquema entonces es extensivo a las conexiones remotas efectuadas vía Red Privada Virtual, transfiriendo los datos del autenticación del usuario a través de LDAP ó Kerbero a las ACL’s de Windows 2000.

Asimismo, es de notar que se estima un universo de usuarios remotos controlados y reducido, es decir, sólo aquellos usuarios que Fundelec autorice para el uso del sistema podrán accederlo vía Internet ó a través de una llamada telefónica, por lo que, su instalación en el lado del cliente no debe ser un obstáculo para la implementación.

Por tanto, los beneficios aportados a FUNDELEC con el desarrollo del presente trabajo, se remontan al hecho de poder establecer una vía de comunicación segura, confiable y compatible con los estándares utilizados en Internet, entre las empresas eléctricas ←→ MEM-FUNDELEC y MEM-FUNDELEC ←→ Agentes del sector, lo que acelerará el proceso de intercambio de información y por ende se dispongan de más herramientas para la reestructuración, organización y proyección nacional e internacional del Sector Eléctrico Venezolano.

Referencias **B**ibliográficas

Understanding Virtual Private Networking, Adtran, 2001

Virtual Private Networks: Technologies and Solutions, Ruixi Yuan,Timothy Strayer, 2002

Creating and Implementing Virtual Private Networks, Casey Wilson y Peter Doak, 2004

Firmas Digitales, Puig de la Peña Iván, 1997

Acceso remoto y VPN, Vincenzo Mendillo, Febrero 2001.

Implementing Virtual Private Networks, Steven Brown, McGraw-Hill Book Co., 1999.

Intranets and Virtal Private Networks, PSINet, 2000.

Virtual Private Networking: An overview, Microsoft Corporation, 2000.

Intranets and Virtual Private Networks (VPNs) Tutorial, The International Engineering Consortium, January 1999.

Methods and protocols for secure key negotiation using IKE, Michael S. Borella, *IEEE Network*, July/August 2000.

Virtual Private Networking with Windows Server 2003, Microsoft Corporation, 2003.

Windows 2000-based Virtual Private Networking: Supporting VPN interoperability, Microsoft Corporation, 2000.

How to build secure LANs with IPSec, Jerry Ryan, The Applied Technologies Group, Inc., 2001.