ANEP

Consejo de Educación Secundaria

Informe Técnico

Sistema de control y seguimiento de gastos en Centros Educativos

Abstract

El presente documento expone detalladamente los trabajos realizados en el marco del proyecto de grado “Sistema de control y seguimiento de gastos en Centros Educativos” realizado para el Consejo de Educación Secundaria.

El cual brinda un marco integral que permite resolver los problemas de generar aplicaciones de alcance Nacional en un organismo con escasos recursos para su instalación y mantenimiento operativo, mostrando la aplicación practica de las técnicas utilizando el desarrollo, instalación y mantenimiento de una aplicación particular: “Control y seguimiento de gastos en Centros Educativos”.

En el presente documento se expondrá el perfil institucional, la infraestructura de comunicaciones, propuestas realizadas en cuanto a conectividad, estudios de contingencias, consideraciones para el desarrollo de aplicaciones en el marco del organismo, estudios sobre herramientas de instalación, administración y monitoreo remoto, así como las conclusiones generales del proyecto, consideraciones sobre trabajos futuros y apéndices sobre confidencialidad sobre redes publicas así como la utilización de antivirus en una Wan[1].

Se complementa con la documentación de la aplicación desarrollada y el correspondiente manual de usuario, además se dispone del documento llamado “Introducción general” cuya lectura en primer termino es recomendada.

[1] Wide Area Network ver [1]

Índice

Tabla de Ilustraciones

1 Introducción

El presente documento introduce en profundidad los aspectos técnicos de las metodologías, herramientas y técnicas estudiadas en el marco del proyecto “Control y seguimiento de gastos en Centros Educativos”.

Se recomienda en primer término la lectura del documento “Informe General”, que introduce al proyecto en toda su extensión. Como se expuso en dicho documento el proyecto atravesó dos etapas claramente diferenciadas, en la primera etapa se disponía de una red wan con conexiones de baja calidad, en la segunda etapa dicha red evoluciona hacia una red wan con conexiones de alta calidad.

El cambio en las características de las comunicaciones disponible provocó que algunos objetivos cambiaran, de forma de resolver mejor los desafíos planteados al comienzo del proyecto.

Sin embargo lo trabajado en la primer etapa del proyecto no solo sirvió como base del trabajo realizado en la segunda etapa, sino que algunas contribuciones tienen valor propio y permanente por si mismas, como ser por ejemplo el relevamiento de conectividad y la primer propuesta presentadas en los capítulos 3 y 4. Otras de las contribuciones serán sin duda piedras angulares de futuros trabajos que apunten a brindar alternativas a la solución existente como ser por ejemplo el modelado teórico presentado en el apéndice 8.5.

En el capitulo siguiente introduciremos los objetivos del proyecto así como un desarrollo en profundidad de los mismos.

A continuación comienza el primer gran tomo de este documento denominado “Primera Etapa”, dicho tomo formado por los capítulos 3 y 4 donde se introduce el “relevamiento de la infraestructura de comunicaciones” y la “primer propuesta”, dos aportes importantes para el organismo generados en esta etapa.

El relevamiento introduce en primer término un perfil institucional para que el lector tome conocimiento del contexto en el que se trabajara para luego si profundizar en la infraestructura de comunicaciones.

Como consecuencia directa del capitulo anterior se presenta la primer propuesta en materia de comunicaciones documento fundamental que fue uno de los ingredientes en el cambio en materia de comunicaciones del organismo.

A continuación comienza el segundo tomo denominado “Segunda Etapa”, el mismo esta formado por los capítulos 5,6 y 7.

En el capitulo 5, Contingencias, se introducen los riesgos mas importantes que se podrían producir en un sistema que apuntara a ser utilizado a nivel nacional en el ente, así como estrategias para su minimización.

A continuación, en el capítulo 6, con la misma óptica genérica se procede a analizar las ventajas y desventajas de diversos entornos de programación para el desarrollo de aplicaciones destinadas a Centros Educativos.

Como se vio en la introducción la falta de herramientas adecuadas de implantación, instalación, actualización y control remoto fueron importantes factores en el fracaso de intentos anteriores, es en base a está consideración que se introduce el capitulo 7, Herramientas, en dicho capitulo se introducirán primeramente las herramientas de instalación y actualización para continuar luego con las herramientas de administración y control remoto.

Finalmente en el capitulo 8, Apéndices, se analizaran diversos temas, comenzando con un completo análisis de antivirus para Centros Educativos, punto que no debe faltar en ninguna estrategia de implementación a gran escala, a continuación se presenta un trabajo introductorio al tema de VPN, tecnología que deberá ser estudiada a fin de asegurar la confidencialidad de las comunicaciones utilizadas por el organismo. Ademas se incluyen una completa referencia a la programación de la herramienta NSIS, herramienta seleccionada en el capitulo 7.1.3 como el instalador ideal para el Consejo de Educación Secundaria.

El capítulo Apéndices finaliza con una serie de trabajos donde se muestra el rumbo original del proyecto en un contexto de wan con conexiones de baja calidad, incluyendo la solicitud original del proyecto, la ampliación del mismo así, como el modelado teórico, trabajos que deberían ser retomados en caso de que la realidad en comunicaciones volviera a cambiar o se quisiera disponer de alternativas para el caso de contingencias.

2 Objetivos

2.1 Introducción

Este proyecto fue presentado en el mes de Febrero del 2003. Se comenzó a trabajar en el mismo en el mes de Julio del mismo año.

El Consejo de Educación Secundaria solicito el desarrollo de un sistema de "Control y seguimiento de gastos en Centros Educativos", sistema a ser implantado a lo largo de todo el País, que contemplara la realidad del organismo de forma de minimizar los costos de implantación y operativos del sistema.

Como fue expuesto en el documento "Informe General", al comienzo del proyecto se determino que seria beneficioso realizar una investigación mas profunda sobre el desarrollo de aplicaciones y flujo de datos en una Wan desconexa[2], sin embargo a lo largo del proyecto se produjeron cambios de importancia en la infraestructura de comunicaciones.

Dichos cambios determinaron un antes y un después en el desarrollo del proyecto, por lo que se puede hablar de dos etapas claramente diferenciadas en el mismo, en el documento "Informe General" se expuso extensamente cuales eran las características de los objetivos originales, y como estos objetivos se transformaron a lo largo del proyecto, a continuación se presentaran los objetivos finales, con un detallado análisis de los mismos.

2.2 Objetivos

Por los motivos expuestos en la introducción, es decir el cambio en la realidad de las posibilidades de la infraestructura de comunicaciones del organismo, los objetivos finales del proyecto se transformaron en los siguientes:

- **Estudiar la infraestructura de comunicaciones del Consejo de Educación Secundaria**
- **Proponer estrategias de desarrollo de aplicaciones a ser utilizadas en todo el País**
- **Proveer mecanismos de instalación y actualización de aplicaciones a través de una Wan de alcance nacional**
- **Proporcionar mecanismos de control y monitoreo de aplicaciones remotos**
- **Crear el sistema de "Control y seguimiento de gastos en Centros Educativos"**

[2] Se llamo Wan desconexa a la wan disponible en primer termino en el ente, ya que la mayoría de sus nodos no estaban permanentemente conectados

Es decir se busca un enfoque integral que permita resolver los problemas de generar una aplicación de alcance Nacional en un organismo con pocos recursos para su instalación y posterior mantenimiento.

Claramente el primer objetivo es de importancia vital para tomar decisiones racionales en cuanto al desarrollo de aplicaciones distribuidas, es en base a un conocimiento certero de la infraestructura disponible que se podrá determinar la estrategia mas conveniente a la hora de desarrollar aplicaciones que justamente descansen en dicha infraestructura a pesar de la obviedad de este razonamiento dicho relevamiento no existía en el ente.

Dicha estrategia deberá ser integral contemplando por ejemplo los riesgos de la solución planteada, así como estrategias para superarlos.

Paralelamente se debería contar con herramientas y mecanismos que permitieran instalar, dar soporte y monitorear a una red de alcance nacional sin disponer de técnicos en todos los puntos del país, esto es proveer mecanismos de instalación, control y monitoreo remotos.

Finalmente se plasmara lo estudiado con la aplicación de "Control y seguimiento de gastos en Centros Educativos", tal cual fue solicitado por el Consejo de Educación Secundaria.

A continuación se desarrollara cada uno de los objetivos y su interrelación.

2.3 Primer objetivo

"Estudiar la infraestructura de comunicaciones del Consejo de Educación Secundaria"

Se busca conocer y documentar la realidad del organismo en lo que a comunicaciones se refiere.

Dicho objetivo modesto en principio tiene fundamental importancia dado que cuando se comenzó a trabajar en este proyecto no existía información escrita sobre la infraestructura de comunicaciones, parte de la información estaba distribuida entre los técnicos que habían trabajado en tal o cual conexión, parte estaba dispersa en otros organismos, parte se había olvidado y parte nunca se había estudiado.

Realizando este relevamiento se encontraron algunas sorpresas, como por ejemplo el caso de los liceos con RuralCel[3] , en todas las discusiones y análisis eran nombrados como el gran problema y tomados como escollo para la instalación de aplicaciones en red, sin embargo el organismo ignoraba la cantidad de liceos que tenían este tipo de teléfonos, y tampoco fue fácil el obtener la información de Antel que permitió contarlos, para descubrir que la cantidad de liceos en estas condiciones era insignificante.

[3] Teléfono celular utilizado por Antel en áreas rurales que se caracteriza por las dificultades que presenta a la hora de transmitir datos digitales.

2.4 Segundo objetivo

" Proponer estrategias de desarrollo de aplicaciones a ser utilizadas en todo el País"

Aquí se busca por ejemplo analizar entornos de desarrollo, modelos de replicación de datos, análisis de riesgos, estrategias de implantación, etc. genéricas mas allá de la aplicación concreta a desarrollar, es decir trabajar con un marco general que disminuya la necesidad de análisis de estos aspectos para cada aplicativo concreto a desarrollar.

2.5 Tercer objetivo

"Proveer mecanismos de instalación y actualización de aplicaciones a través de una wan de alcance nacional"

En el análisis post mortem[4] de otros proyectos que intentaron implantarse en los ámbitos liceales se detecto que el descuido a la hora de planificar la instalación y sobre todo la posterior actualización de los sistemas instalados generó dificultades considerables.

La falencia en la planificación de la instalación de parches provocó en lo inmediato que no existieran canales de distribución de los mismos, por lo que cuando fue necesario se debió recurrir al Correo Nacional con las previsibles demoras, además al no haber planificado la instalación misma del parche el proceso era simple para un técnico, pero sumamente difícil para un funcionario de liceo.

Estas dificultades desembocaron luego en otras mas graves como fue el hecho de que existieran diversas versiones de los sistemas funcionando[5] que volcaban información a los sistemas centrales con sus propias peculiaridades debido a su versión, haciendo mas complicado el proceso dado que por esto mismo no era posible aplicar correctivos genéricos a los datos recibidos.

Por todo lo expuesto se considera prioritario un detallado estudio de las alternativas existentes en el campo de los instaladores de aplicaciones, determinar las necesidades del organismo, y automatizar en lo posible la solución elegida.

[4] En particular de la implantación del nuevo sistema de liquidación de sueldos, análisis realizado por un equipo encabezado por el autor de este proyecto ver [8]
[5] A raíz de la demora en la distribución e instalación la misma no era uniforme

2.6 Cuarto Objetivo

"Proporcionar mecanismos de control y monitoreo de aplicaciones remotos"

Cuando se producen dificultades (y estas se producen no importa lo bien planeado que este el aplicativo, su instalación o la plataforma utilizada) se debe prestar ayuda técnica, comúnmente denominada "soporte".

El problema es que cuando las instalaciones están distribuidas a lo largo y ancho del País es muy costoso y a veces imposible[6] enviar técnicos a cada lugar físico, por lo que es adecuada una estrategia basada en administración remota a la hora de diagnosticar y solucionar el inconveniente.

Se plantea por lo tanto el estudio y comparación diversos sistemas de manejo remoto de equipos, de forma de minimizar los desplazamientos del personal de soporte con la intención de reducir los costes asociados a estos, así como también aumentar la disponibilidad del personal ya que si este se encuentra concentrado en un lugar con conexión simultanea a los Centros Educativos en un momento dado pueden atender mas llamadas y solucionar mas problemas que si se están desplazando por toda la Republica.

2.7 Quinto objetivo

"Crear el sistema de Control y seguimiento de gastos en Centros Educativos"

Se debe realizar el análisis e implementación del sistema en cuestión probando las estrategias presentadas a lo largo de todo el proyecto.

[6] Por razones presupuestales en determinados periodos del año es muy difícil conseguir rubros para solventar viáticos, pasajes, etc.

Primera Etapa

Como se ha expuesto en la introducción el proyecto puede ser divido en dos etapas claramente diferenciadas, en la primera la infraestructura de comunicaciones se destacaba por sus conexiones de baja calidad. En cambio en la segunda etapa dichas conexiones se caracterizan por su confiabilidad y alta calidad.

Dichos cambios provocaron una adaptación o evolución de los objetivos primarios, sin embargo mucho de lo investigado en esta primera etapa demostró ser un aporte fundamental al organismo en si y a este proyecto en particular.

A continuación se presentaran dos de los aportes más interesantes de esta primer etapa, aunque es importante señalar que los aportes de esta primer etapa no se agotan aquí, como parte de los objetivos permanecieron encontramos documentos, que generados originalmente para esta etapa se encuentran en la segunda parte de este informe pues fueron finalizados en la segunda etapa del proyecto, este es el caso por ejemplo de las herramientas de instalación.

Además de los estudios que fueron continuados en la segunda etapa y que por lo tanto se presentan en el tomo correspondiente, hay algunas contribuciones que no tienen utilidad inmediata, como ser por ejemplo el modelado teórico, pero no hay duda que estas contribuciones tendrán una importancia fundamental a la hora de estudiar alternativas a la realidad actual o para el estudio de planes de contingencia ya que son el punto de partida de posibles estudios de alternativas, estos aportes se encuentran en el capitulo de apéndices.

3 Relevamiento de la infraestructura de comunicaciones

3.1 Introducción

El presente capitulo expone la situación al comienzo del proyecto en relación a la conectividad existente entre el Centro de Cómputos del Ces y el resto de los nodos a ser contemplados en el proyecto.

Como ya ha sido expuesto se carecía de un relevamiento completo que detallara la infraestructura de comunicaciones del organismo, lo cual era un escollo insoslayable a la hora de planificar soluciones serias que se implantaran mas allá de la Lan de las oficinas centrales.

Primeramente se introducirá al organismo como tal para luego realizar un detallado relevamiento en cuanto a su realidad en el campo de las comunicaciones.

Para mantener la lógica del proyecto se presentara la realidad en cuanto a comunicaciones tal como se encontró al comienzo del proyecto para introducir su evolución en el epilogo.

3.2 Objetivo

Introducir el estado de la infraestructura de comunicaciones existente en el Consejo de Educación Secundaria, no es objetivo de este documento el proponer solución a los problemas planteados, sino tan solo plantear parte de los mismos y actuar como entrada al escenario del proyecto

Finalmente se caracterizará los distintos tipos de nodos a conectar teniendo en cuenta topología y arquitectura existente.

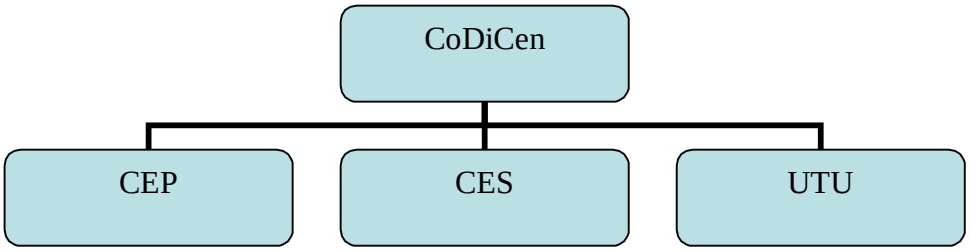
3.3 Perfil institucional

3.3.1 Descripción

El Consejo de Educación Secundaria[7] es el organismo del Gobierno Uruguayo encargado de regular la Educación Secundaria impartida en el País, así como de dictar los cursos correspondientes de forma gratuita cumpliendo con el mandato constitucional del derecho a la educación

Jerárquicamente depende del Consejo Directivo Central[8] , a pesar de lo cual tiene independencia administrativa por lo que es capaz de funcionar autónomamente regulado por las normas y dirigido por una junta de tres personas denominada "Consejo".

Junto a la UTU encargado de la formación técnica profesional y el CEP encargado de la formación primaria forma el núcleo de la ANEP (Administración Nacional de Educación Publica) que se completa con el CODICEN, superior jerárquico de los tres organismos (denominados "desconcentrados").



Estructura de la Anep.

Sin embargo esta estructura fue creada en tiempos relativamente recientes, antiguamente cada uno de los tres desconcentrados existía en forma totalmente autónoma, y el CoDiCen ni siquiera existía[9], por lo que los tres desarrollaron infraestructuras y culturas organizacionales distintas, lo que a su debido tiempo se tradujo en estructuras informáticas distintas y desconexas.

3.3.2 Dimensiones del organismo

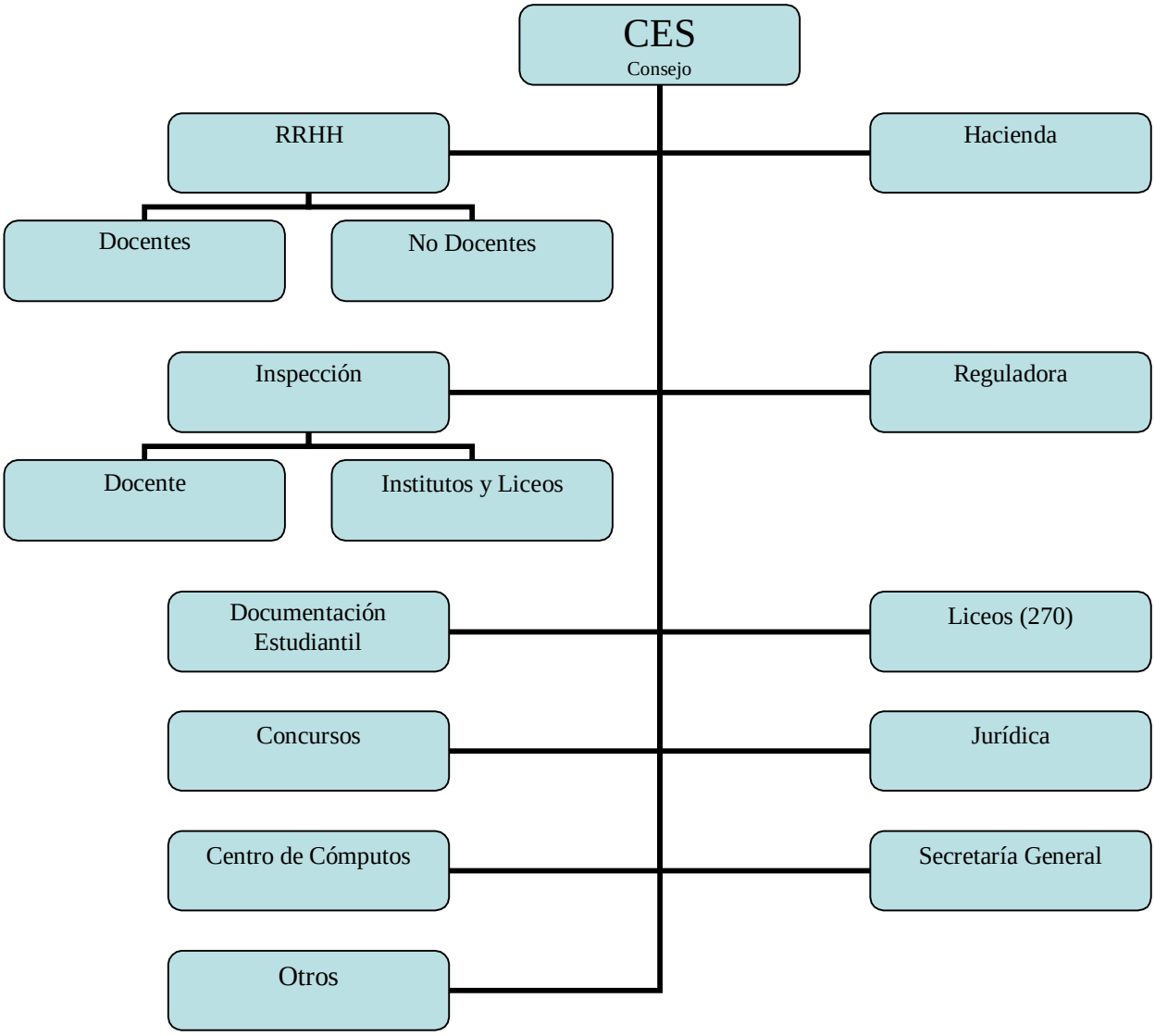
El CES cuenta con aproximadamente 20,000 funcionarios, dicha plantilla esta compuesta por unos 15,000 profesores y unos 5,000 empleados administrativos y de servicio.

Presta servicios a cientos de miles de personas por año (alumnos) de los cuales debe preservar información indefinidamente.

[7] CES de aquí en más.
[8] CODICEN de aquí en más.
[9] Creado con el nombre de Conae en enero de 1973.

3.3.3 Estructuración del organismo

Haremos un somero análisis de los departamentos y divisiones mas importantes del desconcentrado sobre todo desde el punto de vista de flujo de datos.



Organigrama del CES

Como se aprecia en el organigrama el CES se subdivide en varias dependencias, como gran organización que es, tiene multitud de departamentos y oficinas, en este diagrama se han indicado solamente las oficinas mas importantes desde el punto de vista de necesidades

informáticas y flujo de datos, al resto se las ha agrupado genéricamente, sin embargo a simple vista se desprende un gran problema, y es la dispersión los nodos, en efecto los 270 nodos (liceos) en los cuales esta distribuidos mas del 80% del funcionariado total se encuentra cada uno en un lugar físico distinto a lo largo y ancho de todo el país.

El panorama es peor si se considera que de el diagrama anterior de once oficinas, tan solo 3 se encuentran en el mismo lugar físico en el que se encuentra el consejo, cada una de las otras se encuentra en distintos edificios repartidos por todo el Centro y Ciudad Vieja de la ciudad de Montevideo, además las pequeñas reparticiones agrupadas en “otros”, agregan otra cantidad de departamentos y oficinas repartidas por la ciudad.

3.3.4 Flujo de datos

A continuación se detallaran los flujos de datos mas importantes sin tener pretensiones de totalidad.

3.3.4.1 Flujo a nivel de organismos dentro de la ANEP

Los flujos a nivel de organismo más importantes se dan de la siguiente forma:

Del CEP al CES, todos los pases de alumnos de enseñanza primaria a enseñanza secundaria.

Del CES a UTU y viceversa los pases de alumnos de ambos desconcentrados.

Del CES a CODICEN, información varia.

3.3.4.2 Flujo dentro del CES

La información en general fluye desde los liceos a las oficinas centrales en determinadas épocas y se da el flujo inverso en otras, por ejemplo desde los liceos a las oficinas centrales viajan la actuación del alumnado, las tomas de posesión de los docentes, etc., desde las oficinas centrales viaja la distribución de alumnos al comienzo del año, los planes de estudios, etc.

Si bien no tenemos en general flujo intra liceal, si tenemos un alto flujo de datos internamente entre las oficinas centrales, como se recordará estas se hallan distribuidas por el Centro y ciudad vieja de la Ciudad de Montevideo por lo que nuevamente se presentan problemas de conectividad.

3.4 Infraestructura de comunicaciones existente

3.4.1 Introducción

La infraestructura de comunicaciones del CES ha evolucionado en base a la solución de necesidades puntuales a veces incluso por iniciativas de otros organismos y en distintos momentos en el tiempo, todo esto ha tendido a que la infraestructura se fragmente o no se complemente.

Se puede dividir en dos grandes bloques, comunicaciones internas al organismo y comunicaciones externas, por ejemplo con el Codicen.

Dentro de las comunicaciones internas al organismo existen tres grandes núcleos, Liceos, Oficinas ubicadas en los edificios centrales del Consejo y otras oficinas.

Las comunicaciones externas, se pueden agrupar en dos categorías, Internet y a la ANEP.

A continuación se analizarán estas categorizaciones.

3.4.2 Comunicaciones internas al organismo

3.4.2.1 Oficinas ubicadas en los edificios centrales

Este es el núcleo informático operativo del CES, parte de una iniciativa del propio organismo por dotarse de una infraestructura de comunicaciones y físicamente se extiende a través de dos edificios adyacentes.

Es una Lan de 10/100 mbps, con protocolo TCP/IP sobre servidores NT 4.0 con aproximadamente 300 puestos de trabajo

A su vez es el nodo que se encuentra conectado a internet a efectos de proporcionar correo electrónico.

3.4.2.2 Otras oficinas

Se trata de oficinas pequeñas a medianas, con cantidades de terminales que varían desde dos a cincuenta.

La mayoría de estas oficinas se hayan desconectadas de la red central, pero en este momento se esta implementando la incorporación de las cinco mas importantes a través de bridges sobre adsl con velocidades que oscilan entre los 128 y 256 kbps según la oficina, todas estas conexiones están multiplexadas en una única conexión de 512 kbps que las conecta a la red central.

El protocolo sobre el que trabajan es nuevamente TCP/IP, pero aun no se ha determinado la manera más conveniente de funcionamiento, es decir si se instalaran servidores en estas oficinas, routers u otros dispositivos.

3.4.2.3 Liceos

Por las distancias involucradas es aquí donde se presentan mayores problemas.

Los liceos se pueden sub-dividir en tres categorías:

- Con aulas informáticas conectadas a Internet
- Liceos urbanos o con conexiones telefónicas de calidad
- Liceos con RuralCel

3.4.2.3.1 Liceos con aulas conectadas a Internet

Se utilizan tres tecnologías, ADSL, ISDN y Frame Relay, en general el ancho de banda de estas líneas es de 64 kbps pero han dado distinto resultados, en general el servicio ISDN ha sido mas difícil de administrar y los encargados del mismo están desconformes, esta situación no se da en el caso del ADSL y el Frame Relay, sin embargo en las entrevistas con los encargados se detectaron otros problemas en estos casos derivados en la imposibilidad de incorporar proxys en las redes de estas aulas. En efecto, las 15 o 20 maquinas navegan a través de una sola que hace NAT, por lo que el ancho de banda es dividido en 20, sin contar con los beneficios que proporcionaría por ejemplo el cache de un proxy.

El problema radica en que por convenio estas conexiones son solo para internet es decir, AntelData asegura la conexión a internet pero no esta previsto que se usen para otra cosa, por ejemplo a excepción del Frame Relay, las puntas de las conexiones no llegan a Codicen.

Ninguna de estas redes está conectada al CES.

3.4.2.3.2 Liceos urbanos o con conexiones telefónicas de calidad

En estos casos se cuenta con módems de 56 kbps, estas líneas serian utilizadas con el servicio 0800ANEP, el cual podría ser conectado directamente a la lan del CES.

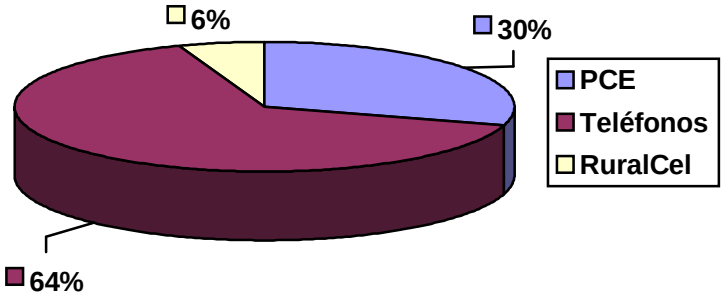
3.4.2.3.3 Liceos con RuralCel

RuralCel es el nombre comercial dado por Antel a la comunicación inalámbrica existente en el interior del País, básicamente son teléfonos celulares analógicos.

En este caso no se puede conseguir velocidades mayores a 4600 bps y lo que es peor dicha comunicación esta expuesta a frecuentes cortes, por lo cual este constituye el peor caso en cuanto a comunicaciones.

3.4.2.3.4 Resumen

En el siguiente grafico puede ser apreciada la composición de nuestras comunicaciones con los liceos.

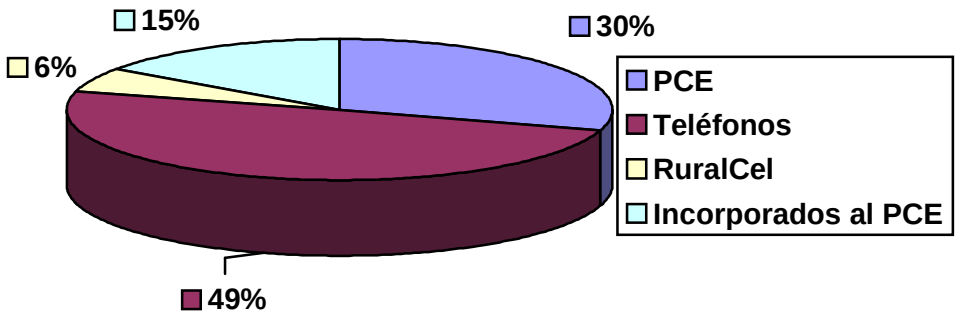


Composición de las comunicaciones Liceales

Aquí es importante señalar que el sistema RuralCel sera remplazado en los próximos años por la tecnología GSM [16] de mejores prestaciones a la hora de transmitir información.

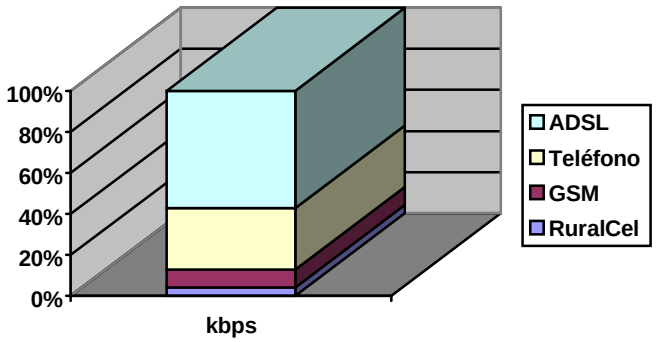
Por otro lado es muy importante señalar que el PCE crece sin pausa abarcando a la mayoría de los liceos de alta matricula. Este hecho se aprecia claramente en la siguiente grafica que

actualiza la anterior con los datos disponibles al 27/2/2004, en ella se aprecia claramente como en aproximadamente cuatro meses la cantidad de liceos conectados al PCE ha aumentado en un 50%.



Situación de Conectividad al finalizar el proyecto

En la siguiente grafica se realiza una comparativa entre los anchos de banda que brindan cada una de las soluciones planteadas



Ancho de banda de las conexiones Liceales

Claramente se aprecia la diferencia en cuanto a capacidad de transmisión, otro elemento a tener en cuenta es que fácilmente se puede cuadruplicar la capacidad de la conexión ADSL mientras el resto son tecnologías con "techo" es decir no pueden superar su velocidad máxima que es de 4 kbps para el caso de los Rural Cel, 9.6 Kbps para el caso de GSM[10], entre 33.6 y 56 kbps para línea telefónica[11] y para graficar un ejemplo se tomo un ADSL de 64 kbps.

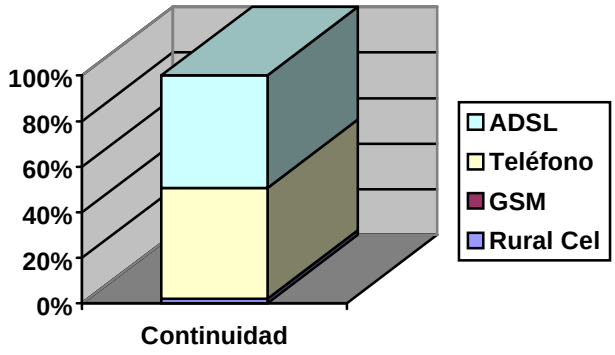
Pero las diferencias se acentúan aun mas si se considera la continuidad de la comunicación, en efecto las líneas ADSL están conectadas las 24 horas sin problemas, nuestras pruebas han

[10] Si se utilizan las prestaciones GPRS sobre GSM, el ancho de banda podria aumentar hasta 144kbps [17], sin embargo como se ignora el costo que tendrá en nuestro país en la grafica solo tomamos el ancho de banda mínimo

[11] Sin embargo por restricciones propias de la norma que tienen que ver con la línea telefónica, difícilmente se superen los 44 kbps en el caso de una línea telefónica promedio.

demostrado que difícilmente se pueda mantener una conexión Ruralcel por mas de una hora[12], es decir entre el periodo comprendido entre la primer y segunda hora se producirá un corte de la comunicación en cambio con conexiones telefónicas ordinarias nuestra experiencia ha demostrado que se pueden sostener conexiones de 12 horas sin mayores problemas[13].

En la siguiente grafica damos una interpretación grafica a estos datos donde el 100% identifica a una conexión de 24 horas.



3.4.2.4 Otros

También se cuenta con algunas líneas analógicas dedicadas, vestigios de cuando se utilizaban terminales tontas conectadas a un Vax central.

Sin embargo la calidad de las mismas es baja.

3.4.3 Comunicaciones externas al organismo

El CES cuenta con una línea Frame Relay que lo comunica con el CES, dicha línea de 2 Mbps, se conecta transparentemente a la lan interna a través de routers Cisco.

A través de la misma el consejo obtiene la salida a internet ya que en la otra punta del enlace existe un servidor propiedad del Ces, con ip pública y es el servidor de mail del Consejo así como el proxy utilizado por la lan interna.

Esta conexión es quizás el nudo de comunicaciones mas importante del consejo pues a través de el podemos comunicarnos con el Cep, con Utu o con el mundo.

[12] Utilización de servicio RuralCel en mi domicilio privado por mas de cuatro años, amen de dedicarme configurar equipos para utilizarlos en el departamento de Canelones
[13] Utilización de modems por mas de dos años para conectarnos a internet durante el horario de trabajo.

3.5 Conclusiones

Del relevamiento anteriormente expuesto concluimos que:

- Se dispone de una melange de tecnologías implementadas en distintas oportunidades y con distintos objetivos
- Dichas tecnologías no fueron implantadas con un fin a largo plazo como puede ser la ínter conectividad de los centros
- Hay mucho para hacer en cuanto a la integración de las mismas y la implantación de algún tipo de solución nueva para poder lograr una conectividad real a nivel institucional

En las reuniones de relevamiento realizadas los distintos responsables indicaron que seria condiciones de un modelo que satisfaga las necesidades de la Anep las siguientes:

- Que se abstraiga de la tecnología subyacente para lograr la conexión física
- Que sea modular
- Que incorpore de alguna forma la tecnología existente
- Que sea de relativamente fácil administración y mantenimiento
- Que sea abierta
- Que no dependa de un único SO (esto se debe a que dentro del organismo existen tres As400, en el orden de decenas de Novell, de NT 4.0, de W2K y algunos linux)
- Que no requiera grandes inversiones[14]

[14] Este punto es relativo, dado que al ser un organismo tan grande, las inversiones por cuestiones de escala son grandes, lo que se debe evitar es un costo alto por centro a conectar.

4 Primer propuesta de cambio sobre la infraestructura de comunicaciones

A partir de las reflexiones obtenidas en el relevamiento anterior en este capitulo se introducen los primeros elementos y sugerencias para propiciar un cambio en la realidad de infraestructura de comunicaciones del organismo.

A los efectos de mantener la coherencia con el resto del proyecto se presenta la propuesta en su forma original y finalmente en el epilogo se detallan los frutos de esta propuesta.

4.1 Introducción

El presente documento expone la primer propuesta en cuanto a infraestructura de comunicaciones en el Ces.

4.2 Objetivo

Servir de base a para las solicitudes en materia de red de datos a realizar a Antel.

Servir base para determinar que se puede hacer y que no se puede hacer, en este sentido la propuesta presentada por este documento constituye un ideal a alcanzar.

Observación: La propuesta presentada no es idea integra de quien suscribe el documento, sino que es el resultado de varias reuniones con compañeros de trabajo, con funcionarios de otros desconcentrados y de la experiencia diaria de trabajo.

4.3 Alcance

Como se trata de una primer propuesta solo atacará el problema de conectividad al nivel mas bajo, no subiendo al nivel de aplicaciones ni de base de datos.

4.4 Definiciones básicas

4.4.1 Introducción

Como se expuso anteriormente la Anep en su totalidad cuenta con una gran heterogeneidad de enlaces, algunos centralizados algunos no, algunos utilizados algunos no.

Toda esta variedad y dispersión trae grandes problemas de soporte, mantenimiento y se tiene la impresión que en general se sub utiliza lo que hay [13].

En esta primera parte del documento se introducirán las bases de una infraestructura practica y racional que sea la base de partida del resto del trabajo.

4.4.2 Definición del Objetivo del CES en cuanto a conectividad.

Lo fundamental cuando queremos lograr un objetivo es determinar claramente cual es ese objetivo, en el caso del CES no existía un objetivo en materia de comunicaciones, es decir el equipo de redes carecía de una meta a la cual orientar su actividad.

Por eso un primer paso consistió en determinar ese objetivo

Nuestro objetivo es estar interconectados de manera eficaz y económica.

Esta frase aparentemente trivial resume quizás algunos enunciados básicos pero importantes:

- Se quiere tener conectividad entre los distintos nodos del CES.
- No necesariamente administrar las conexiones.
- Se desea que el esquema de conexión sea eficaz
- No se desea una tecnología en particular
- Se busca economía en la solución
- No se busca soluciones exóticas de alta tecnología que sean caras de mantener o administrar, mas sutilmente se desea evitar el tener una ensalada demasiado grande de tecnologías, por los costos asociados a administrar multitud de soluciones en particular, se debería además optimizar los costos asociados a los probables cambios tecnológicos (comprar por ejemplo 300 router y desecharlos un par de años después no es admisible).

4.4.3 Definición del esquema de interconexión física

4.4.3.1 Introducción

Luego de analizar múltiples alternativas, a la luz del objetivo anterior se hizo evidente que en realidad no era importante la conexión física en si, es mas seria conveniente transferir su implementación totalmente a un tercero de forma de tener un conecto en cada lugar que de alguna forma interconectara al organismo, algo parecido al servicio telefónico.

Por ejemplo si el lector solicita una línea telefónica a Antel, este la instala y luego usted trae su teléfono lo conecta y ya esta, totalmente ignorante de si tiene una línea digital, si su voz es luego transmitida por microondas, etc.

Ese seria el ideal para el organismo, ahorrándose de paso el problema del mantenimiento de los equipos "en las puntas" (routers, etc) y aislándolo de alguna manera de los cambios tecnológicos.

Tan se debería que definir ciertos niveles de confiabilidad y capacidad en las líneas para solicitar a Antel que los satisfaga[15].

Es importante señalar que este enfoque que quizás parece obvio, no lo es y durante años la Anep ha discutido con Antel soluciones a problemas puntuales, pero sobre todo las discusiones han sido "quiero un adsl de aquí a allá", o "preciso un frame relay de tales características" lo cual ha redundado en cosas incoherentes como tener liceos conectados pero solo para navegar por Internet y no para transferir los pases por ejemplo.

4.4.3.2 Determinación de los niveles mínimos de confiabilidad y capacidad pedidos

Este es un punto delicado, dado que determinara los niveles mínimos aceptables, a partir de los cuales se edificaran las demandas del organismo [11].

Obviamente un piso es la realidad actual, la cual analizamos en un documento aparte pero que podemos resumir para el propósito que nos ocupa en la siguiente tabla:

Caso	Calidad del servicio
Ruralcel	Es el peor caso
Líneas discadas con módems de 56kbps	Es el caso mas común actualmente
Adsl con velocidades ≥ 64kbps	Caso mas favorable

Comparativa de calidad del servicio de comunicaciones

[15] AntelData o cualquier otro proveedor que pudiera surgir con alcance Nacional

De estos casos el Ruralcel, no es aceptable en cuanto a prestaciones, es decir solo se utilizaría si no hay otra alternativa, pero se plantea una interrogante muy importante de que sea utilizable en la práctica.

El segundo caso ya es un piso aceptable para la mayoría de las tareas, los inconvenientes planteados aquí se basa en la interrupción de las comunicaciones, y en el costo de las llamadas desde el interior por ejemplo, además este tipo de conexiones son difícilmente utilizables para otro tipo de tareas que no sean la transferencia puntual de datos administrativos.

Finalmente, las conexiones continuas son el mejor caso, aunque sean de reducida velocidad, para el organismo es mejor tener una conexión permanente que permita optimizar su uso (transferencia de datos administrativos en la noche, correo e internet en el día, etc), y no tanto el ancho de banda sobre todo si se tiene una tasa de errores baja.

De todo esto, se extraen los siguientes requerimientos mínimos:

- **Deseamos una conexión que se comporte por lo menos como una línea discada de al menos 33.600bps.**

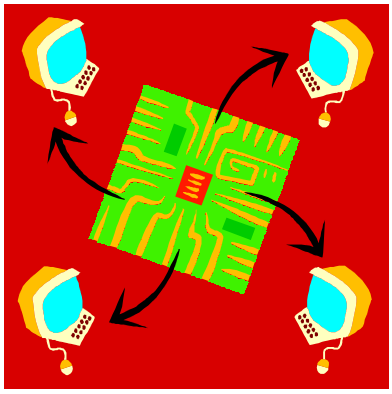
Y el siguiente requerimiento deseable:

- **Preferimos una conexión continua aunque tenga tasas de transferencia bajas, sobre todo si dicha conexión tiene bajas tasas de errores.**

4.4.3.3 Determinación de los protocolos a utilizar

En este punto hay poco para discutir, hoy en día el estándar TCP/IP es *el* protocolo a utilizar.

Pero siendo consecuentes con nuestro objetivo queremos establecer las consideraciones que solicitamos para nuestras conexiones, que son las siguientes:



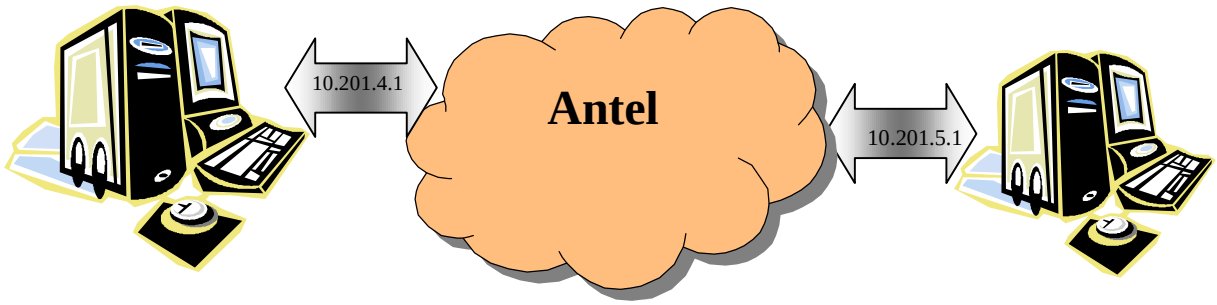
Se desea que cada punto de conexión provisto por Antel proporcione una dirección ip pasible de ser utilizada como default gateway, así como una subnet apropiada de acuerdo a las cantidades de pc a conectar en cada punto.

Es decir se busca una conexión basada en la filosofía del enchufe, es decir que definido para un punto los siguientes datos:

- Dirección ip del enlace
- Subnet

Sea cuestión de conectar el aparato al hub local y ya estamos conectados.

De esta manera se otorga plena libertad a Antel para manejar las conexiones de la forma que quiera, asi como para cambiarlas en el tiempo de la forma que Antel quiera.



Adicionalmente no deseamos que la conexión de Antel permita pasar paquetes DHCP (caso más común)[16]

[16] A los efectos de simplificar la administración en sitios remotos

4.5 Resultado

Las conclusiones planteadas en este documento fueron presentadas a Antel, en una reunión con personal de AntelData, personal del CES y quien suscribe, teniendo una favorable acogida en Antel, en este momento nos encontramos a la espera de la reelaboración del tema por parte de AntelData[17]

4.5.1 Conclusiones

Luego de esa primera reunión se sucedieron contactos a diversos niveles entre ambos organismos, finalmente en el CES el tema escalo hasta llegar a los máximos niveles de autoridad que decidieron que los objetivos presentados en este documento fueran los buscados por el organismo y que los desarrollos informáticos se deberían orientar en dicho sentido.

Es por esta decisión que cambio en cierta forma la realidad a la que nos enfrentamos dado que partimos de una Wan fuertemente desconexa para orientarnos hacia una Wan con conexiones permanentes merced a la utilización de la red tendida en el marco del PCE[18], esta decisión fue tomada entre diciembre y enero y aun no han concluido las negociaciones entre los organismos en cuestión, pero carece de sentido desarrollar con las miras puestas en una realidad que se percibe como pasada.

Afortunadamente ya se cuenta con cinco puntos conectados por la nueva infraestructura que sirvieron a los efectos de realizar pruebas y estudios a lo largo de esta etapa del proyecto.

En concreto las características de la nueva red están basadas en una administración por parte de Antel Data y conexiones de 64kbps.

[17] Obviamente este era el resultado luego de la primer reunión con Antel Data.
[18] Programa de conectividad educativa

Segunda Etapa

En esta parte del informe se presentaran los estudios realizados teniendo en cuenta la nueva infraestructura de comunicaciones.

Ello no es óbice para señalar que muchos de lo generado en esta segunda etapa, tubo sus raíces al comienzo del proyecto y que simplemente se replanteo y adapto a la nueva realidad.

5 Contingencias

5.1 Introducción

A continuación se expondrán las estrategias y procedimientos a utilizar para asegurar el correcto funcionamiento de sistemas instalados a lo largo de todo el País, frente a diversos tipos de contingencias que pueden afectar el funcionamiento de dichos sistemas.

Primeramente se clasificarán los distintos riesgos y luego se propondrán estrategias para enfrentarlos.

5.2 Riesgos

Se clasificaran de acuerdo a su probabilidad (alta, media, baja) y a su gravedad (grave, moderado y leve).

5.2.1 Tabla de riesgos

Riesgo	Gravedad	Probabilidad
Robo de los equipos en los liceos	Grave	Alta
Robo de equipos y carencia de respaldos	Grave	Media
Rotura de equipos (en particular HDD)	Grave	Alta
Rotura de equipos (en particular HDD) y carencia de respaldos	Grave	Media
Desconfiguración de equipos	Moderada	Media
Interrupción en las comunicaciones	Grave	Baja
Virus	Moderada	Baja
Saturación en los canales de comunicación	Leve	Media
Carencia de viáticos para el movimiento de Técnicos al Interior	Moderada	Alta
Usuarios insuficientemente capacitados	Leve	Baja
Fragmentación de la Wan	Grave	Baja

Tabla de riesgos

5.2.2 Riesgos Graves

5.2.2.1 Robo de los equipos en los liceos

Se presentan dos casos, en el primer caso, el equipo robado es el servidor del liceo, en el segundo es una terminal, o el liceo trabaja sobre el servidor Web del CES.

El segundo caso, es muy leve, dado que se traduce en una reducción temporal de la capacidad de trabajo del liceo (hasta que el terminal sea repuesto)

Pero en el primer caso, se paraliza el liceo de un día para el otro.

La estrategia en este caso consiste en tener siempre en reserva un número suficiente de servidores ya configurados, a los que cargarles el ultimo respaldo y enviarlos al liceo en cuestión, en este caso se estima un máximo de dos días para retornar a la normal operativa, y un promedio de un día en la mayoría de las veces.

5.2.2.2 Robo de equipos y carencia de respaldos

Este caso es similar al anterior e igual que el anterior reviste gravedad si no se trabaja en modo Web y el equipo robado es el servidor.

Aquí se presenta el agravante de que los respaldos o no existían o fueron robados o cualquier otra razón impide contar con ellos.

La estrategia en este caso es idéntica a la del 5.2.2.1 con el agregado de que los datos deben ser levantados desde el servidor central, por lo que se pierde el trabajo realizado desde la ultima replicación hasta el momento en que se produjo el inconveniente, de relevamientos efectuados podemos concluir que una sincronización semanal es suficiente para que los perjuicios sean bajos

5.2.2.3 Rotura de equipos (en particular HDD)

Este caso es similar al 5.2.2.1

5.2.2.4 Rotura de equipos (en particular HDD) y carencia de respaldos

Similar al 5.2.2.2

5.2.2.5 Interrupción en las comunicaciones

Al revés de las anteriores este caso es grave en entornos Web y leve en ambientes con servidores locales.

La estrategia a aplicar consiste en tener Modems [9] como alternativa a la conexión dedicada, de esta forma podremos seguir trabajando, la penalización en las comunicaciones no es muy elevada dado que el CES dispone de un banco de modems para atender las peticiones, por lo que los equipos se conectarían directamente con los servidores del CES.

El problema se agravaría si el liceo no puede comunicarse por modem, en este caso si se estima que la interrupción es prolongada, la única alternativa es enviar un servidor local, pero la experiencia del Centro de Cómputos (experiencia documentada a travez de un registro de incidencias) con AntelData, indicaria que las interrupciones no son prolongadas.

5.2.2.6 Fragmentación de la Wan

Nos referimos aquí a la posibilidad de que por alguna razón se vuelva al escenario original de comunicaciones del organismo donde solo tenemos comunicación por intermedio de líneas discadas.

Si bien las posibilidades son pocas, no se debe dejar de tener en cuenta este caso.

En caso de que se produciera esta incidencia la mejor alternativa es retomar los estudios propuestos al comienzo de este proyecto de forma de asegurarnos el flujo de datos e instalación de aplicaciones en este escenario.

Preventivamente seria conveniente retomar dicho estudio lo antes posible de forma de no depender fuertemente de la infraestructura de comunicaciones para el funcionamiento del organismo.

5.2.3 Riesgos Moderados

5.2.3.1 Desconfiguración de equipos

Este riesgo puede ser tratado preventivamente mediante la sustitución de equipos Win 9x por equipos de la familia NT, dado que en ellos es mas fácil controlar a los usuarios.

Aquí tenemos dos casos, desconfiguración total o parcial.

En el primer caso el riesgo es idéntico al visto en el punto 5.2.2.3 con la ventaja de que no existe riesgo para la integridad de los datos, pero en el segundo, basta que en el peor de los casos funcione la conexión via modem, para intervenir remotamente con las herramientas analizadas en el tercer objetivo.

5.2.3.2 Virus

Este riesgo esta analizado en un documento aparte, aquí solo se establece que por tratarse de una wan privada, con adecuados controles y herramientas este riesgo puede ser minimizado.

5.2.3.3 Carencia de viáticos para el envió de técnicos al interior

Este riesgo puede ser minimizado mediante la utilización de herramientas de administración y soporte remotas.

5.2.4 Riesgos leves

5.2.4.1 Saturación en los canales de comunicación

Este riesgo es leve en el caso de la utilización de aplicaciones Win (alcanzaria con agendar replicaciones mas espaciadas para bajar la presión sobre el canal de comunicación) y es mas grave en el caso de aplicaciones Web.

En el caso de aplicaciones Web, podemos comprar mas ancho de banda a Antel o coordinar con los liceos el uso del ancho de banda, mediante por ejemplo calendarios de utilización, instalación de servidores departamentales, etc.

Seria conveniente en este escenario retomar la investigación sobre comunicaciones en una Wan desconexa planteadas al comienzo del presente proyecto.

Pero las pruebas que hemos hecho sobre conexiones ADSL nos indican que este caso es remoto, máxime que podemos descongestionar el canal principal, forzando una cantidad razonable de liceos se comunique directamente por modem con los servidores centrales.

5.2.4.2 Usuarios insuficientemente capacitados

Este riesgo debe ser tratado preventivamente en el diseño e implantación de los sistemas por medio de adecuados diálogos, y suficiente capacitación, además los sistemas deben ser programados “a la defensiva” como es de orden.

6 Entorno a utilizar

De forma similar al capitulo anterior, se introducirá una breve discusión de las ventajas y desventajas de los enfoques Web y Windows a la hora de realizar aplicaciones para la realidad enfrentada.

Esta es una discusión obligada a la hora de plantearse la creación de sistemas a ser instalados en un gran número de puestos de trabajo dado que definirán en gran medida los costos de administración asociados a la instalación y mantenimiento de la aplicación.

Si bien dicha seria mas correcto plantear la discusión en termino de aplicaciones Web y aplicaciones tradicionales, donde entenderíamos por tradicionales cualquier tipo de aplicación que corra en relación directa con un sistema operativo, (OS400, Windows, Unix, etc), este no es el caso que nos ocupad dado que restricciones impuestas por el organismo indicaban que el sistema operativo de los equipos seria Windows.

Previamente se introduce el tema de replicación de datos dado que es un componente fundamental a la hora de trabajar con aplicaciones de alcance nacional en el ambiente Windows.

6.1 Introducción

El presente documento expone los argumentos existentes para elegir un entorno u otro y finalmente recomienda el entorno más favorable para el organismo.

6.1.1 Objetivo

Analizar las ventajas y desventajas de cada uno de las alternativas en el contexto del organismo.

Determinar un conjunto de guías para ayudarnos a decidir entre estas alternativas.

Aplicar dichas guías para realizar una elección en el caso concreto del sistema de gastos de centros educativos.

6.2 Replicación de datos

La replicación de datos permite que ciertos datos de la base de datos sean almacenados en más de un sitio, y su principal utilidad es que permite aumentar la disponibilidad de los datos y mejora el funcionamiento de las consultas globales a la base de datos. [5] Por ejemplo los datos pueden ser almacenados localmente en cada uno de los liceos, de forma de que estos puedan funcionar sin necesidad de disponer de una conexión permanente al servidor central [12].

La replicación en SQL Server consiste, en el transporte de datos entre dos o más instancias de servidores. Para ello SQL Server brinda un conjunto de soluciones que permite copiar, distribuir y posiblemente modificar datos de toda la organización. Se incluyen, además, varios métodos y opciones para el diseño, implementación, supervisión y administración de la replicación, que le ofrecen la funcionalidad y flexibilidad necesarias para distribuir datos y mantener su coherencia [7].

6.3 Componentes del modelo de replicación

Para representar los componentes y procesos de una topología de replicación se utilizan metáforas de la industria Editorial. El modelo se compone de los siguientes objetos: el publicador, el distribuidor, el suscriptor, la publicación, el artículo y la suscripción; así como de varios agentes, que son los procesos responsabilizados de copiar los datos entre el publicador y el suscriptor. Estos agentes son: agente de instantáneas, agente de distribución, agente del lector del registro, agente del lector de cola y agente de mezcla [7].

La replicación de datos es un proceso que ocurre entre servidores de base de datos, en el caso del Consejo de Educación Secundaria se utilizan SQL Server. Los servidores SQL Server pueden desempeñar uno o varios de los siguientes roles: publicador, distribuidor o suscriptor.

El publicador es un servidor que pone los datos a disposición de otros servidores para poder replicarlos. El distribuidor es un servidor que aloja la base de datos de distribución y almacena los datos históricos, transacciones y metadatos. Los suscriptores reciben los datos replicados.

Una publicación es un conjunto de artículos (este concepto: "artículo de una publicación", es diferente del concepto "artículo o registro de una base de datos", como se explicara más adelante) de una base de datos. Esta agrupación de varios artículos facilita especificar un conjunto de datos relacionados lógicamente y los objetos de bases de datos que desea replicar conjuntamente. Un artículo de una publicación puede ser una tabla de datos la cual puede contar con todas las filas o algunas (filtrado horizontal) y simultaneamente contar de todas las columnas o algunas (filtrado vertical), un procedimiento almacenado, una definición de vista, la ejecución de un procedimiento almacenado, una vista o una función definida por el usuario.

Una suscripción es una petición de copia de datos o de objetos de base de datos para replicar. Una suscripción define qué publicación se recibirá, dónde y cuándo. Las suscripciones pueden ser de inserción o de extracción; y una publicación puede admitir una combinación de

suscripciones de inserción y extracción. El publicador (en las suscripciones de inserción) o el suscriptor (en las suscripciones de extracción) solicita la sincronización o distribución de datos de una suscripción.

El publicador puede disponer de una o más publicaciones, de las cuales los suscriptores se suscriben a las publicaciones que necesitan, nunca a artículos individuales de una publicación. El publicador, además, detecta qué datos han cambiado durante la replicación transaccional y mantiene información acerca de todas las publicaciones del sitio.

La función del distribuidor varía según la metodología de replicación implementada. En ocasiones se configura como distribuidor el mismo publicador y se le denomina distribuidor local. En el resto de los casos el distribuidor será remoto, pudiendo coincidir en algún caso con un suscriptor.

Los suscriptores además de obtener sus suscripciones, en dependencia del tipo y opciones de replicación elegidas, puede devolver datos modificados al publicador. Además puede tener sus propias publicaciones [7].

6.4 Escenarios típicos de la replicación

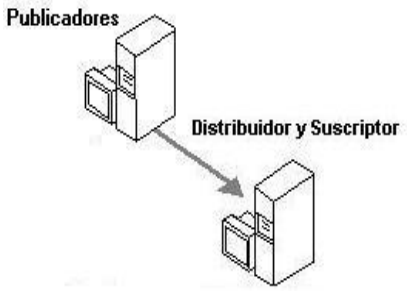
En una solución de replicación pudiera ser necesario utilizar varias publicaciones en una combinación de metodologías y opciones. En la replicación los datos o transacciones fluyen del publicador al suscriptor pasando por el distribuidor.

Por lo tanto en su configuración mínima una topología de replicación se compone de al menos dos o tres servidores SQL Server que desempeñan los tres roles mencionados.

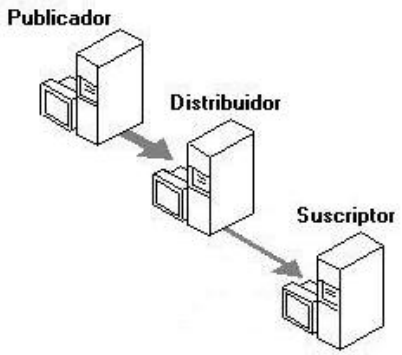
Variando la ubicación del servidor distribuidor podríamos contar con las siguientes variantes:

- El rol de distribuidor desempeñado por el publicador (Fig Publicador – Distribuidor)
- El rol de distribuidor desempeñado por el suscriptor (Fig Distribuidor – Suscriptor)
- Un servidor de distribución, independiente del publicador y del suscriptor (Fig Distribuidor independiente)

Publicador-Distribuidor



Distribuidor-Suscriptor



Distribuidor independiente

En la mayoría de las configuraciones, el peso fundamental de la replicación recae, sobre el servidor de distribución. Por tanto éste puede ser un criterio para determinar su ubicación, teniendo en cuenta las configuraciones (posibilidades físicas) de los servidores, así como otras responsabilidades que pueden estar desempeñando (servidor de dominio, servidor de páginas web entre otras) [7].

Existe la posibilidad de contar con un servidor que se suscriba a una publicación y a la vez la publique para el resto de los suscriptores, esto puede ser muy útil cuando se cuente con una conexión muy costosa con el publicador principal. Por ejemplo el publicador principal en Montevideo en el Consejo de Educación Secundaria y los suscriptores en los Liceos de Maldonado, Piriapolis, San Carlos, Pan de Azúcar, etc. En casos como este, se puede elegir un suscriptor, digamos el servidor de Maldonado el cual se suscribe al publicador en Montevideo y a la vez actúa como servidor de publicación para los servidores de Piriapolis, San Carlos, Pan de Azúcar y demás, minimizando los costos si la conexión es telefónica. Evidentemente en una configuración tal pueden nuevamente combinarse la ubicación de los dos distribuidores y aumentar el número de variantes que pueden presentarse pero las consideraciones para determinar la ubicación del servidor que fungirá como distribuidor son las ya mencionadas.

6.5 Tipos de replicación

Los tipos básicos de replicación son:

- replicación de instantáneas (snapshots)
- replicación transaccional (transactional)

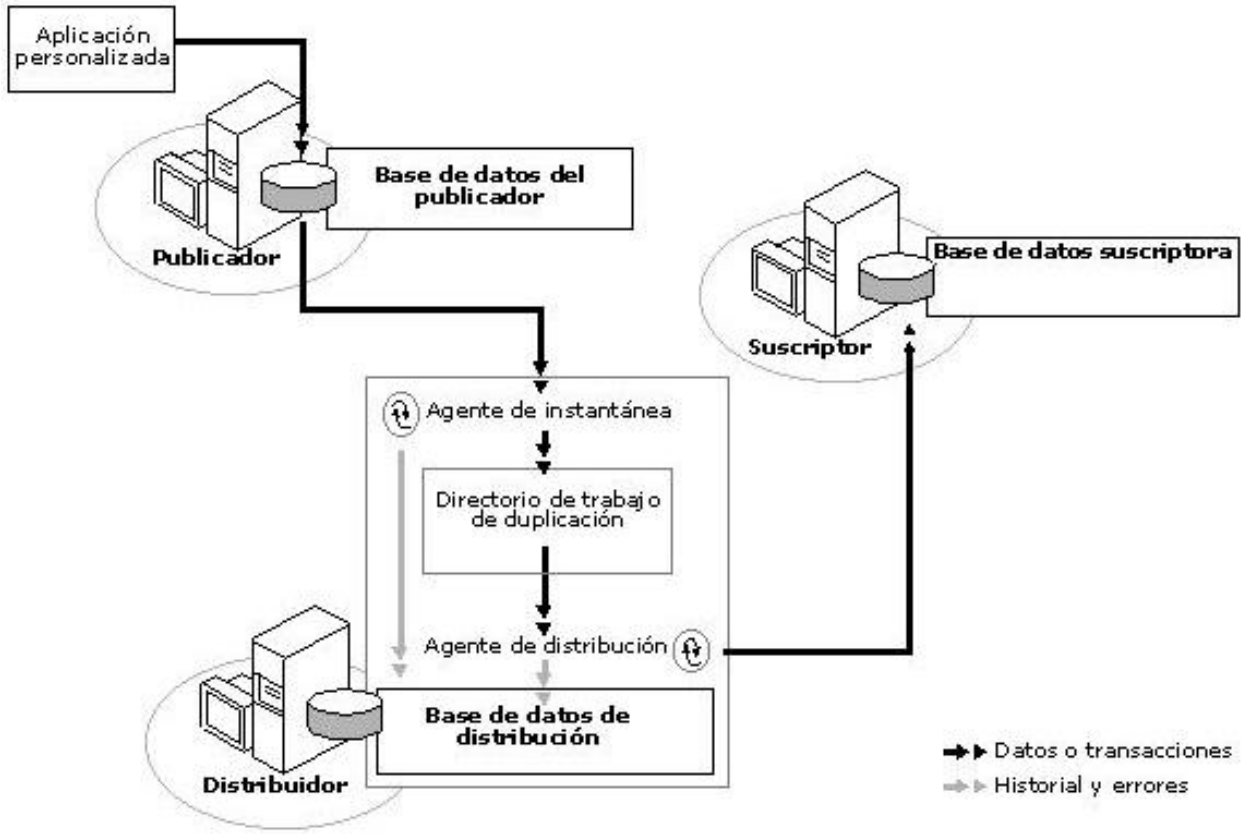
- replicación de mezcla (merge)

Para ajustarse aún más a los requerimientos de los usuarios se incorporan opciones como son la actualización inmediata en el suscriptor, la actualización en cola y la transformación de datos replicados [7].

6.5.1 Replicación de instantáneas (Snapshot)

En la replicación de instantáneas los datos se copian tal y como aparecen exactamente en un momento determinado. Por consiguiente, no requiere un control continuo de los cambios. Las publicaciones de instantáneas se suelen replicar con menos frecuencia que otros tipos de publicaciones. Puede llevar más tiempo propagar las modificaciones de datos a los suscriptores.

Se recomienda utilizar: cuando la mayoría de los datos no cambian con frecuencia; se replican pequeñas cantidades de datos; los sitios con frecuencia están desconectados y es aceptable un periodo de latencia largo (la cantidad de tiempo que transcurre entre la actualización de los datos en un sitio y en otro). En ocasiones se hace necesario utilizarla cuando están involucrados algunos tipos de datos (text, ntext, e image) cuyas modificaciones no se registran en el registro de transacciones y por tanto no se pueden replicar utilizando la metodología de replicación transaccional.



Flujo de datos en la replicación de instantáneas o snapshot

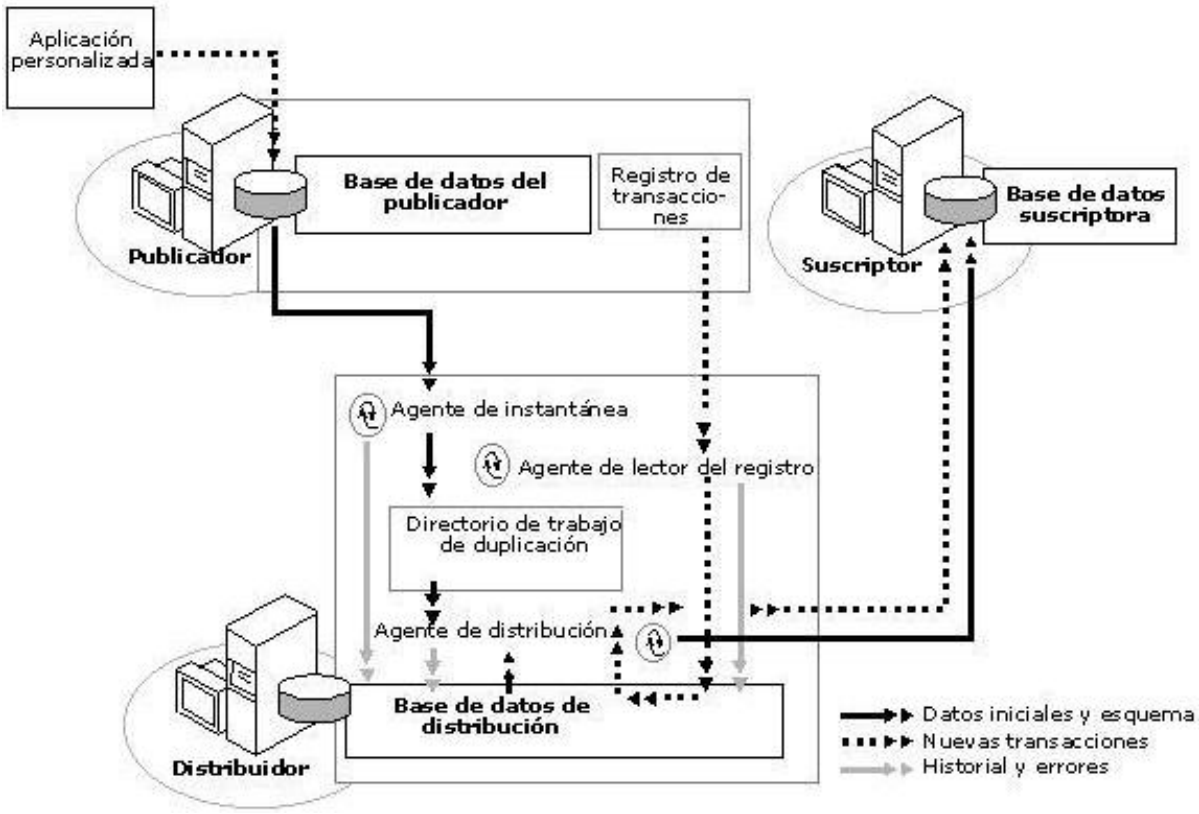
Los servidores OLAP son candidatos a la replicación de instantáneas. Las consultas ad-hoc que aplican los administradores de sistemas de información son generalmente de solo lectura y los datos con antigüedad de horas o días no afectan sus consultas.

Por ejemplo un departamento desea hacer una investigación sobre demografía de los artículos vendidos hace dos meses. La información de la semana pasada no afectará sus consultas; además el departamento no está planeando hacer cambio en los datos, solo necesita el almacén de datos. Hay que destacar además que cuando están involucrados algunos tipos de datos (text, ntext, e image) cuyas modificaciones no se registran en el registro de transacciones [7] y por lo tanto es necesario transportar estos datos del publicador al suscriptor para lo cual es necesario utilizar la replicación de instantáneas, al menos como una solución parcial.

Con la opción de actualización inmediata en el suscriptor se permite a los suscriptores actualizar datos solamente si el publicador los va a aceptar inmediatamente. Si el publicador los acepta, se propagan a otros suscriptores. El suscriptor debe estar conectado de forma estable y continua al publicador para poder realizar cambios en el suscriptor. Esta opción es útil en escenarios en los que tienen lugar unas cuantas modificaciones ocasionales en los servidores suscriptor.

6.5.2 Replicación transaccional

En este caso se propaga una instantánea inicial de datos a los suscriptores, y después, cuando se efectúan las modificaciones en el publicador, las transacciones individuales se propagan a los suscriptores. SQL Server almacena las transacciones que afectan a los objetos replicados y propaga esos cambios a los suscriptores de forma continua o a intervalos programados. Al finalizar la propagación de los cambios, todos los suscriptores tendrán los mismos valores que el publicador.



Flujo de datos en una replicación transaccional

Suele utilizarse cuando: se desea que las modificaciones de datos se propaguen a los suscriptores, normalmente pocos segundos después de producirse; se necesita que las transacciones sean atómicas, que se apliquen todas o ninguna al suscriptor; los suscriptores se conectan en su mayoría al publicador; su aplicación no puede permitir un periodo de latencia largo para los suscriptores que reciban cambios.

Es útil en escenarios en los que los suscriptores pueden tratar a sus datos como de sólo lectura, pero necesitan cambios a los datos con una cantidad mínima de latencia. Ejemplo: un sistema para el procesamiento y distribución de pedidos. En este tipo de escenario, podría tener varios publicadores recibiendo pedidos de mercancías. Estos pedidos se replican entonces a un almacén central donde se despachan los pedidos. El almacén puede tratar los datos como de sólo lectura y requiere nueva información en forma periódica.

Con el uso de la opción de actualización inmediata en el suscriptor se pierde aún más la autonomía de sitio, pero se reduce el tiempo en el cual los sitios actualizan sus copias de los datos. Para hacer modificaciones en la base de datos del suscriptor éstas se realizan (o intentan) también en la base de datos del publicador en una confirmación de dos fases (2PC[19]) por lo que si su modificación se confirma indica que es válida y luego en cuestión de minutos, o según la planificación hecha, estos cambios son duplicados a las demás bases de datos suscriptoras.

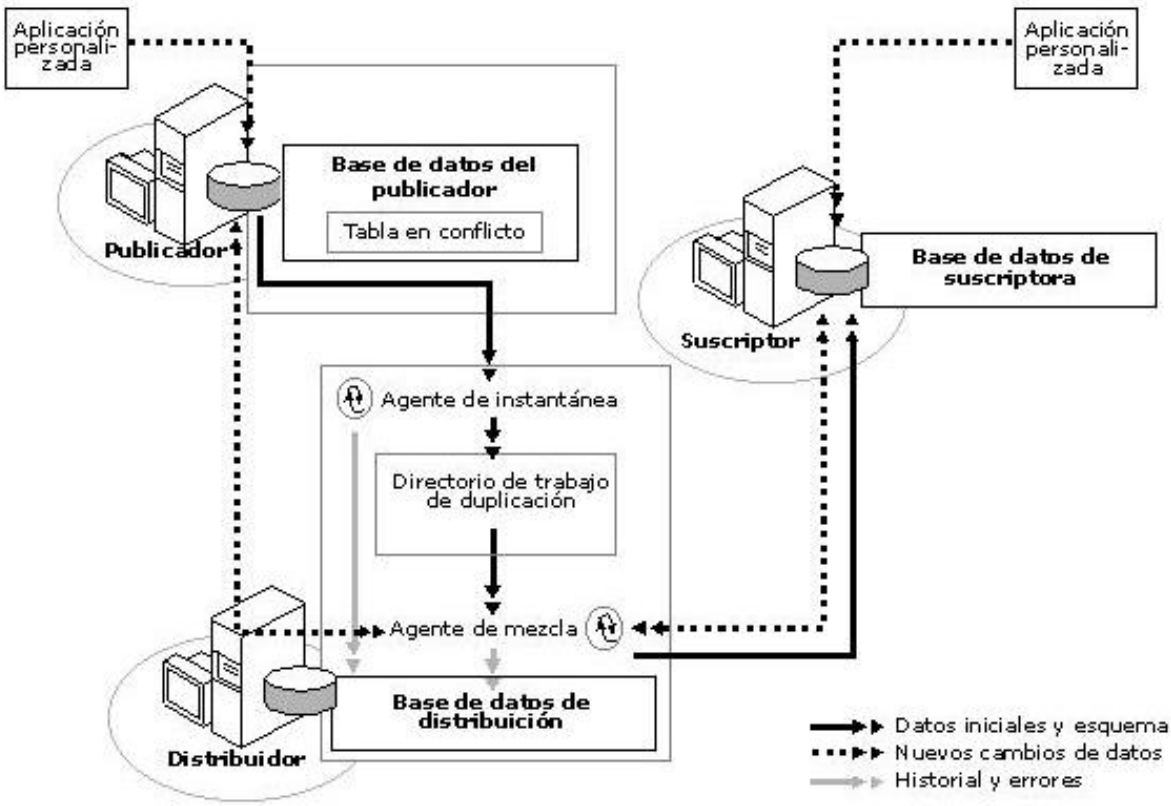
[19] Two Phase commit ver [5]

6.5.3 Replicación de mezcla (Merge)

Permite que varios sitios funcionen en línea o desconectados de manera autónoma, y mezclar más adelante las modificaciones de datos realizadas en un resultado único y uniforme.

La instantánea inicial se aplica a los suscriptores; a continuación SQL Server 2000 hace un seguimiento de los cambios realizados en los datos publicados en el publicador y en los suscriptores. Los datos se sincronizan entre los servidores a una hora programada o a petición.

Las actualizaciones se realizan de manera independiente, sin protocolo de confirmación, en más de un servidor, así el publicador o más de un suscriptor pueden haber actualizado los mismos datos. Por lo tanto, pueden producirse conflictos al mezclar las modificaciones de datos. Cuando se produce un conflicto, el Agente de mezcla invoca una resolución para determinar qué datos se aceptarán y se propagarán a otros sitios. Es útil cuando: varios suscriptores necesitan actualizar datos en diferentes ocasiones y propagar los cambios al publicador y a otros suscriptores; los suscriptores necesitan recibir datos, realizar cambios sin conexión y sincronizar más adelante los cambios con el publicador y otros suscriptores; el requisito de periodo de latencia de la aplicación es largo o corto; la autonomía del sitio es un factor crucial.



Flujo de datos en replicación Merge o de mezcla

Es útil en ambientes en los que cada sitio hacen cambios solamente en sus datos pero que necesitan tener la información de los otros sitios. Por ejemplo podría crearse una base de datos que registre el historial académico de los alumnos liceales. En cada liceo del país, se puede trabajar con los datos de sus alumnos (dado que un alumno es alumno de un solo liceo

en un momento dado) y no se requiere estar conectado permanentemente a la base de datos centralizada en Montevideo.

6.6 Factores para elegir el método de replicación a utilizar

En la elección de un método adecuado para la distribución de los datos en una organización influyen varios factores. Los cuales podemos agruparlos en dos grupos: factores relacionados con los requerimientos de la aplicación y factores relacionados con el entorno de red.

Dentro de los factores relacionados con los requerimientos de la aplicación, los fundamentales son [6]:

- Autonomía
- Consistencia transaccional
- Latencia

La autonomía de un sitio da la medida de cuanto puede operar el sitio desconectado de la base de datos publicadora.

La consistencia transaccional de un sitio viene dado por la necesidad de ejecutar o no inmediatamente todas las transacciones que se han ejecutado en el servidor, o si es suficiente con respetar el orden de las mismas.

La latencia de un sitio se refiere al momento en que se deben de sincronizar las copias de los datos. ¿Necesitan los datos estar el 100% en sincronía? O si es admisible determinada latencia ¿de qué tamaño es aceptable el rezago? [6].

Entre los factores relacionados con el entorno de red están la velocidad de transmisión de datos de la red, deben considerarse factores como el ancho de banda de la red. Debe analizarse además la confiabilidad de la red. Por otra parte en el caso que los servidores SQL no permanezcan todo el día encendidos, como pudiera suceder en algunas organizaciones, deben considerarse los horarios de disponibilidad de cada servidor.

La consideración de estos factores sirven de guía en la configuración del ambiente de replicación. Además se deben considerar las siguientes preguntas: ¿Qué datos se van a publicar? ¿Reciben todos los suscriptores todos los datos o sólo subconjuntos de ellos? ¿Se deben particionar los datos por sitio? ¿Se debe permitir que los suscriptores envíen actualizaciones de los datos? Y en caso de permitirlas ¿Cómo deben implementarse? ¿Quiénes pueden tener acceso a los datos? ¿Se encuentran estos usuarios en línea? ¿Se encuentran conectados mediante enlaces caros?

6.7 Fases generales para implementar y supervisar la replicación

A pesar de que existen varias formas de implementar y supervisar la replicación, y el proceso de replicación es diferente según el tipo y las opciones elegidas, en general, la replicación se compone de las siguientes fases:

- configuración de la replicación
- generación y aplicación de la instantánea inicial
- modificación de los datos replicados
- sincronización y propagación de los datos.

6.8 Conclusión

La replicación es muy útil para mejorar la disponibilidad de datos, lo cual pudiera llevarse al caso extremo, conocido como bases de datos distribuidas replicadas totalmente, en el cual consiste en la replicación de la base de datos completa en cada sitio en el sistema distribuido y garantiza notablemente la disponibilidad de datos, pues el sistema puede continuar operando cuando exista en servicio al menos uno de los servidores SQL Server. La desventaja es un alto costo para mantener la consistencia de las copias en cada sitio [5].

En el caso particular del Consejo de Educación Secundaria, es una solución efectiva que permite el funcionamiento de aplicaciones en todo el país.

Por la misma naturaleza del funcionamiento del ente, los datos se encuentran particionados naturalmente entre liceos de forma que se puede implementar replicaciones de mezcla sin mayores problemas, constituyéndose en un caso ideal para el empleo de este tipo de replicación ya que se obtendrían todas sus ventajas con un mínimo de sus inconvenientes.

Es decir cada liceo podría funcionar de forma independiente con una alta autonomía de sitio, incluso sobre conexiones con anchos de banda bajos, y no es probable que se produzcan demasiados conflictos a la hora de la sincronización.

Sin embargo, este enfoque requiere la instalación de servidores SQL en cada uno de los liceos del país, lo cual conlleva mayores costos de infraestructura, licenciamiento y mantenimiento por lo que no lo hace una solución efectiva desde el punto de vista económico si se dispone de buenas comunicaciones baratas.

A pesar de eso, cuando hablamos de aplicaciones criticas para la organización que justifiquen el costo asociado a la infraestructura a mantener es una solución de primer orden.

6.9 Análisis de las características de los distintos entornos

6.9.1 Entorno Windows

Es el entorno clásico donde se genera una aplicación y luego esta debe ser instalada en cada uno de los equipos.

Ventajas:

- No dependen fuertemente del ancho de banda de su conexión con el servidor[20]
- Los diálogos con el usuario pueden ser realizados con mucha mas maleabilidad[21]

Desventajas:

- Requieren instalación especifica por cada programa que creemos en cada uno de los puestos de trabajo
- Dicha instalación varia de acuerdo a la versión de Windows, e incluso dentro de la misma versión de Windows, al historial de instalaciones de programas en el equipo
- Las aplicaciones Com son particularmente complejas de instalar[22]
- Son de mantenimiento más caro a nivel de soporte, dado que la estabilidad del S.O. se ve afectada fácilmente por multitud de factores, muchas veces la solución de estos problemas pasa por la reinstalación del S.O.
- Es difícil realizar actualizaciones sincronizadas, en por ejemplo todo el país
- Además como se expuso en 6.8, las técnicas de replicación de datos tienen un mantenimiento inherentemente mas costoso en nuestro escenario

6.9.2 Entorno Web

Este entorno consiste en la utilización de Browsers (navegadores) como entorno de "ejecución"[23], de esta forma se logra independencia del S.O., dado que tan solo se requiere que el navegador soporte determinados protocolos (ej: JavaScript, plug in de flash, etc), para que independientemente del equipo en que se acceda a nuestra aplicación la misma esté lista para funcionar transparentemente.

[20] Si se utilizan técnicas de replicación como las vistas en el inciso anterior

[21] Comparando sobre todo con aplicaciones Web sin la utilización de plugins como Flash o los browsers como vehículos de controles ActiveX o Java

[22] De acuerdo a Microsoft dicha realidad cambia a partir de la adopción de un entorno .Net lamentablemente prácticamente el 90% de los equipos de los que disponemos no son lo suficientemente potentes para soportar este entorno

[23] Notar que muchas veces los programas se ejecutan en el servidor web y lo que vemos en el browser es una pagina Html con el resultado de dicha ejecución

Ventajas[10]:

- Es mucho mas sencillo de instalar
- Requiere soporte mínimo en las terminales, y solo hay un servidor o grupo de servidores localizados en el mismo lugar físico a los que es relativamente sencillo darles adecuado soporte
- Las aplicaciones son fácilmente actualizables
- Es independiente del S.O.[24], alcanza con que en la maquina corra un navegador que soporte los protocolos y plug in adecuados a una velocidad razonable para que podamos utilizarla con tan solo poner una dirección en la barra del navegador

Desventajas:

- Depende fuertemente del ancho de banda disponible

[24] Dentro de ciertos margenes

6.10 A la hora de elegir

Como se expuso en el punto anterior hay características que es determinante a la hora de decidirnos por una alternativa u otra, y dicha característica es el ancho de banda disponible, si las conexiones son permanentes o no, y finalmente el costo del mismo.

Si se dispone de conexiones permanentes con un razonable ancho de banda y un costo aceptable, la mejor solución es claramente la solución Web.

En cambio cuando las conexiones son caras, de muy baja velocidad u esporádicas, la alternativa de utilizar aplicaciones clásicas es la única viable.

Ahora bien, nada es gratis, por lo que en este último caso se debe estar preparado para hacer frente a altos costos de mantenimiento.

¿Cuál es nuestra realidad?

Como se vio en el informe de relevamiento de infraestructura, nuestra realidad es heterogénea, pero a raíz de la primer propuesta y diversas negociaciones con Antel, se esta en el proceso de utilizar las conexiones permanentes disponibles con las aulas de informática a Internet para proveer conectividad a nivel administrativo.

Hoy en día un porcentaje altísimo de liceos, y sobre todo los más importantes ya cuentan con conexiones de dichas características, la intención es usarla, desarrollando nuestras aplicaciones apuntando a un entorno Web, sobre todo porque hoy en día el organismo no tiene posibilidades de ampliar su equipo de soporte.

Adicionalmente se dispone de una batería de líneas 0800 para utilizar en aquellos liceos aun no conectados.

¿Pero y los liceos que no están conectados o cuya conexión al 0800 es demasiado onerosa?

En primer lugar se recomienda dimensionar correctamente al liceo, porque no es lo mismo un liceo de 3000 alumnos que uno de menos de 100.

En segundo lugar se debería cuestionar si realmente es necesario que ese liceo se procese electrónicamente in situ o es más razonable la remisión de la documentación escrita a las oficinas centrales, donde es procesada de la forma tradicional como lo es hoy en día.

En caso de que sea un liceo de entidad suficiente o que se quiera que la aplicación esté instalada a pesar de no disponer conexiones de calidad, sugerimos utilizar un mecanismo de replicación que minimice los costos por conexiones discadas, dicho mecanismo puede basarse en un servidor Web local o en aplicaciones Windows tradicionales.

6.11 Estrategia a utilizar para el sistema de control de gastos de centros educativos

A continuación se aplicaran los criterios establecidos en el inciso anterior a los efectos de determinar el entorno más favorable para la aplicación “Control y seguimiento de gastos en Centros Educativos”.

Para nuestro caso de estudio la mejor aproximación es la creación de un sistema Web y el procesamiento manual de los liceos que carecieran de conectividad.

Para llegar a esta conclusión tuvimos en cuenta que: Un alto porcentaje de liceos tienen conexión permanente y de buena calidad.

Dicho porcentaje crece permanentemente y el objetivo oficial es que en un periodo de tiempo razonable se cubran a prácticamente todos los liceos del País.

Ya están cubiertos los con mayor número de alumnos.

Además, hoy en el día el 100% de los liceos se procesa manualmente, por lo que esta medida no representaría ninguna carga adicional de trabajo.

Sin embargo, decidimos utilizar una estrategia mixta, Win-Web a los efectos de estudiar las divergencias en la creación de aplicaciones para estos entornos en ambiente Genexus para generar experiencia que permita tomar decisiones certeras en el futuro.

7 Herramientas de instalación y control remoto

Como se expuso en capítulos anteriores hay una serie de puntos que si bien no forman parte del desarrollo en si del aplicativo, son fundamentales para una implantación y posterior mantenimiento exitosos.

Los análisis post mortem de otros sistemas que fracasaron precisamente en estas etapas mostraron que si bien no era la única causa, si había sido una causa importante del fracaso la falta de previsión sobre estos aspectos.

Por ejemplo al presentarse los primeros errores en las aplicaciones se hace imprescindible la distribución rápida, uniforme y efectiva de parches.

Asimismo en las primeras etapas de la implantación una efectiva atención de soporte es crucial.

Hoy en día donde merced a la emigración es común que técnicos presten soporte por intermedio de programas de control remoto a familiares o amigos ubicados en destinos tan remotos como España, Estados Unidos o Canadá[25] surge naturalmente la pregunta:

¿Por qué no aplicar esas mismas técnicas dentro del territorio Nacional?

Sobre todo teniendo en cuenta lo exiguo del personal de soporte con el que cuenta el Consejo, los pocos recursos económicos que tiene para solventar su traslado y estadía fuera de Montevideo y la necesidad de atender la multiplicidad de llamadas solicitando ayuda en el Centro de Cómputos.

Todas estas cuestiones serán desarrolladas a lo largo del presente capitulo.

7.1 Instalación

7.1.1 Introducción

El presente capitulo expone la propuesta para generar instaladores de aplicaciones Windows en los entornos objeto del proyecto.

Como ejemplo se desarrolla la generación de un instalador para un programa real y concreto utilizado en el Consejo de Educación Secundaria, esta dirigido a lectores técnicos con preparación equivalente a la de programador.

[25] Casos con los que he tomado contacto de primera mano

7.1.1.1 Objetivo

Determinar las necesidades del organismo en cuanto a paquetes de instalación.

Comparar diversos paquetes de instalación y seleccionar el mas adecuado.

Introducir el paquete seleccionado.

7.1.1.2 Descripción del documento

En primer lugar se definirán las necesidades del organismo en materia de paquetes de instalación.

A continuación se describirán las pruebas desarrolladas para elegir un instalador en particular.

Luego se introducirá al NSIS, que es el lenguaje de generación elegido para la generación del ejecutable de instalación.

Después se explicarán los objetivos del script de instalación, mostrando a continuación la estrategia aplicada para alcanzar los objetivos.

Finalmente se introducirá el script de instalación genérico propiamente dicho.

Como apéndice tenemos la “receta de cocina” para obtener su instalación ejecutable en menos de 3 minutos.

7.1.2 Selección del instalador adecuado

7.1.2.1 Introducción

Primeramente se establecen los requerimientos que debe satisfacer un instalador a los efectos de poder ser utilizado en los computadores del CES.

Luego de determinado estos objetivos se realizará una tabla comparativa entre las opciones existentes.

Finalmente se elegirá alguna de las opciones.

7.1.2.2 Establecimiento de los requerimientos para el instalador

Dadas las características de la red del Consejo una de las primeras cosas que surgen como evidentes es que el instalador debe ser Stand Alone, con esto queremos decir que para instalar el programa solo debe ser necesario ejecutar el instalador, sin tener necesidad de correr ningún programa previo, ni ser requisito determinada configuración de Windows.

Esto es así porque al estar instalando un programa en el Liceo de Rivera, no seria practico que apareciera un mensaje solicitando el Ie 5.5 o superior tan solo para correr el instalador, por mas que no fuera necesario para el programa.

La razón anterior cobra mas fuerza aún si tenemos en cuenta, que el Consejo cuenta con todas las versiones de Windows existentes en funcionamiento (si bien para este estudio el requisito mínimo es que funcione en Windows 95 descartándose las instalaciones de Win 3.11), todos estos equipos tienen en distintos estado su software de base, por lo que no se desea que sea requerimiento *del instalador* determinado service pack.

De aquí se extraen el primer y segundo requisito:

- **El instalador debe ser Stand Alone**
- **Debe funcionar en cualquier Windows a partir del 95 (inclusive) en adelante**

Concomitantemente se extrae el segundo requerimiento:

- **El instalador debe ser estable**

Es decir no se desea un instalador problemático que tenga tendencia a colgarse o ser inestable en instalaciones diversas, sobre todo porque el funcionariado que probablemente lo utilice no esta preparado en materia informática, por lo que problemas aparentemente triviales, generados por un instalador poco robusto puede llegar a provocar una sobrecarga intolerable en el área de soporte.

Analizando las características de los enlaces disponibles encontramos otro requisito importante, dado que al presente muchos liceos y oficinas están conectados por modems, y la calidad de las comunicaciones no es todo lo buena que tendría que ser, seria importante que el instalador introdujera el mínimo overhead posible.

Si bien siempre esta la alternativa de distribuir los programas en cd, como dice Tanenbaum, "no menospreciar el ancho de banda de un camión cargado de cintas"[26], no estaría mal considerando la disponibilidad de recursos del ente que el programa en caso de necesidad pudiera ser distribuido en diskettes.[27]

En definitiva se agregan los siguientes requerimientos:

- **El instalador no debe introducir excesivo overhead (kb's) sobre los archivos a instalar.**

- **Que la instalación generada sea pasible de ser distribuida por MODEM o diskettes**

Otro objetivo interesante que simplificaría el mantenimiento de una red tan grande es que se pudiera automatizar totalmente la instalación.

- **El instalador debe ser automatizable.**

Esto se traduce en un requerimiento aun mas grande:

- **El instalador debería ser flexible**

Finalmente a requerimiento de distintos programadores del consejo, queremos que el instalador:

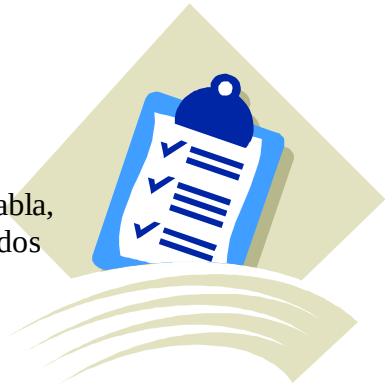
- **Permita un fino control sobre el proceso de instalación y desinstalación de los paquetes**

Este ultimo requisito viene de la mano de uno de los programas mas importantes del consejo, el SecLi32, que es el programa a utilizar por las bedelias liceales, dicho programa tiene mas de 135 componentes (ocx, dll, etc) de los cuales se debe poder tener un control acabado para evitar problemas con la compatibilidad binaria e instalaciones inestables.

[26] Redes de Computadoras, Tercera Edición, Prentice Hall

[27] A veces las grabadores de Cd, se rompen y aun n o son tan comunes en el organismo (solo hay dos) a diferencia de las disketteras y diskettes de los cuales hay abundantes reservas

7.1.2.2.1 Resumen de requerimientos



Los requerimientos pueden ser resumidos en la siguiente tabla, aquellos que son requisitos "sine qua non" están identificados con "☞".

Requisito	Comentario
☞ **Que sea Stand Alone**	Es decir que los paquetes generados por el sean autónomos.
☞ **Compatible con Win 95 y superiores**	
☞ **Que sea estable**	
☞ **Que no introduzca excesivo overhead (kb's) sobre los archivos a instalar**	
Que sea pasible de ser distribuido por MODEM o diskettes	Es decir que genere los paquetes mas pequeños posibles, con controles de integridad (ej: CRC)
Queremos un instalador automatizable.	Que podamos generar exes que se instalen sin intervención del usuario
Queremos un instalador flexible	
Permita un fino control sobre el proceso de instalación y desinstalación de los paquetes	Que haga exactamente lo que le decimos que haga

Requerimientos del instalador

7.1.2.3 Análisis de los candidatos

Se realizo un primer relevamiento de donde se extrajeron tres candidatos:

- Windows Instaler
- Install Shield
- Nsis

El primero es el candidato oficial por así decirlo, ya que es la herramienta de instalación proporcionada por Microsoft.

El segundo es una aplicación que genera paquetes MSI, pero es mas potente y flexible que la utilización del windows installer directamente.

El tercero es el instalador utilizado por Winamp[28].

Para decidirnos por alguno de ellos se realizaron paquetes de instalación de una aplicación compleja[29] en los tres.

Obteniendo los siguientes resultados

Prueba Instalación de un paquete de 3.5 MB	Win Installer Instalador de 19 Mb	Install Shield Idem Win Installer	NSIS Solo agrego 50 kb a la instalación
☞ Que no introduzca excesivo overhead (kb's) sobre los archivos a instalar	☒	☒	☑
Instalación sobre diversas configuraciones	Frecuentemente requiere de tener instalado tal versión del IE o requisitos similares	Idem Win Installer	No requiere absolutamente nada extra para funcionar
☞ Que sea Stand Alone	☒	☒	☑
Instalación sobre Win 95	Requiere la instalación de componentes adicionales	Idem Win Installer	Funciona
☞ Compatible con Win 95 y superiores	☒	☒	☑
Pruebas diversas	No demasiado flexible	Poca estabilidad (queja recurrente en los grupos de discusión de install shield)	
☞ Que sea estable	☑	☒	☑
¿Cumple con los requerimientos primarios?	☒	☒	☑

Comparativa de paquetes de instalación

[28] Popular programa reproductor de música en formato mp3, ver www.winamp.com
[29] Una instalación del SecLi32

Como resultado de las primeras pruebas se selecciono al Nsis y se verifico que cumpla con los requisitos secundarios:

Requisito	Cumplimiento del requisito
Que sea pasible de ser distribuido por MODEM o diskettes	Brinda control de integridad integrado (imposibilita la adulteración de la distribución así como detecta corrupción en la misma por problemas de línea). Además lo pequeño de los paquetes permiten en la practica este tipo de distribuciones.
Queremos un instalador automatizable.	Es totalmente automatizable en la generación de el exe instalador así como en la instalación propiamente dicha
Queremos un instalador flexible	Es muy flexible ya que constituye un pequeño lenguaje de programación en si mismo, además brinda los fuentes del compilador Nsis.
Permita un fino control sobre el proceso de instalación y desinstalación de los paquetes	Por naturaleza del instalador nosotros determinamos a mano que hace, es decir cada paquete a instalar es un pequeño programa que hará lo que le indiquemos, no tiene Wizards ni funciones escondidas, hará lo que le programemos ni más ni menos.

Requisitos secundarios del instalador

7.1.2.4Licenciamiento

Un punto importante que aun no se ha analizado, es el licenciamiento de la herramienta a utilizar.

En este caso, el Nsis es totalmente gratis[30], lo que constituye una ventaja adicional sobre el Install Shield..

7.1.3 Conclusión

Se selecciona al Nsis por haber cumplido con la totalidad de los requerimientos, tener costo nulo, disponer de sus fuentes y haber demostrado suma confiabilidad y flexibilidad en las pruebas realizadas.

En el apéndice 8.2, se presenta un estudio pormenorizado del NSIS así como los scripts desarrollados para la generación de instalaciones en el Centro de Cómputos. Dichos scripts fueron desarrollados en el marco de este proyecto, y su utilidad ha quedado demostrada al sustituir hoy en día los otros métodos de instalación utilizados por el Centro de Cómputos.

[30] Freeware

7.2 Herramientas de control remoto

En este capitulo se analizaran herramientas de control remoto, vale decir, herramientas que permiten mediante el uso de una terminal virtual el control de otro equipo conectado remotamente por cualquier tipo de conexión pasible de transmitir datos.

Estas herramientas están directamente orientadas al mantenimiento y soporte de aplicaciones, quienes tienen experiencia en soporte[31] sabrán que un aspecto muy frustrante de dicha tarea lo constituye el dialogo con los usuarios a través del teléfono. En efecto es común entablar conversaciones prolongadas, que muchas veces concluyen con el desplazamiento del técnico para comprobar que el problema se reducía a un mensaje que inexplicablemente el usuario no veía o no entendía.

Además la cantidad de información que un técnico calificado puede absorber con solo recorrer un sistema es impresionante, es común observar como se turna el personal de soporte en una misma maquina a la hora de resolver un problema particularmente difícil, quizás la expresión que mejor define esta realidad es “sentir la maquina”, es una sensación difícil de entender por quien no se ha desempeñado en estos roles, pero tan solo imaginemos a un mecánico intentando diagnosticar un coche por teléfono y tendremos una idea de esta realidad.

Es por eso que este tipo de herramientas son muy populares entre los administradores de red y personal técnico, dado que evita el desplazamiento inútil a través de las instalaciones del organismo donde se desempeñe, claramente se aprecia la importancia de este tipo de herramientas cuando el organismo se extiende por todo el país como es en el caso estudiado.

Imaginase el lector los inconvenientes causados por el movimiento de un técnico desde Montevideo a Salto para encontrarse que la falla era causada por un problema menor de configuración.

Sin embargo en el Consejo de Educación Secundaria no se encuentra ni extendido ni sistematizado el uso de estas herramientas, sobre todo porque hasta fechas recientes el hardware disponible en los liceos carecía de las funcionalidades mínimas que pudieran permitir el uso de estas herramientas.

7.2.1 Requerimientos

Primeramente se establecerá las características buscadas en la herramienta a utilizar:

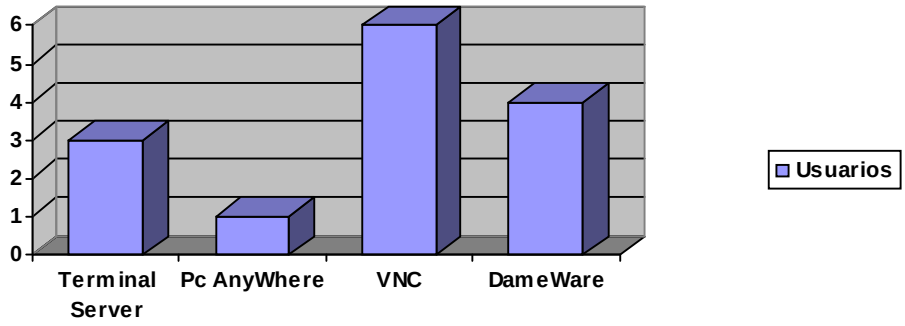
[31] Soporte es el termino genérico con que se nombran las tareas de atención directa a usuarios orientadas al apoyo del mismo y al mantenimiento de la operativa. El autor de este informe fue Jefe de Soporte en Consejo de Educación Secundaria por tres años, actualmente es el Administrador de Red en Jefe.

- Compatibilidad con sistemas Windows NT, 98 y superiores
- Requerimientos de ancho de banda lo suficientemente bajos para permitir su uso en líneas discadas
- Estabilidad
- Instalación sencilla
- Funcionamiento sobre protocolo TCP/IP

7.2.2 Herramientas a comparar

Para la preselección de las herramientas se recurrió a la bibliografía especializada[32] así como a un muestreo realizado entre de 14 administradores de red en los meses de octubre, noviembre y diciembre del 2003[33].

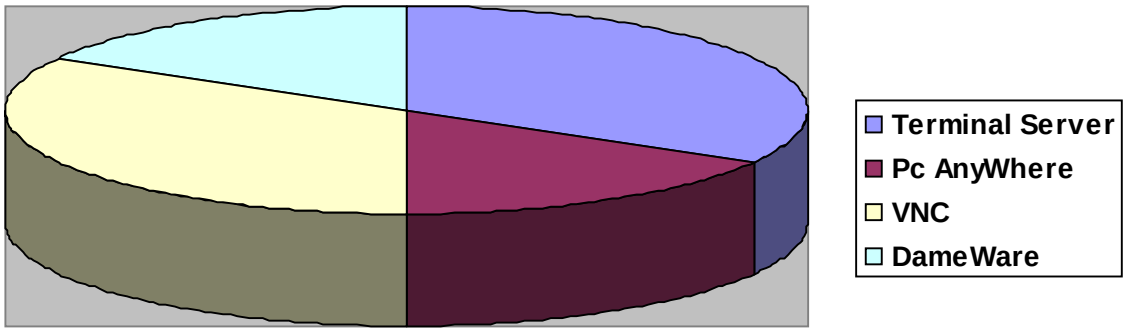
Los resultados de dicho relevamiento mostraron lo siguiente:



Relevamiento de herramientas de control remoto

Si analizamos en cambio la utilización de cada herramienta por centro de cómputos vemos lo siguiente

[32] En particular [2]
[33] Muestreo realizado por el autor de este trabajo en los cursos de MCSA y MCSE realizados en el instituto Empower U



Herramientas de control remoto por centro

Es decir la utilización del Terminal Server de Windows 2000 y el VNC en un primer puesto, seguidos por el PcAnyWhere y el DameWare.

Sin embargo el Terminal Server es un producto que se incluye en el Windows 2000 y XP y superiores, por lo que no cumple con los requerimientos planteados lo que nos fuerza a descartarlo. Por consiguiente realizaremos nuestro estudio sobre las otras tres herramientas.

7.2.3 Características principales

En el siguiente cuadro se resumen las principales características de las herramientas analizadas.

Característica	*VNC*	*Dameware*	*PcAnyWhere*
FreeWare	Si	No	No
OpenSource	Si	No	No
Funciona sobre líneas discadas	Si	Si	Si
Dispone de Instalador Remoto	No	Si	Si
Funciona sobre TCP/IP	Si	Si	Si
Compatible Win 98 y superiores	Si	Si	Si
Estabilidad	Si	Si	Si
Instalación sencilla	Si	Si	No

Tabla comparativa de herramientas de control remoto

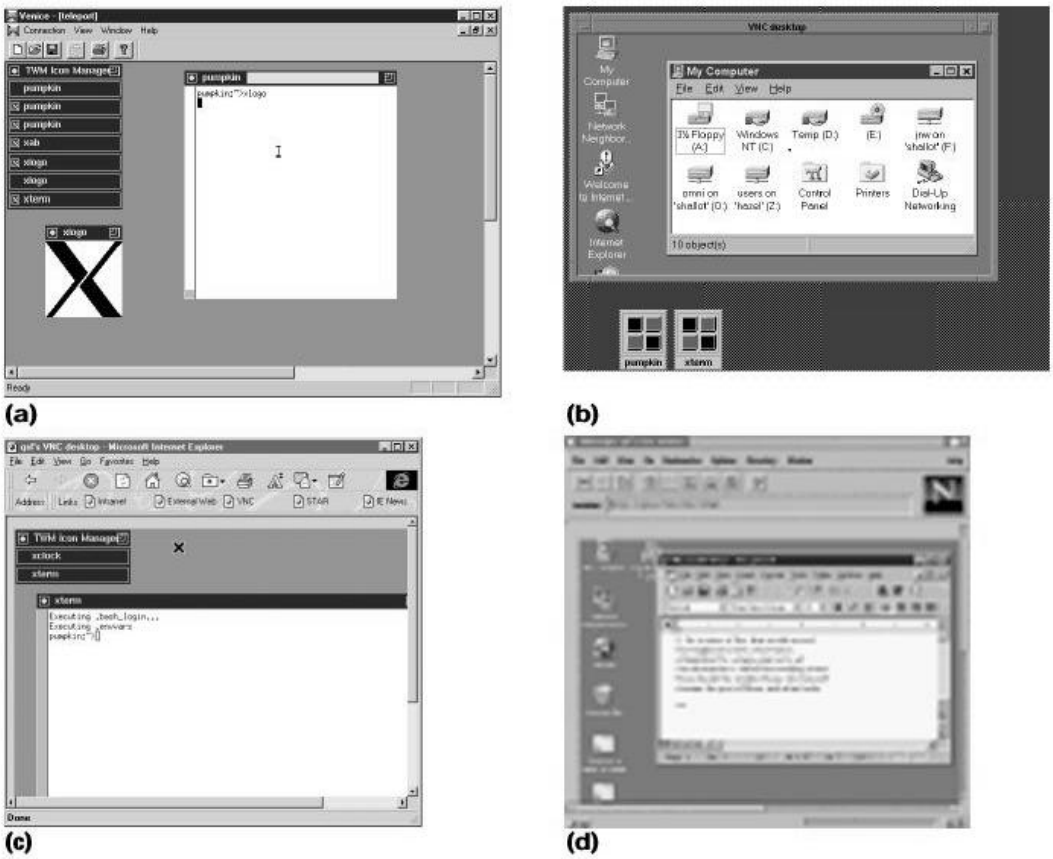
De un primer análisis se desprende que cualquiera de las tres herramientas cumplen con los requisitos básicos planteados.

A continuación se realizara un análisis detallado de cada una de ellas.

7.2.4 VNC

Vnc significa “Virtual Network Computing”, siendo un cliente ultra liviano para control remoto de aplicaciones..

Fue creado en los laboratorio de ORL (Olivetti y Oracle Laboratories) en Inglaterra a principios de la década pasada y se ha convertido en uno de los paquetes de control remoto mas populares por ser multiplataforma, efectivo, fácil de instalar y gratis.



Capacidades multiplataforma de Vnc

En particular sorprende la capacidad multiplataforma del Vnc, en la imagen anterior vemos en (a) un escritorio X[34] desde un cliente Vnc Windows, en (b) un Windows 95 desde un visor para X Windows, en (c) un escritorio X utilizando el visor Java sobre un Internet Explorer y finalmente en (d) un escritorio Windows 9x utilizando también el visor Java pero sobre un navegador Netscape. Es importante señalar que aquí no se acaban las características multiplataforma del Vnc, sino que existen visualizadores para PDA[35].

Esta característica resulta muy interesante dado que en la organización se esta considerando en este momento la utilización de sistemas Linux para la implementación de firewalls, por lo que no deja de ser atractivo que se pueda utilizar el mismo programa para administrar la totalidad de los equipos de la red.

[34] X Windows es el Windows típico de los sistemas basados en Unix

[35] PDA, son los asistentes personales digitales, por ejemplo Palms, Pocket Pc, etc, es decir pequeñas computadoras portátiles del tamaño de una agenda electrónica común.

Otro aspecto interesante lo constituye lo pequeño que es el paquete, el visor o cliente ocupa tan solo 175 Kb y el servidor o host menos de 300 kb, lo cual lo constituye en un candidato pasible de ser transferido utilizando conexiones discadas.

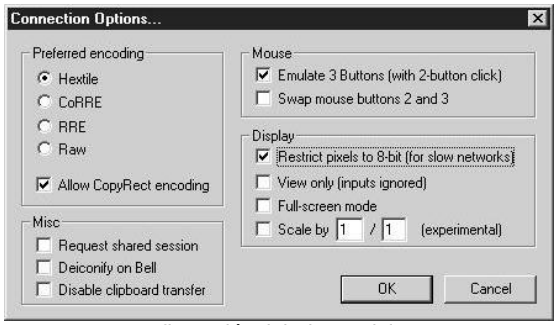
La configuración del cliente es en extremo simple, tan solo requiere que haya conectividad tcp/ip, sobre ella el programa se comunicara transparentemente sin requerir ninguna configuración especifica.

Al lanzar el cliente o visor surge el siguiente dialogo:

Login del Vnc

Como se aprecia, simplemente proporcionando la dirección Ip(o el nombre) del servidor y tras el posterior ingreso de una contraseña estaremos conectados.

Adicionalmente si se desea se pueden configurar unas pocas opciones como se aprecia en el dialogo siguiente.

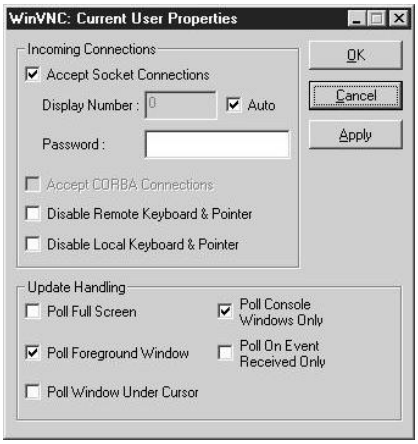


Configuración del Viewer del Vnc

La única opción que es interesante utilizar, es la que restringe la visualización a 8 bits, de forma de reducir la cantidad de datos a ser transferidos a costa de una perdida en la cantidad de colores a mostrar, el resto de las opciones no deben ser modificadas en el entorno considerado, ya que tienen que ver con el uso del mouse en sistemas X Windows, y con las capacidades de visualización de entornos hardware disímiles.

En el caso analizado las opciones por defecto son adecuadas.

Del lado del servidor las opciones no son mas complejas como se vera en el siguiente dialogo:



Configuración del Vnc Server

Como se observa la opción mas importante atañe a la elección de la contraseña que habilitara la conexión, además se dispone de 5 formas distintas de manejar el refresco de pantalla, en general en las pruebas realizadas la configuración por defecto funciono muy bien.

Solamente hay un aspecto censurable en la utilización del Vnc, que es que tras el establecimiento de la conexión [3] la comunicación entre el servidor y el cliente no utiliza ninguna encriptación, por lo que si se desea asegurar la privacidad de la comunicación se deberá utilizar un protocolo seguro de comunicaciones.

Como contrapartida el Vnc es una herramienta confiable, muy simple de utilizar y muy flexible, además se comporta muy bien con comunicaciones discadas.

Creemos por lo tanto que es una herramienta adecuada para los objetivos perseguidos en el Consejo de Educación Secundaria.

7.2.5 DameWare Mini Remote Control

Este programa es muy similar al Vnc pero agrega una serie de características extras, las que favorecen y a su vez perjudican a la herramienta.

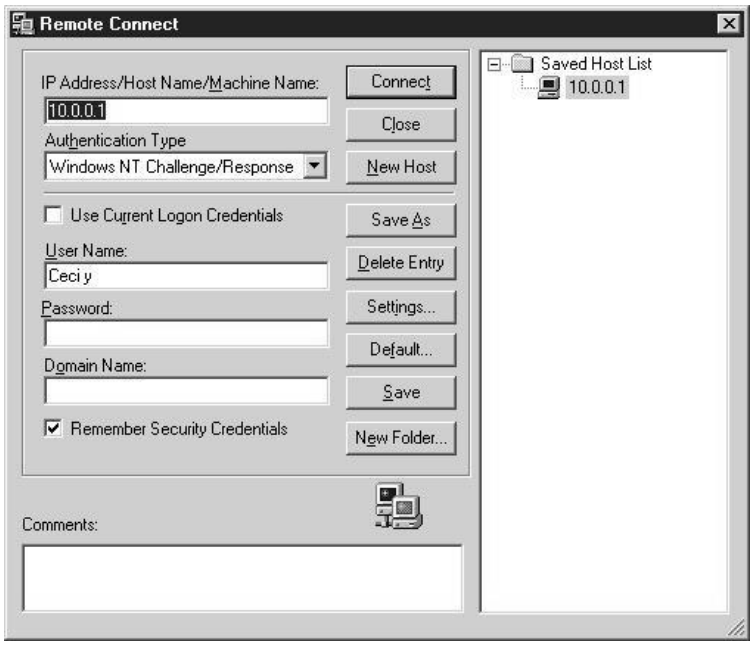
Entre las características útiles introducidas se cuentan la utilidad de transferencia de archivos y la encriptación incluida en el paquete.

Como contrapartida la instalación es un poco mas complicada y mas grande el archivo a instalar, dicho archivo trepa a mas de 7mb es decir un 2400% mas grande que el archivo de instalación del VNC[36].

Este programa tiene la característica de que no dispone por separado de un programa servidor y otro cliente, de forma que el mismo programa puede actuar en cualquiera de los dos roles.

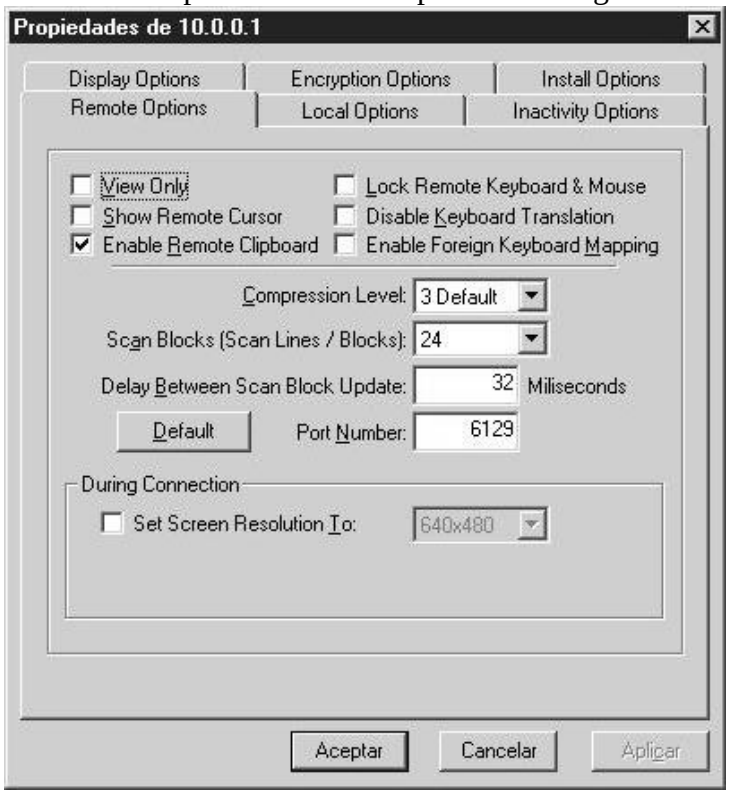
[36] Como se vio en el capitulo de instaladores, este desproporcionado aumento en el tamaño del archivo instalador puede ser debido a la tecnología de instalación utilizada.

Para comenzar a utilizarlo se lanza en un pc el programa, eligiendo la opción de “accept incoming calls”, a continuación se lanza el programa que automáticamente intentara conectarse en modo cliente a través del siguiente dialogo.



Login del Dameware Mini Remote Control

Como vemos ya nos enfrentamos a un dialogo mas complejo que en el Vnc, aun mas complejo si personalizamos las opciones como se aprecia en el siguiente dialogo.



Opciones del Dameware

Si bien todas estas opciones brindan un grado de flexibilidad muy superior al proporcionado por el Vnc, en general introducen características que no son particularmente necesarias en el escenario objetivo del Consejo de Educación Secundaria, por ejemplo, la transferencia de archivos puede hacerse fácilmente a través de las funcionalidades de red comunes, es decir no es necesario disponer de estas facilidades integradas al sistema, pero estas características extras tienen como contrapartida dificultar la configuración e instalación introduciendo mayores puntos de falla.

En resumen es un buen producto, que ofrece mucho mas que el Vnc, pero a excepción de las características de encriptación de las comunicaciones lo que ofrece no es estrictamente necesario, por otra parte el aumento en el archivo de instalación y la complejidad añadida en su uso hacen mas aconsejable la utilización del Vnc en el marco del Consejo de Educación Secundaria.

7.2.6 PcAnyWhere

Este paquete es sin duda el veterano del mercado y como tal ofrece un gran conjunto de opciones y prestaciones, destacando por sobre los otros paquetes analizados.

Sin embargo tiene varias características que desaconsejan su uso para el caso particular del Consejo de Educación Secundaria.

La mas importante de estas desventajas es que a diferencia del Vnc que descansa sobre una comunicación TCP/IP establecida por otros medios, el PcAnyWhere realiza su propio manejo de conexiones discadas, dicha característica no es admisible en el escenario considerado ya que podría interferir con otros programas (por ejemplo rutinas de replicación) que realizan sus propias tareas vía modem.

En la misma línea, este producto se caracteriza por ser mas rápido que las otras opciones consideradas a costa de instalar bastante software en el servidor, lo cual contraria las políticas de instalación de software en los servidores del Consejo de Educación Secundaria.

Adicionalmente la configuración resulto ser la mas compleja del grupo de programas analizados, caracterizada por multitud de configuraciones separadas a las cuales acceder por distintos caminos y una sensación de desconcierto en un primer acercamiento a la herramienta. Es difícil entender por ejemplo porque el wizard para la optimización de la conexión se encuentra separado de los iconos de las conexiones.

PcAnyWhere

7.2.7 Conclusión

Todas las herramientas analizadas cumplen con los requisitos solicitados, sin embargo claramente la herramienta que mas se ajusta a las necesidades del Consejo de Educación Secundaria, es el Vnc.

Tiene a favor el ser multiplataforma, tener un pequeño archivo de instalación y la extrema simplicidad de su instalación, configuración y uso y por si fuera poco es gratis, lo que no es de desdeñar si se considera un volumen de licencias de alrededor de 1000 equipos.

En el debe estaría la relativa inseguridad de el dialogo entre el servidor y cliente por el hecho de transferir la información de forma no encriptada, pero como contrapartida en [4] se explica detalladamente la solución de este problema mediante el uso de SSH.

8 Apéndices

8.1 ¿Qué es GSM?

GSM (Sistema Global para Comunicaciones Móviles) es una tecnología digital inalámbrica de segunda generación (2G) que presta servicios de voz de alta calidad, así como servicios de datos conmutados por circuitos en una amplia gama de bandas de espectro, entre las cuales se encuentran las de 450, 850, 900, 1800 y 1900 MHz.

Integra mensajería SMS (envío y recepción), MMS (servicios Multimedia), envío y recepción de fotografías, capacidad de transmisión de datos GPRS [14].

Con la tecnología GPRS se puede disponer de todos los servicios que hoy son posibles con CDPD, sumándole además la posibilidad de beneficiarse de éstos a través de un terminal móvil, y con una mayor velocidad de transmisión.

Los terminales GSM/GPRS están siempre conectados: no es necesario establecer llamada para acceder a la información. Se podrá realizar y recibir llamadas de voz mientras está transmitiendo datos: no es necesario reiniciar la transmisión de datos una vez finalizada la conversación.

En el caso de recibir una llamada de voz mientras se está transmitiendo datos, se atiende la llamada y luego se retoma automáticamente la comunicación de datos.

Esta tecnología nace en 1982, cuando un grupo de países europeos creó el Group Spéciale Mobile (GSM) [14] para desarrollar una tecnología celular que proporcionara roaming internacional imperceptible al usuario y soporte para servicios avanzados no disponibles en las redes analógicas. El Instituto Europeo de Normas para Telecomunicaciones (ETSI) se hizo cargo del proyecto en 1989 y completó la primera serie de especificaciones técnicas. La primera red GSM fue lanzada en 1991, y fue seguida por varias más el año siguiente. Al adoptarse la tecnología en países no europeos, se hizo evidente que GSM sería una tecnología global y no europea; así fue como la sigla GSM comenzó a significar "Sistema Global para Comunicaciones Móviles".

GPRS (Global Packet Radio Service) es una evolución no traumática de la actual red GSM, utilizando esta tecnología, el ancho de banda base de GSM pasa de 9.5 kbps [1] hasta un tope de 144 kbps [17], lo que claramente brindaría un canal de comunicaciones mas que adecuado para las necesidades del organismo.

8.2 NSIS

8.2.1 Introducción

Luego de completadas las pruebas y haber seleccionado la herramienta, es hora de empezar a trabajar con ella y comprobar si las bondades esperadas, se cumplen.

Para lo cual se desarrollo la instalación de una aplicación compleja utilizada en el consejo, siendo dicha instalación la utilizada actualmente.

A continuación se introducirá la herramienta y se explicaran los fundamentos de su uso siempre apoyados en ese ejemplo.

8.2.2 ¿Qué es el NSIS?

NSIS es el "Nullsoft (SuperPiMP|Scriptable) Install System", que literalmente significa "sistema de instalación (configurable|SuperPiMP) de Nullsoft".

En la práctica es un pequeño lenguaje de programación que permite generar ejecutables totalmente "stand alone" [37].

Este sistema desarrollado por Nullsoft (los creadores del Winamp), es totalmente Freeware y la compatibilidad está asegurada por la amplia difusión del propio Winamp.

8.2.2.1 ¿Por qué el NSIS?

Porque es sumamente estable, rápido, introduce poco overhead[38] sobre los propios archivos a instalar, es gratis y además las pruebas de campo demostraron que es muy bueno.

De todas formas cuando se retome el análisis de los objetivos planteados volveremos sobre el tema, ahí discutiendo punto a punto ventajas y desventajas de este sistema.

8.2.2.2 ¿Dónde se obtiene el NSIS?

Se puede bajar desde http://www.nullsoft.com/free/nsis/.

[37] Significa que es un programa ejecutable que no necesita de ninguna Dll o Ocx para su ejecución en ambiente Win32 (en el caso que nos ocupa).
[38] En este contexto el overhead se mide principalmente en la cantidad de KB añadidos por sobre los binarios a distribuir.

8.2.2.3 ¿Qué versión se utilizo?

Se utilizo la versión 2.0b2, ya que permite soporte del lenguaje Español, así como tiene apariencia gráfica de última generación.

8.2.3 Introducción al NSIS

Básicamente el NSIS es un lenguaje compilado (los fuentes del compilador NSIS, son proporcionados con el paquete estándar y están escritos en C++).

Los fuentes de un programa NSIS son archivos de texto ordinarios con extensión "nsi", y con sólo conocer un puñado de comandos se pueden generar instaladores muy sofisticados, básicamente los comandos se dividen en dos grandes grupos a saber, los comandos básicos como son los de copiar o registrar un archivo, y los comandos de GUI, introducidos en la versión 2.0.

8.2.3.1 Comandos básicos del instalador

OutFile 'instalador.exe'

Indica que el ejecutable a crear se llamara "instalador.exe".

LicencenseData 'LicenciaSecLi32.txt'

Indica el archivo a mostrar en la ventana acuerdo de licencia, este archivo puede ser un txt o un rtf.

Debe estar en el mismo directorio en que se encuentra el fuente al momento de compilar el instalador.

InstallDir "$PROGRAMFILES\SecLi32"

Define el directorio hacia donde será instalado el programa en la máquina del usuario.

Tiene multitud de variables definidas para hacer cosas simpáticas, en particular, la más utilizada es &PROGRAMFILES, que se expandirá en la máquina del usuario al famoso"C:\archivos de programa\", se probo en plataformas inglés, español y con el disco duro ubicado en otras unidades y funciona bien.

En este ejemplo, el programa se instalaría en "C:\archivos de programa\SecLi32".

InstallDirRegKey HKEY_LOCAL_MACHINE "SOFTWARE\ConsejodeEducación Secundaria\SecLi32"

Este comando chequea si en el registro está definido un directorio especial de instalación, si es así, utilizará ese valor en vez del definido en InstallDir.

DirShow Hide

Este comando evita que aparezca el browser para que el usuario pueda cambiar el directorio de instalación.

Section "esta sección"

SectionEnd

Este comando se utiliza para definir distintas secciones dentro del instalador, por ejemplo, definir "Instalación típica"," Instalación Personalizada", etc.

Como nosotros no damos esas opciones, directamente utilizamos Section "" que indica la sección por defecto.

SectionEnd indica el fin de la sección.

SetOutPath "C:\LosQuieroAca**"**

Este es uno de los comandos más utilizados, indica el directorio donde serán ejecutados los comandos cuando se utilice el instalador.

Es decir, al encontrar el comando anterior, el instalador dejará todos los archivos en el directorio "LosQuieroAca" del disco C.

Normalmente se utiliza la variable de entorno **$PROGRAMFILES** que es sustituida por la ubicación del directorio "archivo de programas" en la máquina cliente.

Por ejemplo la utilización más típica es **SetOutPath** "**$PROGRAMFILES**\SecLi32".

Si no existe el directorio destino, lo crea.

File ".\DondeEstan\MiOcx.ocx"

Este comando es sin duda el más importante del lenguaje, tiene dos propósitos, el primero es indicar que el archivo indicado se incluya en el paquete de instalación, cuando el mismo es generado.

Luego cuando la instalación es ejecutada en la maquina cliente, este comando indica que el archivo anteriormente incluido, sea extraído en el directorio indicado por **SetOutPath.**

 Este comando soporta el uso de wilcards, por ejemplo el comando **File** ".\binarios\cpresentación" incluirá y luego descomprimirá todos los archivos

ubicados en el directorio “\binarios\cpresentación” hijo del directorio donde se encuentre el archivo fuente de la instalación al momento de la compilación

ExecWait “Programa.exe Parametros”

Ejecuta y espera la finalización del programa indicado.

CreateDirectory “C:\Directorio”
Crea un directorio, se utiliza en conjunto con la variable $SMPROGRAMS para crear el directorio en el menú Program Files.

CreateShortCut “Nombre del Acceso Directo” “exe” “Parametros” “Lugar donde crear el acceso”

Crea un acceso directo.

WriteUnistaller “$INSTDIR\unistSEcLi32.exe”

Indica como se llamará el desinstalador, a su vez determina donde quedará ubicado de acuerdo al $OutPath definido en el contexto de esta instrucción.

Section Uninstall;

Indica que aquí comienza la sección del desinstalador.

UnistallText “Desinstalador del sistema”

Especifica el título de la ventana del desinstalador.

Delete “archivo”

Elimina el archivo, soporta wildcards.

RMDIR “directorio”

Elimina el directorio en cuestión

SetShellVarContext all

Indica si cuando modificamos el escritorio, etc, los cambios son sólo para el usuario activo o para todos.

8.2.3.2 Nueva GUI

A partir de la versión 2.0b1 del instalador se introduce un completo set de comandos para el manejo de la GUI estilo MSI.

A continuación se detallaran los comandos más importantes.

!define MUI_PRODUCT "SecLi32"

Indica el nombre del producto a instalar

!define MUI_Version "1.1.0"

Indica la versión del producto a instalar

A continuación se introduce una serie de pantallas predefinidas:

!define MUI_WelcomePage
Página de bienvenida.

!define MUI_LicensePage
Acuerdo de Licencia.

!define MUI_FinishPage
Pantalla de despedida.

!define MUI_ABORTWARNING
Advertencia de no finalización de la instalación.

!define MUI_UNISTALLER
Definición de instalador con entorno MUI (moderm UI)

!define MUI_UNCONFIRMPAGE
Se le pregunta confirmación?

!define MUI_UNFINISHPAGE
Página de finalización de la desinstalación

!Include "MUI.nsh"
Incluye la biblioteca que define el entorno MUI (modern user interface del NSIS).

!InsertMacro MUI_System
Se habilita el entorno MUI (modern user interface del NSIS).

!InsertMacro MUI_Languaje "Spanish"
Se selecciona el lenguaje.

8.2.3.3 Definiciones genéricas del NSIS

SetCompress Auto

Comprime los datos, siempre y cuando la compresión reduzca el espacio utilizado.

SetDataBlockOptimize on

Optimiza la compresión del archivo.

SetCRCCheck on

Realiza una verificación utilizando el algoritmo CRC32 de la integridad del archivo, en caso de que falle, no permitirá la instalación.

Atención hay una opción en línea de comando que inhibe este control.

AutoCloseWindow False

Indica que no se vaya la ventana del instalador una vez finalizada la instalación.

SetDateSave On

Cuando copia los archivos preserva la fecha original de los mismos.

8.2.4 Cómo se alcanzaron los objetivos planteados

- ✓ El compilador elegido está escrito en C++ por lo que es capaz de generar ejecutables para windows que no necesitan absolutamente ningún runtime, ni instalación previa de nada, requisito que ni siquiera es cumplido por los paquetes MSI.

- ✓ El sistema elegido introduce un overhead de tan solo 30 kb sobre los archivos a distribuir, logrando paquetes un **500%** más pequeños que los obtenidos por MSI, esto también facilita su posterior distribución por la vía que sea.

- ✓ Los paquetes generados son sumamente estables, se testearón en varias plataformas NT, W2K, XP, 98 y 95, en distintos idiomas y además es el utilizado por el popular WINAMP, lo que asegura su compatibilidad en los más variados entornos.

- ✓ Se logró crear un script, mediante el uso de WildCards, facilidades del lenguaje y una aplicación de desarrollo propio, que automáticamente toma los archivos de una estructura de directorios en particular y con un simple clic derecho genera la ultima versión del paquete de instalación.

- ✓ El sistema es sumamente flexible, flexibilidad que se ve aumentada por sus características de pequeño lenguaje de programación y por el hecho de que sus fuentes son proporcionados.

- ✓ El sistema es sumamente secuencial y estable, permitiéndonos reproducir lo que haría un operador humano con un alto nivel de detalle.

- ✓ Por los tamaños obtenidos se hace viable su distribución vía MODEM o incluso diskette, además el sistema provee controles de CRC que garantiza su inmunidad frente a contaminaciones por virus o ruidos en la línea.

8.2.5 El script de instalación generado para el SecLi32

El script de instalación es el programa fuente a partir del cual se creará el ejecutable que distribuirá nuestra aplicación.

A los efectos de este estudio se decidió crear el paquete de instalación utilizado por la aplicación SecLi32, dicha aplicación es la aplicación insignia del Centro de Cómputos y técnicamente es una aplicación muy compleja dado que esta creada en base a la arquitectura Com, se compone de mas de 175 módulos independientes a instalar[39] sobre los que se debe llevar un acabado control a los efectos de no estropear la registry de windows con instalaciones que superpongan diversas versiones de alguno de esos módulos.

Luego de que se corrompe una registry la solución mas practica y estable pasa por la reinstalación del equipo, con esto damos una idea de lo delicado del tema.

8.2.5.1 Filosofía de la instalación

Uno de nuestros principales objetivos, es la estabilidad de los equipos a instalar.

Dicha estabilidad podría verse comprometida si se realizan instalaciones superpuestas de archivos del programa.

Es decir, el secli es un conglomerado de Dll y Ocx que implementan distintos casos de uso.

Tomemos por ejemplo el ocx PFICALUMNO.ocx.

Dicho modulo puede ser modificado y a la hora de actualizar las estaciones de trabajo alcanzara con sobrescribir el ocx anterior que no pasará nada., a menos que haya lo que se denomina “una rotura en la compatibilidad Binaria”, o dicho mas claramente que la firma electrónica interior del archivo difiera.

Dicha firma electrónica, es generada automáticamente por VB en el momento de compilar la componente, y denota un cambio en la interfase de la misma.

Ahora bien si borramos (sobrescribiendo por ejemplo con un archivo que se llama igual pero tiene distinta firma) al componente original, estaremos introduciendo inestabilidades en el registro del sistema.

[39] Ocx y Dll’s

Como además no podemos desinstalar fácilmente un componente si hemos perdido el archivo en cuestión, se adoptó una postura conservadora que consiste en los siguientes pasos:

1. Se desinstala todo lo que haya en los directorios destino
2. Se copian los nuevos archivos
3. Se instala

Con este enfoque se asegura que no se producirán problemas por pérdida de compatibilidad.

8.2.5.2 El Script en detalle

Lo que hace el script es:

1. Copia la utilidad MTSReg32[40]
2. Se invoca desregistrando todo
3. Se copian los ocx y dll nuevos
4. Se Llama nuevamente al MTSReg32 registrando todo

Para el desinstalador el paso 3 borra todo rastro del programa y el 4 por supuesto no existe.

8.2.5.3 Pasos necesarios para generar una instalación partiendo del script

A continuación se transcribe los cuatro pasos necesarios para generar la instalación del sistema de ejemplo. Claramente estos pasos se refieren al entorno de trabajo utilizado en el Consejo de Educación Secundaria, y carecerán de sentido en otros ambientes de desarrollo, se ponen aquí a los efectos de ilustrar el grado de simpleza obtenido en la generación de instaladores.

Instale el NSIS versión 2.0b2 que se encuentra en //alfa/software/util/nsis.

Entre a Sourcesafe[41], y hágase un check out del directorio \binarios\instalador, recursivo.

Dé clic derecho sobre el archivo Sec1Gui.nsi.

Elija Compile NSI with bz2.

Haga check in.

[40] es una utilidad que a diferencia del regsvr32 que solo registra de a un ocx o dll por vez, esta utilidad registra todos los ocx o dll que existan en determinada ruta facilitando enormemente la registración cuando hay dos centenas de ellos.
[41] Entorno controlado utilizado en el Centro de Cómputos

Y eso es todo, fácil no?

8.2.5.4 Resultado obtenido

El resultado final fue inmejorable, dado que desde diciembre que se esta utilizando el script desarrollado para este proyecto como el script para generar la instalación del sistema SecLi32 abandonando los paquetes de instalación utilizados con anterioridad-.

Además se ha expandido su uso para otros sistemas, incluso sistemas desarrollados hace tiempo han visto migradas sus instalaciones a esta herramienta.

Este sin duda ha sido un gran aporte de este proyecto a la operativa diaria y futura del Centro de Cómputos.

8.3 Antivirus para Centros Educativos

8.3.1 Introducción

Primeramente se hara una introducción genérica de las diferencias existentes entre un antivirus domestico y uno organizacional para luego llevarlo al caso concreto de los liceos.

Finalmente presentaremos el antivirus corporativo utilizado en la red central del CES y evaluaremos la conveniencia de su uso para los liceos.

Adicionalmente este capitulo cuenta con un apéndice donde damos una introducción básica al tema de virus y antivirus y que es un buen punto de partida si usted es ajeno al tema.

8.3.2 Virus en ambientes organizacionales

8.3.2.1 Introducción

Los principales problemas en una red no provienen solamente de los intrusos que interceptan la seguridad sino de la propagación de virus a lo largo y ancho de toda la red. La infección viral representa la mayor dificultad de todos los incidentes de seguridad y han creado tremendos problemas en organizaciones de todos los tamaños.

La protección contra virus en un ambiente corporativo es un problema difícil debido a la combinación de sistemas heterogéneos y el libre intercambio de datos a través de documentos compartidos, e-mail e Internet. Por lo tanto requiere una solución significativamente más robusta que la que se requiere en computadoras en el hogar.

Debido a la complejidad de una red corporativa y la realidad del comportamiento humano, la administración de un sistema antivirus de red introduce muchos problemas.

El mayor de ellos es la actualización del antivirus y su distribución uniforme a través de toda la organización.

Un elemento clave para proveer consistencia a lo ancho de la red es la capacidad para actualizar el software automáticamente en forma rápida y controlada.

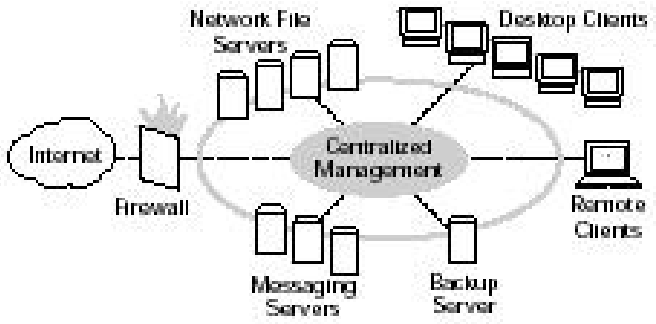
Otra característica importante de los antivirus es la generación de reportes, escribir en archivos log toda la actividad relacionada con los virus y centralizar la administración y el manejo del mismo.

Los administradores necesitaran de todos estas capacidades en la guerra continua contra los virus de computadoras.

8.3.2.2 ¿En qué se diferencia un antivirus corporativo de uno doméstico?

- Múltiples puntos de entrada de virus

  Una red corporativa consiste de muchos niveles de funcionalidad. Generalmente basado en arquitectura LAN, las cuales están interconectadas a través de switches a servidores de e-mail y a servidores de archivos, y conectados al mundo vía routers y gateways.



Antivirus y red corporativa

Estas redes tienen varios puntos claves a tener en cuenta por donde es posible la entrada de virus.

Primeramente a través de Internet, causado por los archivos infectados que se bajan por los navegadores o usando FTP.

En segundo término sistemas de mensajería que soporten adjuntar archivos de todo tipo y acceso remoto.

También las aplicaciones de grupo de trabajo son una amenaza, el hecho de compartir documentos a través de la red que es el corazón de estas aplicaciones, hace que jueguen un papel importante para el crecimiento de virus macro.

Otro punto de infección son las unidades externas (disqueteras, etc.).

- Problemas de escala

No es lo mismo disponer de 20 minutos para actualizar el antivirus en una computadora doméstica, que hacerlo para 100 computadoras, donde cada una lleva 20 minutos, lo cual se resume en 33 horas hombre, 4 días de trabajo exclusivos para actualización.

- Altos costos de propiedad, tiempos perdidos

No es posible hoy en día tener una persona dedicada exclusivamente a la administración de antivirus, simplemente por un tema económico, por lo tanto el administrador de la red es el que se encarga de estas tareas, seria un tiempo perdido para él dedicarle 4 días full-time a la actualización de antivirus.

- Crítico

Un solo virus que en ingrese en la red puede paralizar a toda la empresa y eventualmente provocar una catástrofe, es de fundamental importancia tener un respaldo actualizado.

Destacamos que los mismos virus afectan tanto a las estaciones de trabajo NT y Win98 como a los servidores NT, 2000, XP.

Es una buena política hacer respaldos diariamente ya sea en CD, cinta, zip, etc.

8.3.2.3 **Características deseables de un antivirus corporativo**

8.3.2.3.1 Administración del Domino centralizado

Para que un sistema de antivirus sea realmente efectivo, debe ser capaz de manejar un dominio completo de 100 o 1000 nodos como si fuera una sola entidad.

Las facilidades de administración del producto deben controlar toda la actividad potencial de virus en cada computadora y en cada punto de entrada a la red.

La clave para mantener el control en un dominio entero es la administración y manejo centralizado.

8.3.2.3.2 Cuarentena y seguimiento del origen

Un segundo aspecto del manejo completo del dominio es la capacidad de aislar clientes infectados.

Cuando un sistema de protección de nodo identifica una posible infección, la facilidad de control central debería ser capaz de terminar su acceso a la red. Esto previene que el virus se expanda. Una vez que todas las computadoras infectadas estén en cuarentena, la aplicación central deberá notificar al administrador.

Un software de antivirus inteligente también debería ser capaz de identificar el usuario loggeado en el momento de la infección y llevar un registro de usuarios que generalmente infectan el sistema pudiendo tomar las medidas pertinentes, además es posible identificar los focos más comunes de infección.

8.3.2.3.3 Alarmas y Alertas

Los administradores de redes deben ser notificados cuando se captura un virus en la red.

El sistema de alarmas y notificaciones debe tener un gran rango de opciones personalizables, como notificar el nivel de actividad de los virus, identificar quienes son

los administradores seleccionados cuando ocurren problemas, diferentes niveles de mensajes de texto para guardar en el archivo log.

El proceso de notificación debe incluir e-mail a los administradores, alertas en pantalla, entradas en el archivo log, Estas alarmas y alertas deben estar integradas al resto de la arquitectura del sistema de administración de la red.

8.3.2.3.4 Estado del Arte en la Identificación de Virus

El antivirus debe ser capaz de identificar un gran número de tipos de virus, cada tipo posee dificultades únicas relacionadas con su identificación, inoculación y reparación, y cada uno será detectado por de diferente forma.

Por lo tanto el antivirus que se use debe poder identificar cada uno de estos tipos y debe acomodarse a nuevos tipos de virus.

8.3.2.4 Características fundamentales para evaluar si un antivirus puede ser candidato a corporativo

Lista de requerimientos que un antivirus deberia cumplir para proveer suficiente protección para una red.

- Tener NCSA Certification.

  National Computer Security Association, es una asociación que provee una visión completa y objetiva de la industria del software antivirus y provee de un centro de información referente a nuevos virus.

  NCSA es un proceso de certificación formal en el cual se evalúa el antivirus siguiendo ciertas bases generales, su validez dura un año y cada dos meses se hacen rechequeos del software.

  Para que el antivirus pase el proceso de certificación debe ser capaz de detectar 100% de los virus que están en la "wild list" actual así como el 90% de los virus conocidos.

- Detectar y Curar virus en tiempo real

- Herramientas administrativas, manejo de dominio

- Consola de administración individual

- Instalación y actualización automática

- Interfaces gráfica fácil de usar

- Prevenir que estaciones de trabajo infectadas copien archivos a servidores
- Seguimiento del origen de la infección
- Poner en cuarentena estaciones de trabajo infectadas
- Debería permitir al resto del sistema continuar trabajando después que un virus se detectó, se aisló y se curó
- Actualización automática de definiciones de virus semanalmente en clientes y servidores
- Compatibilidad con navegadores de Internet populares
- Compatibilidad con SNMP existente
- Compatibilidad con diferentes plataformas de manejo centralizado
- Tener paredes para prevenir que los virus lleguen a los servidores
- Operación sobre, a través o detrás de firewall, proxies y hosts remotos

Otros aspectos importantes

- No requerir intervención humana, deben operar con o sin un humano presente. Automatizar la detección, la cura y la reparación alivia el problema de confiar en una persona para desempeñar estas tareas.
- No interferir con el desempeño del sistema, debe ser transparente para el usuario, usar poca memoria, ejecutarse rápido, no bajar la performance del sistema y actualizarse automáticamente.
- Multicapas, para que una solución sea efectiva, el módulo central debe ser capaz de ser expandido o extendido a través de componentes adicionales diseñados para agregar protección en puntos de entrada específicos.

8.3.3 Protección Antivirus para la Organización

La protección antivirus en una corporación requiere una solución mucho más robusta que la que requieren las computadoras aisladas o pequeñas redes.
Una red corporativa generalmente esta basada en arquitectura LAN que interconecta a través de switches los servidores de mail y archivos los cuales a su vez están conectados a Internet a través de routers y/o gateways, requiere una solución eficiente.

8.3.3.1 ¿Donde proteger la red?

Una de las mayores preguntas que se hacen los administradores de sistemas es donde se debe instalar el software antivirus. En una corporación, toda la información relevante se encuentra almacenada en los servidores de la red.

Estos Servidores de archivo son el primer punto de entrada de los virus. Para protegerlos los administradores deben realizar una protección a varios niveles. Es importante reconocer que la mejor protección es una solución a varios niveles que maneja 4 atributos principales:

INTEGRACIÓN – La solución debe incluir un desarrollo coordinado que integre todas los niveles de protección en un único paradigma.

UNICO PUNTO DE ADMINISTRACIÓN – Como un elemento esencial de esta solución integral debe haber un único punto de administración de la seguridad.

AUTOMATIZACIÓN – La solución debe incluir la actualización automática de los antivirus.

VARIAS CAPAS – La solución debe ser a varios niveles para asegurarnos que los componentes correctos están distribuídos de la forma más eficiente. Es necesario instalar el software antivirus en Servidores, Estaciones de Trabajo y Sistemas de Mensajería.

8.3.3.2 Gateways y Firewalls

Algunos sugieren que tiene sentido instalar todo el software antivirus en el gateway para prevenir la entrada de los virus a la red. Esta solución tiene como gran problema la degradación de la performance. Los gateways o routers son diseñados para leer el cabezal de un paquete y luego pasarlo a su destino final lo más rápido posible. Si deben realizar el chequeo de virus, el gateway o router debería recibir todos los componentes del archivo, reconstruirlo y almacenarlo temporalmente mientras se realiza el scaneo.

La performance del router o gateway se puede degradar muy rápidamente causando severos cuellos de botella dentro y fuera de la red.

8.3.3.3 Workstations

Es esencial tener una parte del software antivirus residiendo en cada una de las workstation de la red ya que este es uno de los principales puntos de entrada de los virus a la misma. Este enfoque tiene gran sentido porque toda la carga de trabajo es compartida por todas las computadoras del sistema, poniendo solo un pequeño overhead en cada estación.

A pesar de que un gran número de infecciones se producen por las bajadas de internet y los archivos adjuntos a los e-mail, todavía la fuente de infección más común (a nivel corporativo en el CES) sigue siendo el disquete. El scaneo en tiempo real se debe hacer en las workstations para mantener las infecciones fuera.

8.3.3.4 E-mail Servers

Los servidores de mail son el segundo lugar natural para el scaneo de antivirus. Dado que todos los mensajes de e-mail , los cuales son fuente primaria de infección , llegan a los servidores y son archivados en mailboxes antes de ser enviados a destino, es practico incluir software antivirus en los mismos. En un promedio de 100 a 1 entre workstations y servidores de mail, la relación costo eficiencia de esta solución tiene sentido. Desafortunadamente, esta solución no cubre todas las formas en las cuales los virus pueden entrar a las pc.

8.3.3.5 Backup Servers

Los servidores de Backup se utilizan para respaldar la información. Si los archivos de backup están corruptos , éstos no pueden ser utilizados con el fin de restaurar la información. El software de backup , como parte de su proceso, abre los archivos muchas veces. Esto provoca que el software antivirus scanee el mismo archivo varias veces. esto crea ineficiencia. Esto se complica con el hecho de que cuando un virus es detectado, el sistema se detiene hasta que se limpie .Proteger los backups de infecciones de virus, es esencial para mantener a salvo y segura la red.

8.3.3.6 Servidores de Internet y Servidores de Archivos

Cualquier lugar de la red donde residan archivos o bases de datos son posibles puntos a ser afectados por virus.

Una solución empresarial requiere software antivirus instalado en servidores de mail, servidores de archivos y workstations. Por encima de todo esto se necesita un esquema de administración que controle y garantice el éxito.

8.3.3.7 El Factor Humano

Mucha gente en un ambiente libre y descoordinado, tiene algún software antivirus generalmente desactualizado. Por ello es necesario que el sistema se actualice fácilmente y en forma regular. El antivirus debe tener un fuerte manejo centralizado y un alto nivel de funciones automatizadas (actualizaciones, notificaciones de infección, detecciones, limpieza, y reportes).

Un sistema empresarial de protección antivirus debe tener un esquema en el cual los administradores puedan exigir a los usuarios acatamientos. Esto va a prevenir que el usuario desactive la protección antivirus, por ejemplo. Podrán llegar a indicar que todo archivo público, privado o del sistema sea regularmente inspeccionado.

El manejo central del software antivirus reduce los tiempos de los administradores incluyendo la habilidad de actualizar la base de datos de los virus desde una única ubicación y setear los parámetros de chequeo para cada sistema de la empresa.

La habilidad de un software antivirus de detectar numerosos virus no es la única medida de su efectividad. También se debe tener en cuenta la habilidad para prevenir infecciones de virus, la gran cantidad de archivos, drives y sistemas que puede manejar y la facilidad para alertar al administrador sobre posibles infecciones y orígenes de virus.

8.3.3.8 Estructuración y Administración de Protección Antivirus

La estructura actual de las herramientas de protección antivirus, requiere cumplir los siguientes pasos: Planificación, Búsqueda, Testing, Mantenimiento y Estructuración del sistema.

PLANIFICACIÓN - Determinar que tipo de información o datos están presente en la red.
BÚSQUEDA – Identificar un software que se ajuste exactamente a las necesidades de la empresa.
TESTING – En un grupo reducido de equipos, instalar y testear el correcto funcionamiento, para asegurarse que funciona bien y es compatible con la red instalada y las aplicaciones.
MANTENIMIENTO – Asegurarse que el software puede ser administrado por el personal de la empresa y que se actualiza correctamente o sea que baje las actualizaciones con la lista completa de virus.
ESTRUCTURACION DEL SISTEMA - Una vez que está seguro que funciona como se espera, expandirlo a todo el sistema.

8.3.3.9 Protección Antivirus Continua

Desarrollar una buena solución puede requerir una o más de estas actividades:

a. Integrarla a la política de seguridad de la empresa.
b. Actualización inmediata de software.
c. Inspección manual de objetos o eventos sospechosos, tan pronto como son detectados.
d. Vigilancia continua y especial atención en las actualizaciones que puedan comprometer el sistema antivirus.
e. Educación de Usuarios Finales.
f. Cambiar la secuencia de booteo en el CMOS de las computadoras.
g. Ser proactivo en el testing y en fortalecer cada aspecto del sistema de defensa.

8.3.3.10 Desarrollar una Política Antivirus

Muchas organizaciones han aprendido que con solo instalar el producto antivirus no logran salvaguardar su red de infecciones.

Una solución es una política de organizacional que defina en forma clara cómo se debe establecer y mantener la protección antivirus.

Los siguientes items son esenciales para establecer una verdadera política antivirus y levantar una barrera a la infección.

ENFATIZAR EL SOFTWARE – calidad del software a instalar

EQUIPO RESPONSABLE – un equipo formado por dos o más personas entrenadas adecuadamente en el manejo de las infecciones de virus es esencial para una política de protección completa.

PREVENCIÓN AUTOMATICA – cada usuario debe ejecutar una herramienta de protección antivirus en todo momento.

ACTUALIZACIONES – la mejor protección es tener la última versión de los antivirus en el sistema. Actualizaciones automáticas.

BACKUP – Siempre tener un backup libre de virus. En caso de necesitarse que se pueda restaurar fácilmente la información.

SERVIDORES LIBRES DE VIRUS- el punto central de una red son los servidores de archivos, donde datos y servicios son almacenados y accesados. La política debe proteger los servidores de virus a cualquier costo.

IDENTIFICAR LOS RIESGOS – usuarios que repetidamente exponen la red a virus trayendo mucha transferencia de datos del exterior o que intentan evitar la barrera antivirus, deben ser sancionados e incluso retirados algunos de sus privilegios.

8.3.3.11 Conclusión:

La protección antivirus en grandes organizaciones es necesaria y una parte crítica en el desarrollo de una red hoy en día.

REQUIERE UN CONTROL CENTRALIZADO , ACTUALIZACIONES AUTOMÁTICAS Y REPORTES ESTADÍSTICOS.

Debe soportar múltiples plataformas, protocolos y variados tipos de archivos.

Debido a la complejidad creciente de las comunicaciones dentro de las organizaciones y entre las organizaciones, un desarrollo efectivo de una solución antivirus organizacional requiere un esfuerzo adicional. A pesar que la estrategia antivirus debe ser soportado por un software potente, la responsabilidad final de mantener a la organización libre de virus recae sobre el administrador de la red.

8.3.4 Antivirus en la red central del CES

8.3.4.1 Introducción

A lo largo de este documento hemos analizado las diferencias entre un antivirus para uso corporativo y uno para uso doméstico, así como también hemos extractado las principales características que debe exhibir un producto que merezca ser considerado antivirus corporativo.

A continuación se presentara como toda esa teoría ha sido llevada a la práctica en la red central del CES y en el siguiente capitulo se determinara si la experiencia es extrapolable a los liceos.

8.3.4.2 Presentación del caso de estudio

La red central de Secundaria presenta las siguientes características:

- LAN con 300 usuarios
- Más de 200 pcs
- Puntos con acceso discado a Internet
- Alrededor de 5 laptops con poco control
- Servidor de Mail corporativo
- Conexión a Wan con reconocidos problemas de virus
- Futura expansión a Wan de nivel nacional con más de 300 nodos
- Más del 80% del trabajo en plataforma Office

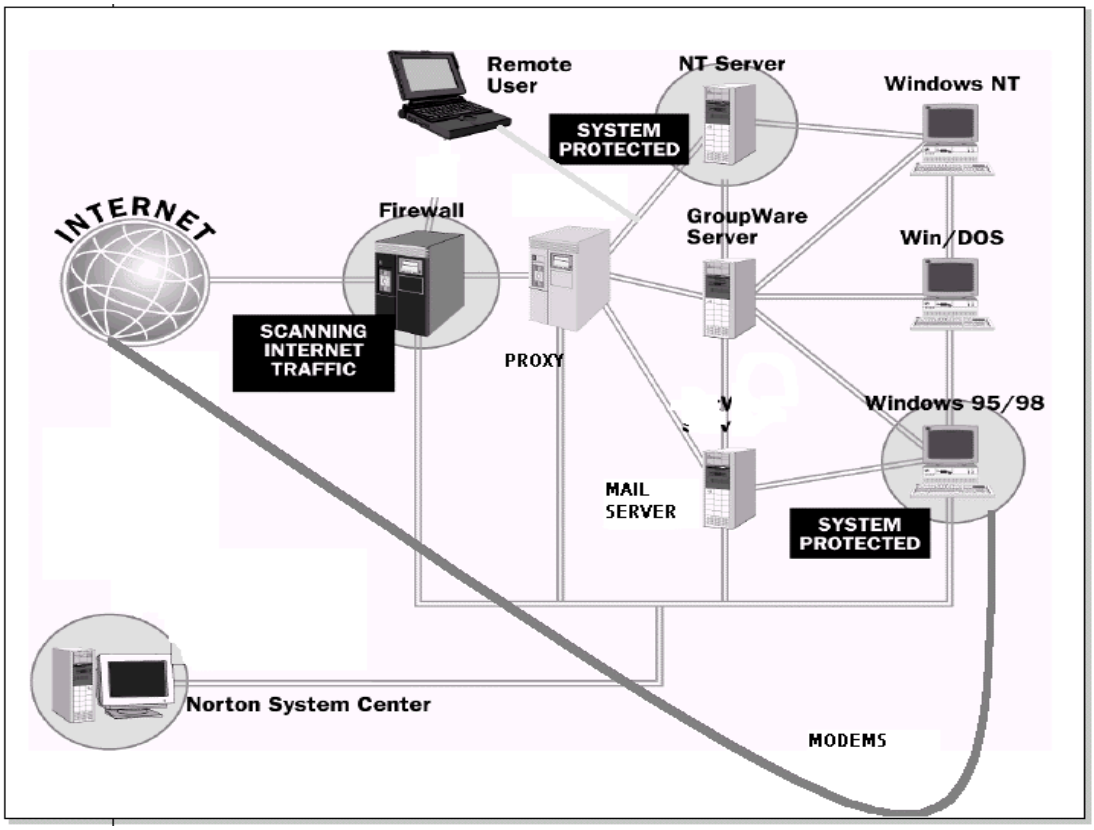
Para dar una imagen más vivida de la situación, se puede agregar que se trata de un organismo público, con oficinas distribuidas en dos edificios conectados por fibra óptica.

Los usuarios contaban con poca preparación en informática, dado que en un año se les había pasado de la máquina de escribir al Windows, salvo una ínfima parte que ya tenían computadoras Win 3.11 sin disco.

Por otro lado el departamento de soporte (que también realizaba tareas de help desk), contaba con un analista que cumplía las funciones de jefe de soporte, administración de red y desarrollo part-time y un par de funcionarios con nula formación en ambientes pc.

Al momento de abordar el problema, los esfuerzos para combatir virus se habían realizado de una forma esporádica, descordinada e infructuosa, pero el detonante para enfrentar seriamente al problema lo introdujo la puesta en marcha del servidor de correo.

A continuación analizaremos punto por punto cada aspecto de esta realidad, y que requerimiento se desprende de cada uno de ellos.



Esquema de red

8.3.4.2.1 Cantidad de usuarios

Como se señalo anteriormente en este capitulo, es necesario educar a los usuarios a través de políticas para que estos ayuden en el combate a la amenaza que suponen los virus.

Sin embargo en el caso del CES esto era imposible por dos razones

a) La alta cantidad y baja preparación de los usuarios unido a la poca gente disponible para formarlos hacía muy difícil la creación y correcta difusión de una política adecuada en materia de contención de virus.

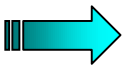
b) Anteriormente se habían impuesto políticas a subgrupos de usuarios pero dichas políticas o eran erróneas o fallaron por problemas tecnológicos (por ejemplo aspectos de dichas políticas indicaban que los datos debían ser guardados solo en diskette (para economizar espacio en el servidor), pero no preveían mecanismos de respaldo con lo que frecuentemente los usuarios perdían sus datos y adicionalmente los diskettes se convertían en reservorios de virus o por ejemplo se había impuesto so pena de sanciones que los diskettes debían ser escaneados… pero los escaners utilizados estaban desactualizados, con todo esto se había llegado a un exceptisismo generalizado de parte de los usuarios a políticas en este aspecto.

A partir de estas dos consideraciones se llegó a un primer requerimiento que fue que el sistema debería funcionar de forma autónoma, no requiriendo intervención del usuario y lo que es mas sutil, no *permitir* que el usuario intervenga, como forma de evitar errores involuntarios por desconocimiento.

8.3.4.2.2 Puestos de trabajo

La alta cantidad de puestos de trabajo y la poca gente disponible para su soporte trajo aparejado el segundo requerimiento, que la instalación sea desatendida, de forma que un solo técnico pudiera instalar múltiples puestos a la vez, y que considerando el bajo perfil técnico de la gente de soporte, ellos no tuvieran que dar ninguna indicación al proceso de instalación.

También el análisis detallado de este punto determinó un requerimiento más, que fue que tanto las definiciones de virus, así como los upgrades del producto se hicieran de forma automática y desatendida, y sobre todo que no fuera necesario una vez que se instala el sistema por primera vez volver a instalar ningún tipo de patch o upgrade de forma manual, sino que los mismos se instalaran de forma automática y desatendida por intermedio de la red.



Es importante considerar que la instalación de un producto en cada una de nuestras estaciones de trabajo y dado los recursos existentes, llevaría semanas, por lo que si frente a un nuevo tipo de virus se hiciera necesario instalar manualmente algún patch, tendríamos una ventana de tiempo muy considerable en la cual nuestra organización no estaría totalmente protegida.

8.3.4.2.3 Accesos externos a nuestra Lan

Tenemos tres posibles accesos externos a nuestra red

a) Laptops

b) Conexiones discadas a internet por parte de algunos equipos con módem

c) Conexión a una Wan por intermedio de la cual estamos conectados a Internet

El problema con los laptops radicaba en que se utilizaban para brindar soporte a los liceos de todo el país, lugares altamente contaminados por distintos tipos de virus, por lo que su conexión a nuestra Lan podía significar la expansión fulminante de un virus por la misma.

Si bien eran utilizados por personal técnico, este personal estaba mas orientado a la electrónica, y lo que es importante no estaba bajo la dirección del centro de cómputos, por lo que no se podía forzar ningún tipo de política sobre los mismos, finalmente el esquema de conexión a nuestra red se basa en DHCP, por lo que en principio era difícil impedir su conexión.

El problema con las conexiones discadas radicaba en que eran utilizadas por niveles gerenciales para chequear correo privado por intermedio del Outlook Express, lo que constituía un punto de entrada importante para distintos virus, nuevamente las gerencias no dependían del centro de cómputos y se negaban a perder este privilegio.

Finalmente la conexión a la Wan que nos proveía acceso a Internet era una nueva fuente de problemas, dado que tenia un historial importante de problemas con virus.

8.3.4.2.4 Servidor de Mail Corporativo

Cuando se planteó la introducción del servidor de mail corporativo se estableció que su puesta en marcha solo sería viable a largo plazo si a su vez, se trabajaba seriamente en el problema de los virus, pues si bien había pequeñas crisis periódicas con los virus, la introducción del correo brindaría la potencialidad necesaria para que estas pequeñas crisis se transformaran en catástrofes que afectaran a toda la organización.

En efecto, un solo virus que atacara por mail, podía reenviarse en la hora pico a los 200 pc's de las oficinas centrales en menos de un minuto, y según sus efectos poner fuera de servicio a toda la infraestructura informática en un momento.

8.3.4.2.5 Plataforma utilizada

Como si las dificultades planteadas fueran pocas, la mayoría absoluta del trabajo se realiza (por las propias características de la organización) en plataforma Office, blanco principal de los nuevos macro virus.

Utilizando una analogía médica, se tenía el caldo de cultivo necesario.

8.3.4.2.6 El futuro

Otro aspecto a considerar, es la expansión futura de la Lan, y aquí nuevamente teníamos cuestiones interesantes, dado que se está en un proceso de transformación de la misma en una Wan de alcance Nacional, por lo que de alguna manera se debería controlar el problema de los virus en la misma.

Es importante notar que a diferencia de una Wan de empresa, donde por lo general se trabaja con aplicaciones propias del negocio inmune a virus (salvo por supuesto cuando éstos afecten al Sistema Operativo), la gran mayoría del trabajo realizado por la organización es en base a Office.

8.3.4.3 Requerimientos

Con el análisis detallado de la realidad anteriormente expuesta se creó una lista de requerimientos que determinó las características que debía cumplir un producto antivirus para ser tomado en cuenta como solución a nuestro problema.

Como se verá, en la misma se dio prioridad a que facilite la administración, los costos de propiedad y que fuera una solución integral en materia de antivirus, es decir que cubra todas nuestras necesidades.

8.3.4.3.1 Lista

- ✓ Actualización desatendida y automática
- ✓ Fuerte protección anti macro virus
- ✓ Protección al servidor de mail
- ✓ Funcionamiento a prueba de usuarios
- ✓ Actualización de la lógica sin necesidad de reinstalar la aplicación
- ✓ Facilidad en el control centralizado de todas las instalaciones
- ✓ Amplia generación de informes
- ✓ Actualización muy frecuente de las definiciones
- ✓ Control por parte de los administradores de la configuración de las instalaciones

8.3.4.3.2 Aspectos relativos a la instalación

La instalación debía ser desatendida, esto es que una vez que se comienza a ejecutar no requiera ningún tipo de confirmación ni elección por parte del usuario.

CON ESTO BUSCÁBAMOS QUE EL PERSONAL DE SOPORTE PUDIERA POR EJEMPLO INSTALAR TODAS LAS MÁQUINAS DE UNA OFICINA A LA VEZ, PUES BASTABA CON QUE SE LANZARA EN CADA UNO DE LOS PC'S DE UNA OFICINA Y VER QUE TERMINARAN.

Adicionalmente buscábamos que el personal de soporte, no estropeara la configuración del antivirus, por elegir erróneamente una opción en el momento de instalar el paquete.

Es interesante señalar que una herramienta que cumpliera con este requisito podría ser lanzada de forma automática, por ejemplo desde un login script finalmente no utilizamos esta estrategia, porque dada la gran diversidad de nuestras plataformas (distintos W95, W98 y W98SE, NT, etc.) era difícil asegurar el correcto funcionamiento de un login script complejo en cada una de ellas sin pruebas que consumirían más tiempo que la instalación manual.

8.3.4.3.3 Protección anti macro virus

Obviamente necesitábamos una herramienta con un desempeño excelente en su defensa frente a este tipo de virus.

8.3.4.3.4 Protección al servidor de Mail corporativo

Siendo hoy en día Internet la principal fuente de virus, es claro que la protección del servidor de Mail es crítica.

Por un lado para evitar enviar mensajes desde nuestra organización contaminados, por otro impedimos que entren virus a nuestra organización y finalmente un resultado inesperado consistió en que actualmente las alertas del servidor de mail sobre que un usuario ha enviado un mail contaminado nos sirve de "alarma de emergencia" que nos ha alertado cuando algo no va del todo bien con algún cliente.

(clientes se denominan en este contexto a los antivirus instalados en los equipos de los usuarios)

8.3.4.3.5 Funcionamiento a prueba de usuarios

En este apartado se identificaron un montón de puntos interesantes, por ejemplo que su funcionamiento sea automático y no pregunte nada al usuario en ningún momento, es decir la experiencia nos demostró que ante la duda era mejor borrar un archivo que no estaba contaminado que dejar pasar un archivo contaminado.

Además algunos aspectos de funcionamiento no inmediatos, como por ejemplo medidas para contrarrestar que algunos usuarios utilizaran el crtl-alt-del para luego cancelar la aplicación.

Usuarios que entraban con "cancelar" y de esa forma no ejecutaban los programas que estaban en el grupo inicio, ni en el login script, etc.

8.3.4.3.6 Actualización de la lógica sin necesidad de reinstalación del programa

Como vimos, de tiempo en tiempo surge alguna nueva tecnología en materia de virus, que de la noche a la mañana torna obsoleto a los antivirus existentes.

Sin embargo la instalación de un patch o en el peor de los casos, la instalación de una versión nueva del antivirus, lleva mucho más tiempo, incluso semanas.

Es inadmisible que nuestra organización permanezca vulnerable por períodos tan extensos de tiempo, por lo que el producto elegido debía de proporcionar algún mecanismo que permitiera actualizar la lógica de la aplicación de forma automática, preferentemente con la distribución misma de las definiciones (signatures) de virus.

8.3.4.3.7 Cuestiones relativas a la administración

Finalmente, la solución debía proveer una consola de administración centralizada, actualizaciones frecuentes, seguimiento de eventos, sistema de alarmas, etc.

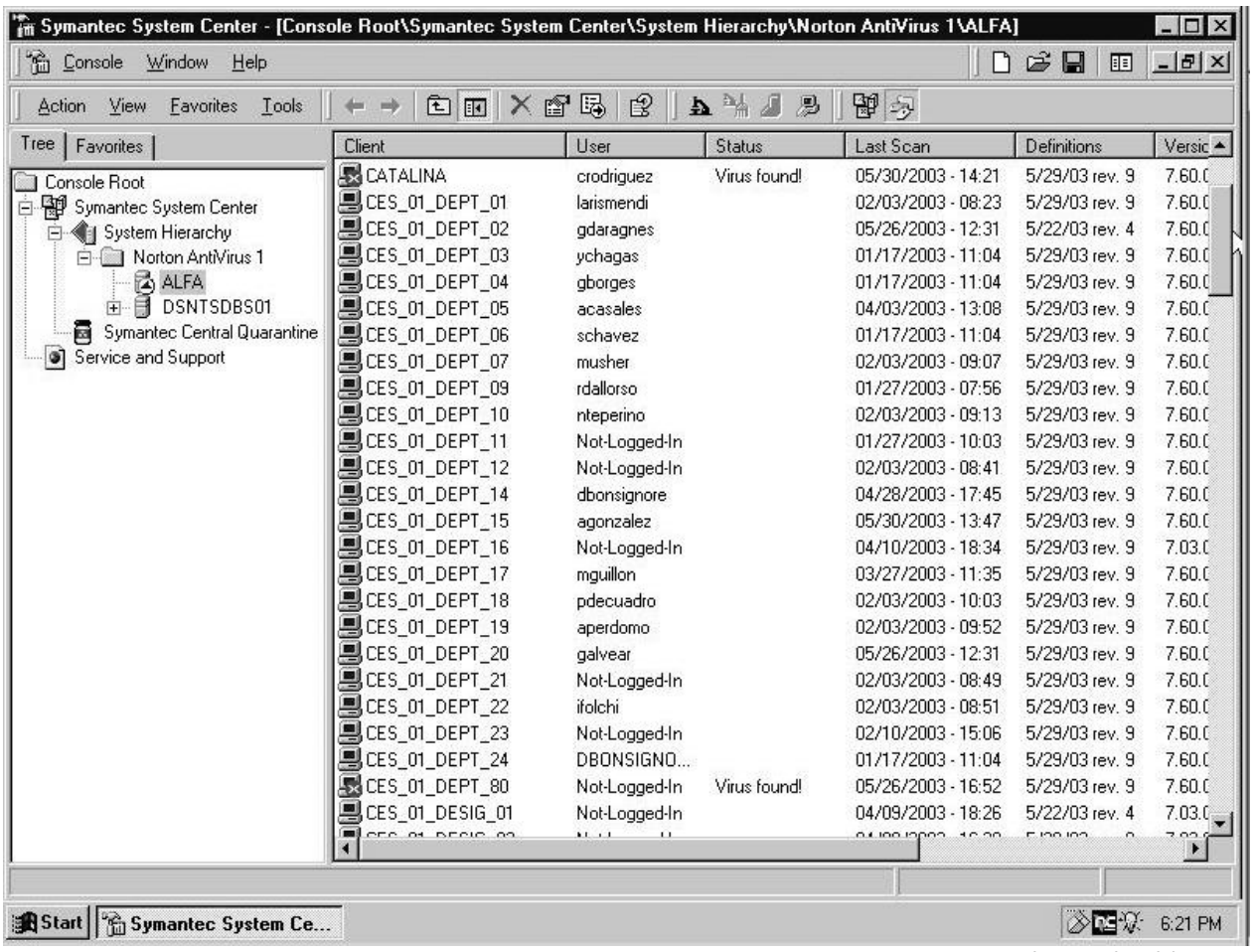
8.3.4.4 Producto elegido

Finalmente el producto oportunamente elegido en el Consejo de Educación Secundaria fue el Symantec (NAV) versión corporativa.

El mismo cumple con todos los requerimientos planteados y se ha constituido en una herramienta idónea para mantener a la organización libre de virus.

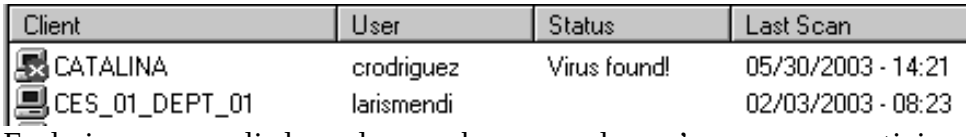
A continuación haremos una introducción al mismo y finalmente en el inciso 8.3.5 evaluaremos si es conveniente extender su uso a las redes liceales.

8.3.4.4.1 Pantallas



Consola central Antivirus

En la captura anterior vemos la consola central del Symantec Antivirus.



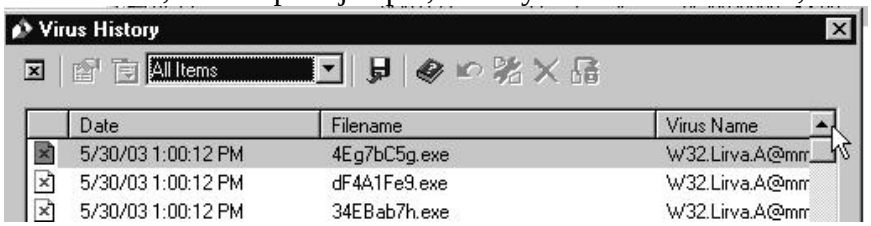
En la imagen ampliada podemos observar a dos pc's, uno cuyo antivirus detecto un virus y otro ok.

El producto nos informa además de que usuario estaba logeado y de la fecha y hora del ultimo escaneo.

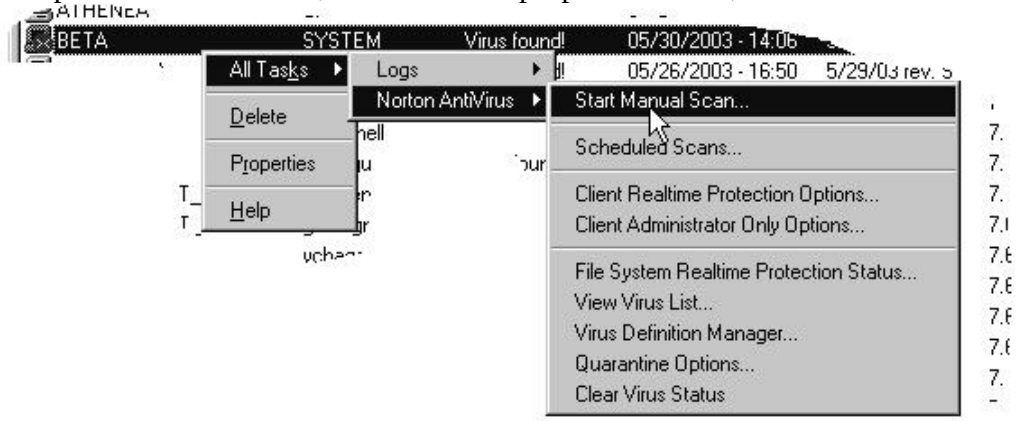
Definitions	Version	Scan E...	Address
5/29/03 rev. 9	7.60.0.926	4.1.0.15	(IP)-10.200.3.104
5/29/03 rev. 9	7.60.0.926	4.1.0.15	(IP)-10.200.3.106

A continuación nos indica la fecha de las definiciones en uso por el cliente, la versión del cliente, la versión de la scan engine (parte que se dedica a la detección propiamente dicha) y finalmente el ip de las maquinas en cuestión.

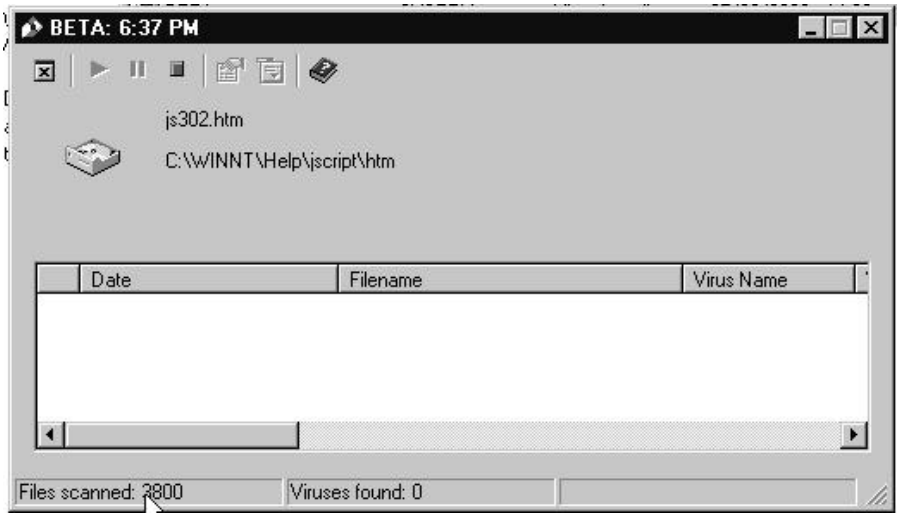
Luego de que hemos detectado un virus en una maquina procedemos a analizar la historia de la infección., viendo por ejemplo, fecha y hora de la infección, acción tomada etc.



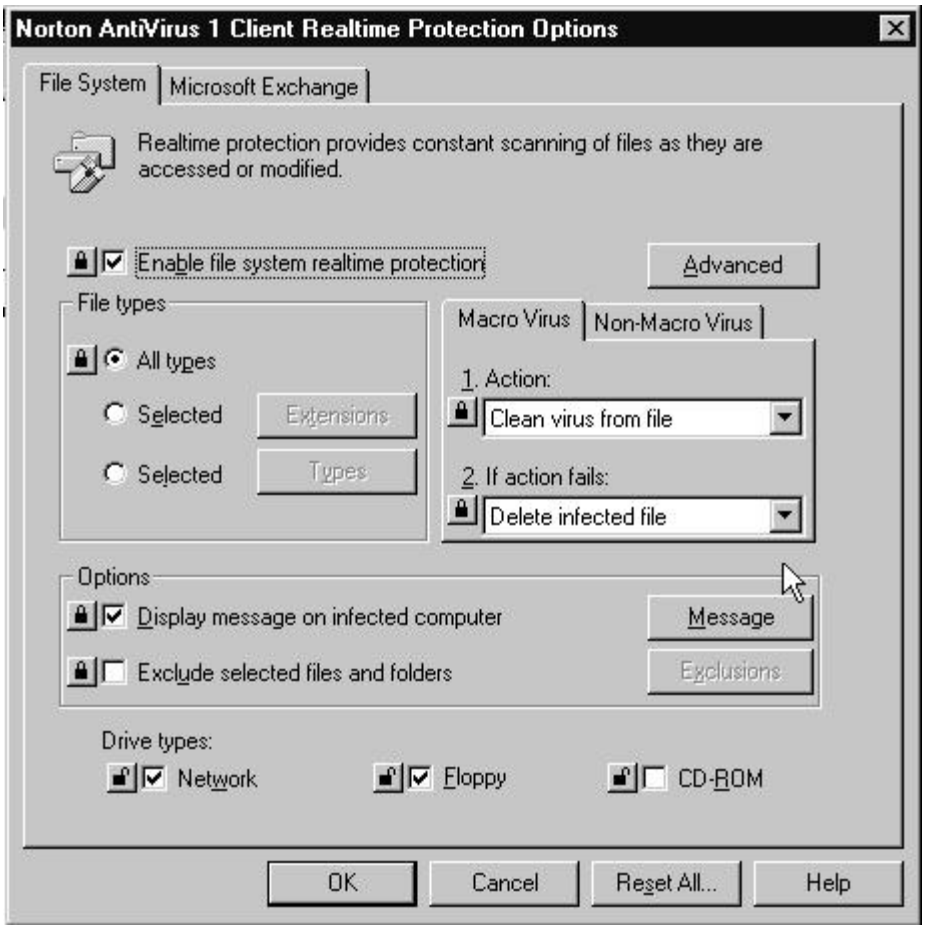
Luego normalmente tomaremos una acción correctiva, que puede ser por ejemplo escanear la computadora en cuestión, desde nuestro propio escritorio, sin necesidad de levantarnos de el.



¿cómodo no?


BETA: 6:37 PM
js302.htm
C:\WINNT\Help\jscript\htm
Date
Filename
Virus Name
Files scanned: 3800
Viruses found: 0

8.3.4.4.2 Pantalla de configuración de cliente



8.3.4.4.3 Esta es por ejemplo una de las pantallas desde donde configuramos las distintas opciones de comportamiento en el antivirus cliente.

Noten el dibujito del candadito al lado de cada opción.

Cuando ese candadito esta cerrado el cliente no puede hacer nada al respecto, el sistema solo tomara la acción indicada sin preguntar.

En este caso, como observaran, la únicas opciones que dejamos libres, son, que si desea escanear manualmente, le permitimos decidir si va a escanear el cdrom o no.
(También esta la posibilidad de escanear la red, pero para eso se precisa una contraseña adicional =)

8.3.5 Redes liceales

Dado que la experiencia recabada con el Norton Antivirus Corporate Edition, ha sido buena, era un fuerte candidato para ser utilizado en los liceos.

Primeramente verificamos que todas las características solicitadas para el antivirus en las oficinas centrales eran aplicables para los antivirus a utilizar en los liceos.

De hecho la diferencia mas significativa radicaba en que los clientes en los liceos podían pasar mas tiempo sin tener contacto con el servidor central que las maquinas normalmente conectadas en la red central.

Sin embargo mediante la correcta utilización del Live Update, se puede subsanar este problema y si no es asi, tenemos siempre a mano la consola de administración que nos indicará que pc's están desactualizados aunque no estemos conectados a los mismos ya que el servidor central de antivirus lleva un registro de cada maquina instalada de manera automatica.

Para lograr esto debemos instalar a los clientes liceales en modo "sometimes managed", dicho modo maneja las conexiones y desconexiones por periodos prolongados de manera automática.

Adicionalmente consideramos que contar con la misma herramienta con la cual ya estamos familiarizados consiste en una gran ventaja, evitando costos de recapacitación, licencias adicionales, etc.

8.3.6 Apéndice: Introducción a Virus y Antivirus

8.3.6.1 Introducción a Virus

8.3.6.1.1 Tipos de Virus

Archivo: Los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS, *.COM e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados. Este tipo de virus de dividen el dos:
Virus de **Acción Directa** que son aquellos que no se quedan residentes en memoria y se replican en el momento de ejecutar el fichero infectado y los virus de **Sobrescritura** que corrompen el fichero donde se ubican al sobrescribirlo.

Sector de Arranque: Este tipo de virus infecta el sector de arranque de un disquete y se esparce en el disco duro del usuario, el cual también puede infectar el sector de arranque del disco duro (MBR). Una vez que el MBR o sector de arranque esté infectado, el virus intenta infectar cada disquete que se inserte en el sistema ,ya sea una CD-R, una unidad ZIP o cualquier sistema de almacenamiento de datos.
Los virus de arranque trabajan de la siguiente manera: se ocultan en el primer sector de un disco y se cargan en la memoria antes de que los archivos del sistema se carguen. Esto les permite tomar total control de las interrupciones del DOS y así, pueden diseminarse y causar daño
Estos virus, generalmente reemplazan los contenidos del MBR o sector de arranque con su propio contenido y mueven el sector a otra área en el disco. La erradicación de un virus de arranque puede hacerse inicializando la máquina desde un disquete sin infectar, o encontrando el sector de arranque original y reemplazándolo en el lugar correcto del disco
Actualmente no constituyen una gran amenaza.

Stealth : Son virus que 'engañan' al sistema operativo para que cada vez que se lee un disco o archivo infectado éste pareciera estar limpio. De esta forma, los anti virus no podían verlo en un archivo cuando el virus estaba activo en memoria y en control del sistema operativo. Los antivirus solucionaron ésto buscando el virus en memoria por si estaba activo, y en disco por si no lo estaba.

Polimórficos: Estos virus son también llamados "mutantes" . Los virus polimórficos trabajan de la siguiente manera: Se ocultan en un archivo y se cargan en memoria cuando el archivo

infectado es ejecutado. Pero a diferencia de hacer una copia exacta de sí mismos cuando infectan otro archivo, modifican esa copia para verse diferente cada vez que infectan un nuevo archivo. Valiéndose de estos "motores de mutación", los virus polimórficos pueden generar miles de copias diferentes de sí mismos. A causa de esto, los rastreadores convencionales han fallado en la detección de los mismos. De hecho, la mayoría de las herramientas de rastreo utilizadas actualmente todavía no pueden detectar estos virus. Hay algunos antivirus que pueden detectar virus polimórficos observando eventos característicos que los mismos deben realizar para sobrevivir y expandirse. Cualquier virus, sin importar sus características debe hacer ciertas cosas para sobrevivir. Por ejemplo, debe infectar otros archivos y residir en memoria.

Tanto para los virus stealths como para los polimorficos se han necesitado actualizar la logica del programa del antivirus además de la lista de virus solamente.

Virus Oaxes*:* Son los que últimamente han aparecido, y difundido mucho, ya que no tienen código de programación alguno: Usan la desinformación y la ingenuidad humana (ya que mucha gente cree todo lo que le dicen por e-mail). Un ejemplo es el que aparecio últimamente donde un mail decia que borren el archivo sulfnbk.exe del directorio /windows/command, que era un virus. Dicho programa es un archivo del sistema, que si lo borramos, el sistema operativo Windows puede empezar a tener fallas. Es un ejemplo tipico de un virus que no puede ser combatido por antivirus sino por politicas.

Macro: De acuerdo con la Internacional Security Association, los virus macro forman el 80% de todos los virus y son los que más rápidamente han crecido en toda la historia de los ordenadores en los últimos 5 años. A diferencia de otros tipos de virus, los virus macro no son exclusivos de ningún sistema operativo y se diseminan fácilmente a través de archivos adjuntos de e-mail, disquetes, bajadas de Internet, transferencia de archivos y aplicaciones compartidas. Los virus macro son, sin embargo, aplicaciones específicas. Infectan las utilidades macro que acompañan ciertas aplicaciones como el Microsoft Word y Excel, lo que significa que un Word virus macro puede infectar un documento Excel y viceversa. En cambio, los virus macro viajan entre archivos en las aplicaciones y pueden, eventualmente, infectar miles de archivos.
Los virus macro son escritos en Visual Basic y son muy fáciles de crear. Pueden infectar diferentes puntos de un archivo en uso, por ejemplo, cuando éste se abre, se graba, se cierra o se borra. Lo primero que hacen es modificar la plantilla maestra (normal.dot) para ejecutar varias macros insertadas por el virus, así cada documento que abramos o creemos, se incluirán las macros "víricas". Con la posibilidad de contener un virus convencional, cambiar un ejecutable o DLL e insertarlo en el sistema.

Virus del Mirc: Son la nueva generación de infección, aprovechan la ventajas proporcionadas por la Red y de los millones de usuarios conectados a cualquier IRC a través del Mirc. Consiste en un script para el cliente de IRC Mirc. Cuando se accede a un canal de IRC, recibe por DCC un archivo llamado "script.ini". Por defecto, el subdirectorio donde se descargan los archivos es el mismo donde esta instalado el programa, esto causa que el "script.ini" original se sobrescrito por el "script.ini" maligno. Bueno después de lo dicho nos preguntaremos ¿y para en que nos afecta a nosotros? Pues muy fácil, los autores pueden desconectarte del IRC o acceder a información privada,(archivo de claves o el "etc/passwd" de Linux).

VBS: Debido al auge de Internet los creadores de virus han encontrado una forma de propagación masiva y espectacular de sus creaciones a través mensajes de correo electrónico, que contienen archivos **Visual Basic Scripts**, anexados, los cuales tienen la extensión **.VBS**

El antiguo **D.O.S.** empleaba archivos **.BAT** (Batch), que eran un conjunto de instrucciones o comandos en lotes. Con el advenimiento de Windows 95/98/NT/Me/2000/XP, este tipo de archivos dejó de ser empleado y fue reemplazado por los **Visual Basic Scripts**. Un Visual Basic Script es un conjunto de instrucciones lógicas, ordenadas secuencialmente para realizar una determinada acción al iniciar un sistema operativo, al hacer un Login en un Servidor de Red, o al ejecutar una aplicación, almacenadas bajo un nombre de archivo y extensión adecuada. Los Scripts pueden ser interpretados y ejecutados por el Sistema Operativo Windows, Novell, etc. o por una aplicación mIRC, pIRC, AutoCad, etc. Los virus pueden ser desarrollados en cualquier lenguaje y tener determinados objetivos de daño y algunos simplemente usan las instrucciones Visual Basic Scripts, como medios de propagación. Asimismo, un VBS puede contener instrucciones que afecten a los sistemas. También es posible editar instrucciones en la Libreta de Notas (NotePad) y guardar el archivo con la extensión **.VBS**.

Actualmente existen 2 medios de mayor difusión de virus en VBS:

1. Infección de canales IRC
(el chat convoca a una enorme cantidad de "victimas")

El IRC (Internet Relay Chat) es un protocolo desarrollado para permitir la comunicación entre usuarios de Internet en "tiempo real', haciendo uso de software especiales, llamados "clientes IRC" (tales como el mIRC, pIRCh, Microsoft Chat). Mediante un software de chat, el usuario puede conectarse a uno o mas canales IRC, pero es necesario que primero se conecte a un servidor chat, el cual a su vez, está conectado a otros servidores similares, los cuales conforman una red IRC. Los programas "clientes IRC" facilitan al usuario las operaciones de conexión, haciendo uso del comando /JOIN, para poder conectarse a uno o mas canales. Las conversaciones pueden ser públicas (todo el canal visualiza lo que el usuario digita) o privadas (comunicación entre 2 personas).Para "cargar" una sesión de chat los usuarios deben registrarse en un servidor chat, elegir un canal y un apodo (nickname). Todo esto se hace mediante un denominado "bachero", que emplea comandos propios del protocolo IRC, permitiendo ejecutar estas operaciones de manera intuitiva y proporcionando al usuario un entorno gráfico amigable.

Como atacan los gusanos (VBS/Worms)

Todos los gusanos del Chat, siguen el mismo principio de infección. Usando el comando SEND file, envían automáticamente una copia del SCRIPT.INI a todas las personas conectadas al canal chat, además de otras instrucciones dentro de un Visual Basic Script. Este script que contiene el código viral sobre-escribe al original, en el sistema remoto del usuario, logrando infectarlo, así como a todos los usuarios conectados a la vez, en ese mismo canal. Este tipo de propagación de archivos infectados, se debe a la vulnerabilidad de las versiones de mIRC anteriores a la 5.31 y todas las versiones de PIRCH, antes de PIRCH98.

2. Re-envío de mensajes de la libreta de direcciones Microsoft Outlook.

Office 95/97/2000/XP, respectivamente, integran sus programas MS Word, Excel, Outlook y Power Point, haciendo uso del lenguaje **Visual Basic for Aplications**, que permiten invocar la ejecución de determinadas instrucciones. En MS Word y Excel, el usuario tiene acceso a un Editor de Visual Basic. Aunque también pueden editar instrucciones y comandos con el NotePad y archivarlo con la extensión **.VBS**

Virus como el **W97M/Melissa** o el **VBS/Loveletter**, al ser escritos en Visual Basic for Aplications, tienen un fácil y poderoso acceso a los recursos de otros usuarios de MS Office. El mas afectado es la libreta de direcciones de MS Outlook, el cual es controlado por las instrucciones del VBS y recibe la orden de re-enviar el mensaje con el archivo anexado, en formato VBS, a todos los nombres de la libreta de direcciones del sistema de usuario infectado.

Estas infecciones también se reproducen entre todos los usuarios de una red, una vez que uno de sus usuarios ha sido infectado.

8.3.6.1.2 Introducción:

El problema para los desarrolladores de antivirus es discriminar con certeza entre virus y no virus sin producir un mayor impacto sobre la utilidad de la computadora.
Para evaluar software antivirus hay que determinar cual es el mas exitoso discriminando entre virus y no virus.

ESTRATEGIAS

En el mundo de los desarrolladores de antivirus hay dos estrategias en la lucha contra los creadores de virus: " Jugar primero" quiere decir predecir lo que el autor del virus va a hacer y "Jugar segundo" es reaccionar a lo que el autor del virus ha hecho.
Hay ventajas obvias al reaccionar a lo que el creador del virus ha hecho pues en este escenario el desarrollador puede analizar los métodos del creador del virus y asegurar la detección del mismo limitando la capacidad del virus de extenderse.
La gran mayoría de los virus pueden ser detectados por un buen software de antivirus antes de que ellos estén en estado "salvaje".
"Jugando Primero" puedo solo trabajar si puedo identificar con precisión lo que el autor del virus esta planeando. En la práctica dicha predicción no es fácil.

8.3.6.1.3 Tipo de Antivirus

Sobre acceso (ON ACCESS): Chequea cuando los archivos son accedidos. Cuando lo implementemos debe ser invisible al usuario ellos no saben que se esta corriendo un antivirus hasta que se intercepta un virus, por eso es el tipo mas popular de productos de antivirus.

Sobre demanda (ON DEMAND): Solo se ejecuta cuando el usuario le dice que se ejecute. Con este método el usuario tiene que recordar revisar archivos y disqueteras frecuentemente.

Podemos clasificar los antivirus como:

- Herramientas de detección:
  Detectan la existencia de virus en una variedad de puntos en el sistema. El virus puede estar activamente ejecutándose, residiendo en memoria o almacenado en un código ejecutable. Puede ser detectado antes, durante o después de su ejecución y replicación.
- Herramientas de Identificación:
  Se usan para identificar que virus han infectado un ejecutable en particular.
- Herramientas de borrado

En muchos casos, una vez que un virus ha sido detectado, este es encontrado en numerosos sistemas o en numerosos ejecutables. Las herramientas de borrado intentan hacer más eficiente la tarea de recuperación del sistema borrando el código del virus del ejecutable infectado

8.3.6.1.3.1 Scanners: (Detección, Identificación, Borrado)

- Ventajas
  Muy pocas falsas alarmas
  Juega segundo
  Puede usualmente desinfectar archivos infectados.

- Desventajas
  Necesita actualización frecuente
  Puede tener problemas con virus polimórficos.

8.3.6.1.3.2 Analisis Heurístico (Detección)

Es la técnica de scanear un archivo que contiene técnicas y código sospechoso.

- Ventajas
  No necesita actualizarce con tanta frecuencia como el scanner.

- Desventajas
  Tiende a dar falsas alarmas, puede dejar pasar por alto virus.

Tiene que reactualizar su logica cada cierto periodo de tiempo cuando aparecen nuevos tipos de virus (ej:stealt,polimorficos,etc)

En la actualidad los antivirus utilizan una combinación de las dos técnicas Scanner y Heurística.

8.3.7 Bibliografía

Guía para la selección de antivirus:

http://www.alw.nih.gov/Security/FIRST/papers/virus/selguide.ps

A Guide to Evaluating Anti-Virus Software http://vx.netlux.org/lib/aas04.html

The Anti-Virus Strategy System http://vx.netlux.org/lib/asg08.html

Evaluating Anti-Virus Solutions Within Distributed Environments

http://vx.netlux.org/texts/html/McAfee/antivirs.html

Lower IT Costs Through Better Anti-Virus Management
http://www.symantec.com/avcenter/reference/nvxwp2b.pdf

Deploying Enterprise-wide Virus Protection:
http://www.itpapers.com/cgi/PViewIT.pl?scid=276&paperid=8044

Can Cryptography Prevent Computer Viruses?
http://www.research.ibm.com/antivirus/SciPapers/VB2000JFM.htm

Los Virus y la telefonía móvil: relación, mito y realidad
http://www.deepzone.org/editions/virgsm/virus&gsm.htm

Zona Virus

http://www.zonavirus.com

Wild List

www.wildlist.org

8.4 Virtual Private Network

8.4.1 Introducción

En la topología de comunicaciones finalmente adoptada los comunicaciones no pasan por una red pública en el sentido estricto del termino, pero ciertamente todas nuestras comunicaciones pasan por un proveedor externo a la organización (AntelData).

Teóricamente alguien con acceso a la red de AntelData podría llegar interferir en nuestras comunicaciones adulterando por ejemplo información.

En el caso de la aplicación que nos ocupa es bastante remoto que esto ocurra sencillamente porque el adulterar estos datos no da ninguna utilidad practica, y el único posible beneficiario es el personal del liceo que recibe las partidas quien es además el encargado de liquidarlas por lo que si quisiera directamente introduciría información falsa sin necesidad de hackear la seguridad de la red, amen que dicha tarea no es nada fácil.

Por otro lado podrían existir sistemas en el futuro a los cuales si fuera interesante modificar sus datos en el camino desde el liceo a las oficinas centrales, es por eso que a modo de completitud en la solución presentada introducimos el tema de VPN, con un enfoque meramente teórico y que es tan solo el punto de partida para futuros trabajos.

Es importante señalar que el presente trabajo esta basado en “Redes inalámbricas y redes privadas virtuales”[42]

[42] Autores: Fabricio Álvarez, Rodolfo Amador, Germán López, Karina Medina, Ana Inés Mora, presentado en la electiva Administración y Seguridad de Sistemas, 2003.

8.4.2 Introducción a VPN

8.4.2.1 ¿ Qué son las Redes Privadas Virtuales ?

Una Red Privada Virtual [1] es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando una red pública (como Internet) como medio de transmisión.

Dado que una VPN no necesita una línea dedicada, cualquiera con acceso a Internet puede usar una. Una vez conectados, los empleados pueden tener acceso a toda la red, como lo tendrían si estuvieran en la oficina. A pesar de que la conexión VPN usa la infraestructura publica, contiene propiedades de seguridad que hacen el acceso inapropiado a los datos muy difícil.

8.4.2.2 Antecedentes

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener cada una, una red local a la sucursal que operaba aislada de las demás. Cada una de estas redes locales tenia su propio esquema de nombres, su propio sistema de e-mail, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

Con el paso del tiempo, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services (RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual mas una tarifa por el uso, en el que se tienen en cuenta la duración de las llamada y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo pais pero en distintas áreas telefónicas y además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia con lo que los costos se incrementan.

Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN mediante lineas telefónicas y al servicio RAS, bajando los costos de estos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

8.4.2.3 ¿ Para qué una VPN ?

Cuando deseo enlazar mis oficinas centrales con alguna sucursal u oficina remota tengo 3 opciones [2] :

- MODEM: La desventaja es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia. Aparte no contaría con la calidad y velocidad adecuadas.

- LINEA PRIVADA: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

- VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

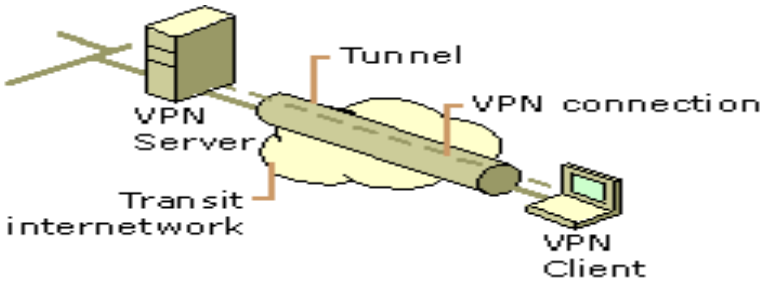
En resumen una Red Privada virtual [1] es una alternativa a medio camino entre la seguridad y garantía que ofrecen las redes totalmente privadas y lo asequible y escalable del acceso a través de Internet.

8.4.2.4 ¿Cómo funciona una VPN?

Una VPN funciona de la siguiente manera:

- Para emular una conexión punto a punto, los datos son encapsulados con un header que provee información de ruteo, permitiendo así que puedan atravesar la red publica hasta alcanzar su destino.
- Para simular una conexión privada los datos a ser enviados son encriptados, obteniendo así confidencialidad. Los paquetes que son interceptados en la red publica por terceros son indescifrables sin las claves de encriptación.

La porción de la conexión en la cual los datos privados son encapsulados es conocida como **túnel**, y la parte en la cual los datos son encriptados es conocida como la **conexión VPN**.



Esquema VPN

Existen dos tipos de técnicas de encriptación que se pueden utilizar en una VPN: encriptación de clave secreta o privada y encriptación de clave pública. Ya que debe ser realizada en tiempo real, los flujos encriptados a través de una red son encriptados utilizados encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

8.4.2.5 Requerimientos básicos para las VPN

Típicamente cuando se implanta una solución a la conexión remota a una red, es porque la empresa necesita facilitar un acceso controlado a los recursos e información de la compañía.
La solución debe permitir **roaming**, o clientes remotos conectados a los recursos de la LAN y debe permitir que oficinas remotas se conecten a otras y compartan recursos e información (router-to-router conections). A su vez, la solución debe asegurar la privacidad e integridad de los datos cuando atraviesan Internet.

Por lo tanto, cuando se desea implantar una VPN hay que asegurarse que esta proporcione lo siguiente [4] :

- **Autenticación de usuarios**.

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Asimismo, debe proporcionar registros de auditoria y contabilidad que muestren quién accedió, que información y cuando.

- **Administración de direcciones**.

La VPN debe establecer una dirección de cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

- **Encriptación de datos**.

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

- **Administración de claves de encriptación**.

La VPN debe generar y renovar las claves de encriptación para el cliente y el servidor.

- **Soportar múltiples protocolos**.

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX), entre otros.

Una VPN sobre Internet, basada en el protocolo Point-to-Point Tunneling Protocol (PPTP) o Layer Two Tunneling Protocol (L2TP), cubren todos estos requerimientos básicos. Otras soluciones, como por ejemplo el Internet Protocol Security (IPSec), cubren solo algunos de estos requerimientos, pero resultan muy convenientes para algunas situaciones específicas.

8.4.3 Clasificación de las Redes Privadas Virtuales

Las VPN se clasifican en [1] :

8.4.3.1 VPNs de lugar a lugar

Son el sucesor de las redes de área extensa (WAN) y se utilizan entre puntos fijos, que están conectados permanentemente.

8.4.3.2 VPNs de Acceso Remoto

La evolución del servicio de acceso remoto (RAS) mediante módem, permiten el acceso a la red de la empresa desde cualquier lugar del mundo por el precio de un llamada local.

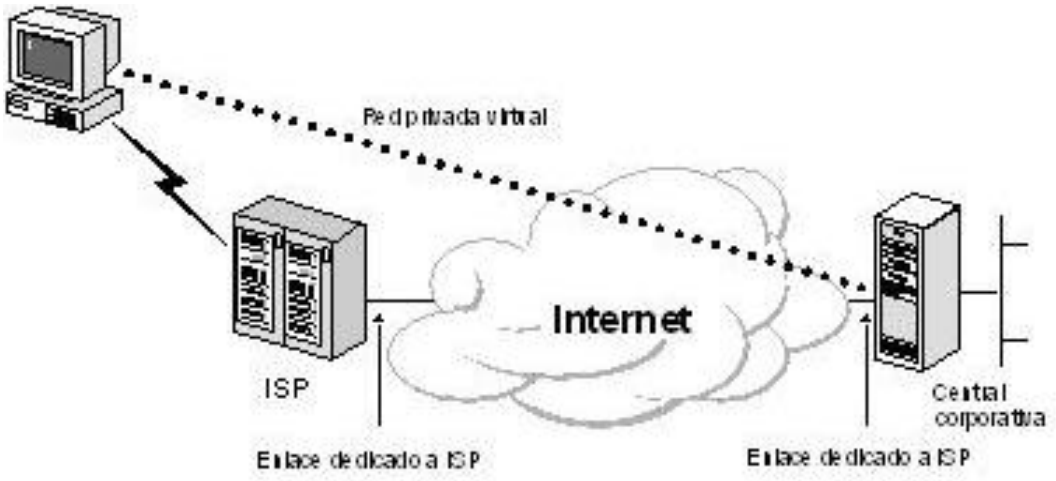
8.4.3.3 VPNs Mixtas

Son el caso más normal, redes con usuarios fijos, conectados siempre a ellas, como empresas con delegaciones dispersas, y con usuarios móviles, como consultores, que necesitan trabajar con los datos corporativos en cualquier lugar del mundo, pero a un coste moderado.

8.4.4 Usos comunes de VPNs

8.4.4.1 Acceso de usuario remoto a través de Internet

Las VPNs [4] deben proporcionar acceso remoto a los usuarios de la corporación a través de Internet, y al mismo tiempo conservar la privacidad de la información (Ver Figura).



VPN sobre internet

En vez de tener que utilizar una línea alquilada o hacer una llamada de larga distancia a un servidor de acceso a red corporativo o externo (NAS), el usuario debe llamar a un número telefónico local NAS de ISP, posteriormente, el software de la VPN crea una red privada virtual entre el usuario que marca y el servidor corporativo de VPN a través de Internet.

8.4.4.2 Conexión de redes a través de Internet

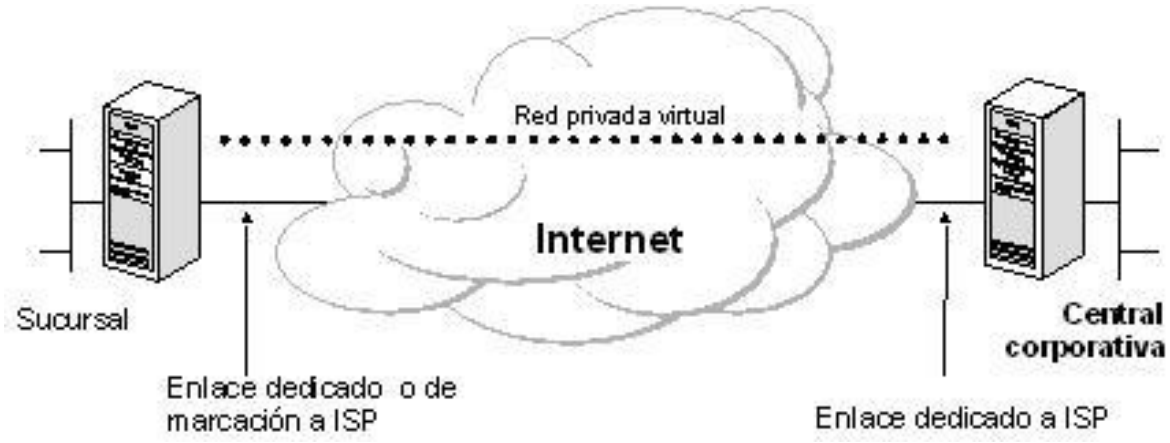
Existen dos formas de usar VPN [4] para conectar dos LAN en sitios remotos. (Ver Figura)

- **Usando líneas dedicadas para conectar una sucursal a la LAN de la compañía.**

En este caso, tanto los routers de la sucursal como los de la central corporativa pueden usar un circuito local dedicado y un ISP local para conectarse a Internet. El software de VPN utiliza las conexiones locales a los ISPs e Internet pública para crear una red privada virtual entre el router de la sucursal y el router corporativo.

- **Usando una línea de discado para conectar una sucursal a la LAN de la compañía.**

En este caso el router de la sucursal llama al ISP local. El software de VPN usa la conexión al ISP local para crear una VPN entre el router de la sucursal y el router de la compañía a través de Internet.

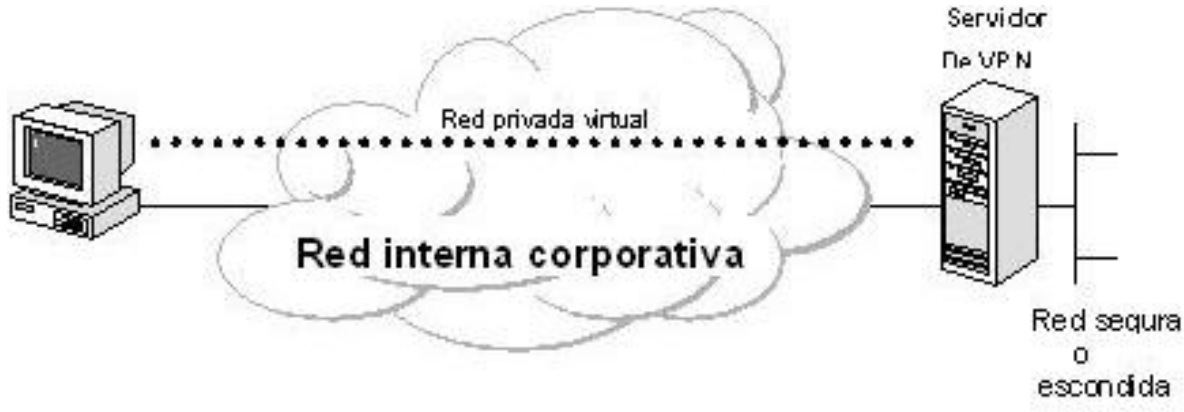


VPN para simular Wan

En ambos casos, las conexiones desde la filial y desde la corporación a Internet son locales. El router de la compañía que actúa como servidor de VPN debe estar conectado al ISP local con una línea dedicada, ya que este servidor debe estar escuchando las 24 horas del día por trafico VPN entrante.

8.4.4.3 Conexión de computadoras a través de una Intranet.

En algunas compañías [4], el departamento de datos tiene su LAN físicamente desconectada del resto de la Intranet de la corporación. Aunque esto protege la confidencialidad de la información del departamento, también crea problemas de accesibilidad a la información para aquellos usuarios que no están físicamente conectados a esta LAN. Una VPN permite que la LAN de un departamento este físicamente conectada a la Intranet de la compañía, pero separada por un VPN server. El cual puede ser configurado para que solo aquellos usuarios con los permisos apropiados puedan establecer la conexión con esta LAN y tener acceso a los recursos del departamento. Adicionalmente, todas las comunicaciones a través de la VPN va a ser encriptada para mayor confidencialidad. Aquellos usuarios que no tienen los permisos adecuados no verán la LAN del departamento.



VPN para confidencialidad de sub redes

8.4.5 Efecto Túnel

8.4.5.1El concepto de túnel

8.4.5.1.1 ¿Qué es un túnel?

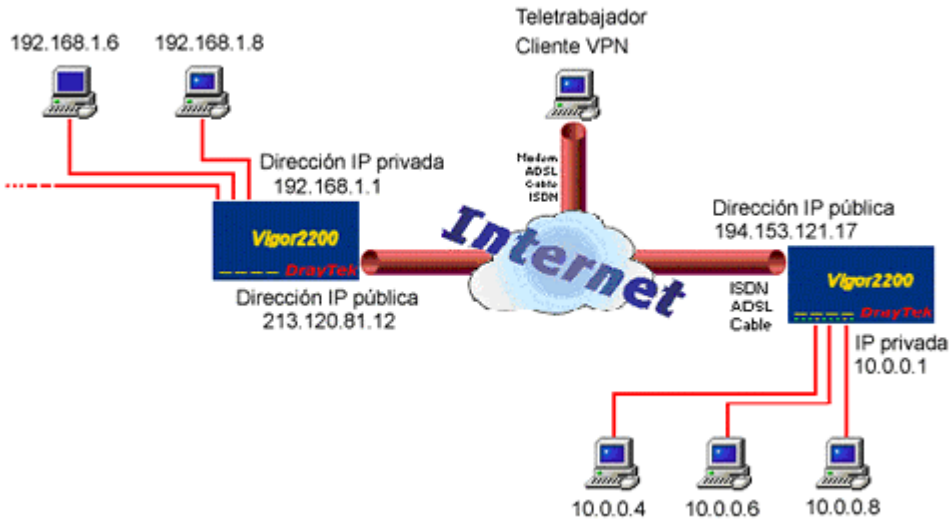
La unión de oficinas remotas o teletrabajadores se podría realizar a través de Internet. Esto es técnicamente posible utilizando direcciones IP públicas, pero sería altamente inseguro. Una VPN crea un túnel a través de Internet para hacer la comunicación más segura.

Entonces bien ¿qué es un túnel?. Un túnel es básicamente una unión punto a punto que utiliza una fuerte encriptación. De esta manera, aunque el túnel utilice una red pública como es Internet, los datos que circulan por el túnel están encriptados. Fuera del túnel los dos routers utilizan direcciones IP públicas (estáticas o dinámicas según sean proporcionadas por el proveedor de servicios) pero dentro del túnel las redes locales utilizan rangos de direcciones privados (por ejemplo 192.168.1.1 a 192.168.1.254) que no son accesibles desde Internet. Esto puede sonar muy complicado pero la analogía con un túnel es muy didáctica.

8.4.5.1.2 El Ejemplo del túnel

Imagine la diferencia entre viajar de Francia a Inglaterra cruzando el Canal de la Mancha en un pequeño barco frente a hacerlo por el Eurotúnel. Si cruza por el Canal de la Mancha, cualquiera puede verle, ven el barco en que viaja, la mercancía que transporta e inclusive podría ser capturado (no hay seguridad ni privacidad ninguna). Sin embargo, a través del túnel, incluso siguiendo la misma trayectoria, no es posible abandonar el túnel o entrar en el más que a través de las entradas designadas, que están bajo vigilancia.

Un observador externo no podrá ver a tres hombres en un barco, sino un túnel que pudiera contener algo o nada.



8.4.6 Tipos de Túneles

Los túneles pueden ser creados de varias maneras [4] :

8.4.6.1 Túneles voluntarios

Los túneles voluntarios se presentan cuando una estación de trabajo o un servidor de enrutamiento el cual utiliza el software de cliente de túnel establecen una conexión, deben tener instalados los protocolos adecuados para crear una conexión virtual al servidor de túnel objetivo.

Si la computadora está conectada a una red LAN, la computadora cliente ya tiene una conexión con la red interna que puede proporcionar el direccionamiento de los datos encapsulados al servidor de túnel de LAN seleccionado.

En caso de no estar conectada a una red LAN, la computadora cliente debe establecer una conexión de discado con la red interna antes de que pueda establecer un túnel.

8.4.6.2 Túneles obligatorios

Los túneles obligatorios se presentan cuando la computadora del usuario no es el punto final del túnel, sino que otro dispositivo como el servidor de acceso remoto entre la computadora de usuario y el servidor de túnel, es el punto final de túnel y actúa como el cliente de túnel.

La computadora o dispositivo de red que proporciona el túnel para la computadora cliente se conoce como procesador central (FEP) en PPTP, un concentrador de acceso L2TP (LAC) en L2TP, o una central internacional de seguridad de IP en IPSec.

8.4.6.3 Protocolos de túnel

Para que un túnel pueda ser establecido, tanto el cliente como el servidor del túnel deben usar el mismo protocolo de túnel.

La tecnología de túnel puede estar basada en protocolos de capa 2 o capa 3 (estas capas hacen referencia al modelo OSI). Los protocolos de capa 2, corresponden a la capa de enlace de datos y usan **frames** como unidad de intercambio. Ejemplos de estos protocolos son PPTP y L2TP, ambos encapsulan el dato en un frame PPP a ser enviado a través de la Intranet.

Los protocolos de capa 3, corresponden a la capa de red, y usan paquetes como unidad de intercambio. El modo de túnel de seguridad de protocolo de Internet (IPSec) es un ejemplo de

protocolo de capa 3. Este encapsula el paquete IP en un header IP adicional antes de ser enviado.

8.4.6.4 Como trabajan los túneles

Para tecnologías de túnel de capa 2, un túnel se asemeja a una sesión, ambos extremos del túnel deben negociar para acordar las variables de configuración, como son los parámetros de asignación de direcciones, encriptación o compresión. En la mayoría de los casos, los datos transferidos a través del túnel son enviados usando un protocolo basado en datagramas.

Los protocolos de capa 3, generalmente asumen que todos los parámetros de configuración ya fueron seteados, generalmente por procesos manuales. Para estos protocolos no existe la fase de establecimiento del túnel. Sin embargo para los protocolos de capa 2, el túnel debe ser creado, mantenido y luego terminado.

Una vez que el túnel es establecido, los datos pueden ser enviados. El cliente y el servidor del túnel usan un **tunnel transfer protocol** para transferir datos. Antes de enviar, tanto el cliente como el servidor, agregan al dato un encabezado. El dato encapsulado viaja a través de la Intranet hasta el otro extremo del túnel, donde se le quita el header y es reenviado a su destino definitivo.

8.4.6.5 Ejemplos de protocolos de Túnel y requerimientos básicos

Como estos protocolos están basados en el protocolo PPP, heredan una serie de propiedades muy útiles. Estas propiedades cumplen además con los requerimientos básicos de VPN.

- Autenticación de usuarios.
- Asignación dinámica de direcciones.
- Compresión de datos.
- Encriptación de datos.
- Administración de claves de encriptación.
- Soporte de múltiples protocolos.

Veremos aquí algunos protocolos utilizados por las VPN:

8.4.6.5.1 Point to point protocol (PPP)

El PPP fue diseñado para enviar datos a través de conexiones de punto a punto de marcación o dedicadas. El PPP encapsula paquetes de IP, IPX, y NetBEUI dentro de las tramas del PPP, y después los transmite a través de un enlace de punto a punto. El PPP se utiliza entre un cliente de marcación y un NAS.

Hay cuatro fases de negociación en una sesión de marcación de PPP. Cada una de estas debe completarse satisfactoriamente antes de que la conexión de PPP esté lista para transferir los datos del usuario.

Estas fases son:

- Establecimiento del enlace de PPP
- Autenticación de usuarios

A) Protocolo de autenticación de contraseñas (PAP)

B) Protocolo de autenticación de intercambio de señales de reconocimiento (CHAP)

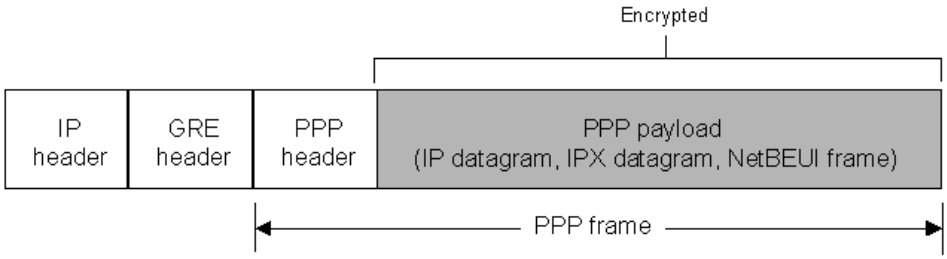
C) Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)

Control de retorno de llamada de PPP
Invocación de protocolos de nivel de red
Fase de transferencia de datos

8.4.6.5.2 Point-to-Point Tunneling Protocol (PPTP)

PPTP es un protocolo de capa 2 del modelo de referencia OSI, que encapsula los frames PPP en datagramas IP para ser transmitidos sobre una red interna de IP, como por ejemplo Internet.
PPTP puede ser usado para conexiones VPN de acceso remoto, o router-to-router. Esta documentado en el RFC 2637.

Este protocolo usa una conexión TCP para el mantenimiento del túnel, y una versión modificada de la encapsulación de enrutamiento genérico (Generic Routing Encapsulation, GRE) para encapsular los frames PPP. El dato del frame PPP puede estar encriptado y/o comprimido. La siguiente figura muestra la estructura de un paquete PPTP que contiene datos.



Paquete PPTP

8.4.6.5.3 Layer 2 Forwarding (L2F) (Transmisión de nivel 2)

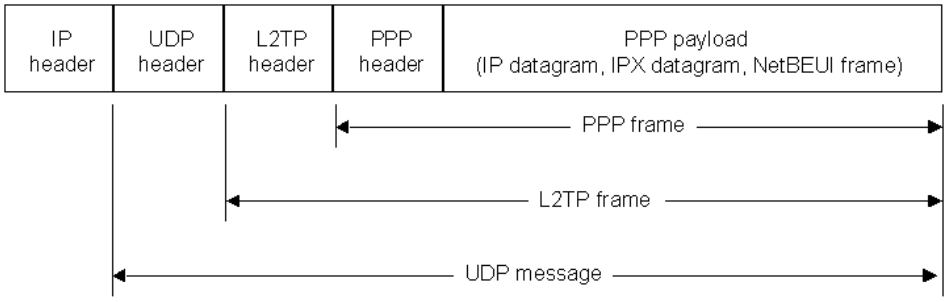
Es un protocolo de transmisión que permite a los servidores de acceso por discado estructurar el tráfico de discado en un PPP y transmitirlo a través de enlaces WAN a un servidor L2F. Después, el servidor L2F "abre" los paquetes y los transmite a través de la red. A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. Asimismo el L2F sólo funciona en túneles obligatorios.

8.4.6.5.4 Layer Two Tunneling Protocol (L2TP)

L2TP reúne las mejores características de PPTP y L2F (Layer 2 Forwarding, tecnología propuesta por Cisco Systems). L2TP encapsula los frames PPP a ser enviados sobre redes IP, X..25, Frame Relay o Asyncronous Transfer Mode (ATM).

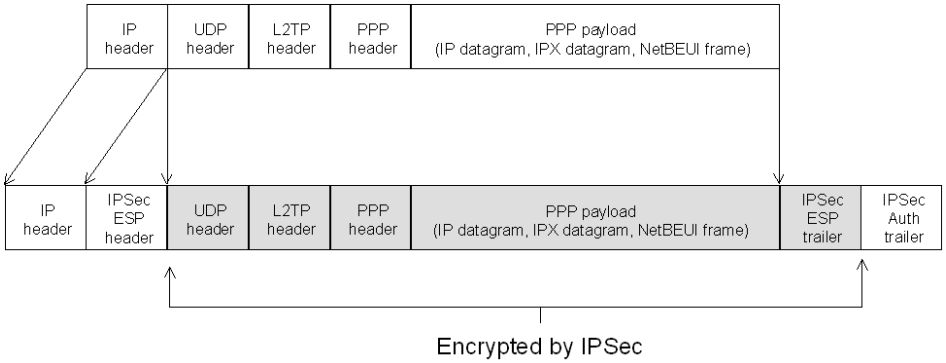
Cuando se configura para usar IP como su transporte de datagramas, puede ser usado como un protocolo de túnel a través de Internet. L2TP esta documentado en el RFC 2661. La siguiente figura muestra la estructura de un paquete PPTP que contiene datos.

El L2TP a través de redes internas de IP utiliza el UDP y una serie de mensajes L2TP para mantener el túnel. También usa UDP para enviar los frames PPP con los datos encapsulados en un header L2TP. El dato del frame PPP puede estar encriptado y/o comprimido.



Paquete L2TP

IPSec Encapsulating Security Payload (ESP) puede ser usado para encriptar el paquete L2TP. Esto es conocido como L2TP/IPSec. El resultado luego de aplicar ESP se puede ver en la siguiente figura:



Paquete L2TP/IPSec

8.4.6.5.5 Internet Protocol Security (IPSec) Tunnel Mode

IPSec es un protocolo estándar de capa 3 que soporta la transferencia segura de información sobre una Intranet IP. Asimismo define los mecanismos de codificación para el tráfico IP y el formato de un paquete para un IP a través del modo de túnel de IP, mejor conocido como modo de túnel de IPSec. Un túnel de IPSec consiste de un cliente de túnel y de un servidor de túnel, los cuales se configuran para utilizar la transmisión en túnel de IPSec y un mecanismo de encriptación negociado.

El modo de túnel de IPSec utiliza el método de seguridad negociada para encapsular y codificar todos los paquetes IP con el fin de lograr una transferencia segura a través de las redes internas IP públicas o privadas. Después, el dato encriptado es nuevamente encapsulado con un encabezado IP de texto plano, y se envía a través de la Intranet para que lo reciba el servidor de túnel. Una vez recibido el datagrama, el servidor de túnel procesa y descarta este encabezado IP de texto plano, y luego desencripta su contenido. Posteriormente, el paquete IP es procesado normalmente y direccionado a su destino original.

8.4.6.6 PPTP comparado con L2TP/IPSec

Tanto PPTP como L2TP/IPSec usan PPP para proveer a los datos de una estructura inicial, y luego agregan headers adicionales para transportarlo a través de la Intranet. Algunas de las diferencias existentes entre ambos protocolos son:

- Con PPTP, la encriptación de datos comienza luego de que el proceso de conexión PPP, y por lo tanto la autenticación PPP, ha sido completada. Con L2TP/IPSec, la encriptación de los datos comienza antes de que la conexión PPP comience, negociando un IPSec security association.
- PPTP usa MPPE, un encriptador de flujo (stream cipher) que esta basado en el algoritmo de encriptación RC-4, y usa claves de encriptación de 40, 56, o 128 bits. Este tipo de encriptadores tratan los datos como un flujo de bits. L2TP/Ipsec usa el estándar DES (Data Encryption Standard), el cual es un encriptador de bloque.
- PPTP requiere solo autenticación a nivel de usuario, basada en el protocolo de autenticación de PPP. L2TP/IPSec requiere también de este nivel de autenticación, y además, autenticación a nivel de computador, usando computer certificates.

8.4.6.7 Ventajas de L2TP/Ipsec sobre PPTP

- IPSec provee por cada paquete de: autenticación de datos (prueba que los datos han sido enviados por un usuario autorizado), integridad de los datos, protección contra reenvios y confidencialidad de los datos. Mientras que PPTP solo provee de autenticación de datos.
- Las conexiones L2TP/IPSec proveen de un alto grado de autenticación, tanto a nivel de computador, como a nivel de usuario.

- Los paquetes PPP intercambiados nunca podrían llegar a ser enviados sin encriptar.

8.4.6.8 Ventajas de PPTP sobre L2TP/IPSec

- PPTP no requiere el uso de certificados, lo cual puede llega a ser necesario en algunos casos
- PPTP puede ser usado sobre Windows XP, 2000, NT versión 4.0, Millennium Edition, 98 y 95. Mientras que L2TP/Ipsec solo puede ser usado con Windows XP y 2000.
- Clientes PPTP y servidores pueden ser ubicados detrás de un NAT (Network address translator), mientras que para L2TP/IPSec no.

8.4.7 Implantación de VPNs

8.4.7.1 Aspectos relevantes en la implantación

Al implantar una VPN [3] se debe tener en cuenta:

- Número de usuarios en cada centro
- Consumo de ancho de banda
- Número de delegaciones a interconectar
- Tipo de comunicación a establecer
    - Remoto Central
    - Todos con todos
- Tipos de accesos que se emplearán en la conexión
    - ADSL
    - Cable
    - RDSI
    - MODEM
- Número de teletrabajadores

8.4.7.2 Herramientas para Implantar una VPN [4]

- **VPN gateway**

Dispositivos con un software y hardware especial para proveer capacidad a la VPN.
Varias funciones son optimizadas sobre varios componentes de software y hardware.

- **Solo Software**

El software está sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN. Algunos ejemplos de estos son el Sistema Operativo Windows 9x, ME, NT, 2000 y XP.

- **Basado en Firewall**

Funciones adicionales son agregadas al firewall para habilitar capacidades de VPN. Algunos ejemplos de esto son los modelos PIX de Cisco como 506, 515, 525 y 535.

¿Qué diferencia hay entre una VPN y un cortafuego?
Un cortafuego se utiliza para "filtrar" tráfico no autorizado. VPN se utiliza para dejar entrar tráfico autorizado. En algunos casos un cortafuegos puede tener capacidades de una VPN y viceversa.

- **Basado en Router**

Funciones adicionales son agregadas al router para habilitar capacidades de VPN, las cuales se encuentran en el IOS de los routers de Cisco como los modelos 804, 806, 827, 905, 1710, 1720, 1750, 2611, 2621, 2651, 3620, 3640, 3660, 7120, 7140 y 7200.
Aunque los router son mejores que los concentradores, existen algunos capaces de realizar VPN como los modelos 3005, 3015, 3030, 3060 y 3080.

8.4.8 ¿Cuáles son las ventajas de las VPN o túneles?

Enumeraremos ahora algunas de las ventajas de contar con una VPN:

1. Permiten unir oficinas remotas a través de Internet así como también permiten el acceso de los teletrabajadores o usuarios móviles ocasionales de una empresa a través de un proveedor de Internet local, en lugar de tener montada una infraestructura de modems y servidores de acceso remoto.

2. Conectividad universal, la ubicación de las oficinas remotas es indiferente, pueden estar a ambos lados de una calle, en la misma ciudad o en cualquier lugar del mundo.

3. Seguridad: Se utiliza encriptación de alto nivel y por lo tanto se puede mantener la integridad, confidencialidad y seguridad de los datos. Con las VPN se puede lograr un nivel de seguridad mucho mayor que con los medios de acceso remoto tradicionales.

   ¿Cómo pueden asegurarme que mis datos son privados al enviarles por Internet?
   Todo el tráfico VPN está encriptado con una clave secreta. Esté clave está negociada dinámicamente utilizando la tecnología VPN.

4. Reducción de costos, permiten ahorrar grandes sumas de dinero en líneas dedicadas.

Al tener menos equipos, menos llamadas, menos conexiones tipo Frame Relay se reduce los gastos a la empresa. Al tener una sola red para gestionar también se reducen los gastos de gestión.

5. Escalabilidad: soportan múltiples túneles simultáneos.

6. Flexibilidad: Las oficinas remotas pueden configurarse rápidamente (tiempos de implantación reducidos y es sencilla de usar).

7. Uniones remotas de carácter temporal pueden establecerse con facilidad.

8. Control de acceso basado en políticas de la organización.

9. Herramientas de diagnóstico remoto.

10. Los algoritmos de compresión optimizan el tráfico del cliente.

11. Las VPNs pueden utilizarse para obtener conectividad con proveedores y partners, permitiendo el uso de nuevas aplicaciones de negocio en red.

8.4.9 Desventajas de las VPN

- **¿El proceso de encriptación afecta el rendimiento de mi red?**

Depende en el tipo de encriptación. Si la encriptación se realizado sólo con Software puede afectar la velocidad del procesamiento de paquetes, así reduciendo el rendimiento de la red. Si la encriptación se realiza en equipos especiales, hay menos problemas de rendimiento.

- **Costos de Implementación**

Si se quiere implementar una VPN [6] patentada se puede requerir importantes sumas de dinero en hardware y software. Existe una alternativa a esto, muy buena especialmente para empresas pequeñas, y es que los ISP ofrezcan los servicios de VPN.
Esto produce como consecuencias:

- Ahorro en continua inversión tecnológica. Es un tercero quien gasta en el equipamiento de la infraestructura, mientras que el usuario solo paga una renta mensual por el servicio que incluye adicionalmente la administración, monitoreo y operación de la conectividad.
- Ahorro del consumo mensual en conectividad, sobre todo si anteriormente se contaba con enlaces internacionales y nacionales.
- Ahorro en capacitación. Ya que es el proveedor quien mantiene y opera la infraestructura, lo cual evita una continua capacitación que el cliente tendría que hacer con su staff de sistemas, para operar y monitorear la VPN.

- **Interoperabilidad de diferentes equipos**

Se intenta lograr en el futuro la interoperabilidad de las diferentes soluciones de VPNs existentes.

8.4.10 Referencias

[1] Servicios de Informática y Telecomunicaciones
servinformatica.html

[2] Trabajo enviado por Roberto Nader Carreño (introducción_vpns.pdf)
Bibliografía en Internet:
http://www.entarasys.com/la
http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml

[3] Divisa iT. Informática y Telecomunicaciones
http://www.divisait.com

[4] http://www.geocities.com/erichernandezp/

[5] http://www.cites.uiuc.edu/vpn/
22 de Noviembre, 2002

[6]
http://www.microsoft.com/latam/windowsxp/descargas/windowsxp/pro/biblioteca/planning/wiresslan/WirelessLANTechnologiesandWindowsXP.doc

[7] Seguridad de las redes inalámbricas: Wardriving y Warchalking
http://www.seguridadenlared.org/es/wireles.php

[8] http://www.wi-fi.org/OpenSection/secure.asp?TID=2

[9] http://www.wi-fi.org/OpenSection/secure.asp?TID=2

[10] http://www.eveliux.com/articulos/wlans.html

[11] www.avaya.com

[12] www.ait.ac.th junio de 2002

[13] www.vnunet.es

[14] http://www.reduh.uh.cu

[15] www.vunet.es (7/2/03)

Seguridad En Una Red Inalámbrica http://redlibre.sin-ip.com.ar/article.php?sid=9

8.5 Modelado Teórico

Como se ha relatado al comienzo del proyecto cuando se comenzó a trabajar en el mismo frente a la realidad de comunicaciones existente se considero adecuado realizar investigaciones sobre la forma de trabajar con una Wan desconexa.

Si bien al cambiar las circunstancias del proyecto dichas investigaciones quedaron detenidas se agrega aquí uno de los documentos producidos dado que será de interés a la hora de retomar la investigación en estos temas hecho que se puede producir como mecanismo de contingencia o por un cambio en la realidad de la infraestructura de comunicaciones

8.5.1 Introducción

El presente documento expondrá un modelo teórico destinado a servir de herramienta para el trabajo en el proyecto planteado.

8.5.1.1 Objetivo

Contar con un modelo adecuado para representar la infraestructura de comunicaciones en el CES.

8.5.2 Modelo

8.5.2.1 Descripción

Como es típico a nivel de topología de redes se utilizará un grafo para modelar las comunicaciones.

En dicho grafo los nodos representaran distintos puntos a conectar (Liceos, oficinas, etc) y las aristas las líneas de comunicación existentes.

Sin embargo el presente modelo se apartara del modelo normalmente aceptado en dos puntos, primero en la definición de conexión y en considerar el grafo como dirigido ya que en algunos casos las aristas pueden tener distintos pesos de acuerdo si el sentido es del nodo A al B o del B al A.

8.5.2.2 Definición del modelo

8.5.2.2.1 Definición de nodo

Un nodo representa un punto a conectar.

Comprende a una o más computadoras interconectadas por enlaces confiables de alta velocidad.

8.5.2.2.2 Definición de arista

Una arista del nodo A al nodo B, representa un enlace unidireccional de A a B.

8.5.2.2.3 Definición de capacidad de una arista

La capacidad de una arista queda determinada por la cantidad de información que es capas de transmitir.

Es decir cada arista tiene asociado un valor que representa la cantidad de información que puede transmitir, expresada en unidades de información sobre tiempo (kbps, mps, etc.).

8.5.2.2.4 Definición de continuidad de una arista

La continuidad de una arista, la entendemos como el concepto intuitivo de confiabilidad.

Decimos cada arista tiene asociado un valor de continuidad tal que:

- **si provee un enlace sin interrupciones y con tasa de errores tendiendo a nula el valor de continuidad es "CA" (continuo, alto)**

- **si provee un enlace sin interrupciones pero con una tasa de errores aceptable el valor de continuidad es "CM" (continuo, medio)**
- **si provee un enlace sin interrupciones pero con una tasa de errores elevada el valor de continuidad es "CM" (continuo, bajo)**
- **si provee un enlace con interrupciones y con tasa de errores tendiendo a nula el valor de continuidad es "DA" (discontinuo, alto)**
- **si provee un enlace con interrupciones pero con una tasa de errores aceptable el valor de continuidad es "DM" (discontinuo, medio)**
- **si provee un enlace sin interrupciones pero con una tasa de errores elevada el valor de continuidad es "DM" (discontinuo, bajo)**

Es decir si tenemos un enlace Lan por ejemplo tendremos un valor de continuidad "CA", si tenemos un enlace por MODEM sobre una línea de alta calidad tendremos en general un valor de continuidad "DA".

La utilidad de esta función radica en que captura un factor esencial de las comunicaciones que es la disponibilidad de la conexión en el tiempo y la confiabilidad de la misma, por ejemplo a veces es mas conveniente contar con un enlace "CA" (línea dedicada de 64kbps por ejemplo) que por ejemplo un enlace "DM" (enlace ISDN a 144kbps), dado que el hecho de poder transmitir las 24horas sin costo adicional compensa con creces la diferencia de capacidad, ventaja que se puede ver incrementada dependiendo de la granularidad de los datos a transmitir, dado que un error puede provocar que se retransmita una sola transacción o un conjunto importante de datos.

8.5.2.2.5 Definición de función de capacidad

A los efectos de simplificar el tratamiento teórico definiremos una función φ_C (función de capacidad) que dado un enlace nos clasificara el mismo de acuerdo a su capacidad.

Sea CC = {c/c es un valor de capacidad}

Se define $\varphi_{C\,(c)}$ tal que a cada valor de capacidad le asocia un natural "n" en el rango 1..5 / n=

1. **si c esta en el orden de los 100Mbps o superior**
2. **si c esta en el orden de los 10Mbps o superior**
3. **si c esta en el orden de 1Mbps o superior**
4. **si c esta en el orden de 512kbps o superior**
5. **si c esta en el orden de 64kbps o superior**
6. **si c esta en el orden de los 28.800bps o superior**
7. **si c esta en el orden de los 2400bps o superior**

Observación:

La propia definición de φ_C establece una relación de ordenes, es decir un enlace de primer orden incluye en si mismo las propiedades de un enlace de cuarto orden y las supera, es decir si establecemos como requisito para determinado objetivo valores de φ_C de tercer

orden implícitamente decimos que si tenemos una conexión de segundo orden obviamente satisfacera el requisito con creces.

8.5.2.2.6 Definición de conectividad de una arista

Entendemos como conectividad de una arista una función Φ que dada una arista AB nos devuelve un par de tuplas (X=(x,y),Y=(x',y')) tal que:

x es φ_C (AB)
y es la continuidad de AB
x' es φ_C (BA)
y' es la continuidad de BA

Por ejemplo dado un enlace punto a punto de fibra óptica de 100mbps entre los nodos A y B, tendremos $\Phi(AB)=((1,CA),(1,CA))$.

En un enlace ADSL de 512 kbps entre A y B y 64 kbps entre B y A tendremos $\Phi(AB)=((4,CA),(5,CA))$.

8.5.2.2.7 Definición de enlace simétrico

Decimos que un enlace AB es simétrico si solo si $\Phi(AB)=\Phi(BA)$

Notación
Si AB es simétrico, entonces notaremos $\Phi(AB)=(x,y)$

8.6 Solicitud original del Proyecto

A modo de referencia se introduce a continuación la propuesta original del presente proyecto de grado.

8.6.1 Identificación del Proyecto

Nombre del Proyecto: **Control y seguimiento de gastos en Centros Educativos**
Año: 2003
Institución en donde se realizara el proyecto: Centro de Cómputos del Consejo de Educación Secundaria, ANEP
Nombre del Responsable del Proyecto por la Institución: Ing. Álvaro Motta
Tel: 9169845 Fax: 9163871 Email: amotta@ces.edu.uy

Estudiantes:

Nombre y Apellido	**Doc. Identidad**	**Teléfono**	**Email**
Carlos García	2.996.431-4	9156136	cgarcia@ces.edu.uy
		0991797 47	

8.6.2 Resumen del Proyecto

El Consejo de Educación Secundaria es una institución de gran entidad que llega a todos los puntos del país con mas de 260 centros educativos, con una plantilla de mas de 5000 funcionarios y más de 15000 docentes.

Como toda gran organización presenta desafíos desde el punto de vista administrativos a la hora de optimizar el uso de recursos, siendo estos más grandes al no ser Secundaria una institución comercial por lo que su expansión no esta dictada por conveniencias logísticas o estratégicas teniendo centros educativos en localidades apartadas con distintas dificultades locativas e incluso con problemas para obtener comunicaciones telefónicas de calidad.

En el marco de la optimización del uso del presupuesto es beneficioso para la administración él poder realizar un seguimiento de los gastos de cada uno de los centros educativos.

La meta de este proyecto es realizar el estudio de factibilidad e implementación del referido sistema.

El Estudiante deberá investigar las distintas posibilidades a la hora de seleccionar la plataforma del sistema, teniendo en cuenta la heterogeneidad de las conexiones disponibles entre cada uno de los centros y Consejo (Adsl, punto a punto, líneas discadas, etc.), siendo esta una Wan de alcance Nacional.

En una segunda instancia deberá implementar la estrategia seleccionada.

La solución encontrada deberá ajustarse a la realidad económica del Ente, donde los recursos disponibles son limitados, por lo que tratara de utilizar al máximo la plataforma disponible así como mantener los costos operativos al mínimo.

8.6.3 Descripción del Proyecto

8.6.3.1 Objetivos

Estudio de factibilidad e implementación de un sistema de seguimiento de gastos de Centros Educativos a nivel Nacional, incluyendo:
- Comparación y selección entre las distintas interfases (Win, Web)
- Adecuación de la solución a la infraestructura de las comunicaciones existentes
- Selección del modelo de base de datos más adecuado a la realidad presentada (BD distribuida, replicación, etc.)
- Plan de deployment y mantenimiento de futuro de la aplicación a nivel nacional (por ejemplo instalación remota de parches, etc.), teniendo como objetivo la minimización de los costos de mantenimientos y de TCO.

8.6.3.2 Resultados Esperados

-Estudio de factibilidad y propuesta de la solución
- Implementación de la solución (en este punto se busca especialmente resolver la implementación en el ámbito de bases de datos, interfase y plan de deployment de la aplicación, quedando a cargo del centro de cómputos la instalación a nivel nacional del sistema así como su ampliación agregándole mas funcionalidades administrativas).
- Documentación de todo el proceso.
- Documentación del sistema.

8.6.3.3 Contexto de Trabajo

Se enmarca dentro de un Centro de Cómputos de una gran organización, pero con grandes limitaciones presupuéstales, aun así, este Centro de Cómputos ha sido galardonado el año pasado con el segundo puesto en el JIAP.

Se caracteriza por enfrentar grandes desafíos desde el punto de vista tecnológico (aplicaciones distribuidas a nivel nacional) en un marco donde a diferencia de lo que ocurre en grandes instituciones, no se cuenta con grandes presupuestos para enfrentar los desafíos, es en este marco donde el ingeniero tiene que esforzarse a la hora de obtener una solución aplicable al organismo.

8.6.3.4 Plan de Trabajo

8.6.3.5 Cronograma

- Relevamiento de los requerimientos del sistema de gastos – mes 1
- Relevamiento de las características de la infraestructura disponible – mes 1
- Plan de factibilidad – meses 1 al 2

- Prototipado y pruebas sobre el prototipo– meses 2 y 3
- Implementación - meses 4 al 7
- Instalación en Centros pilotos - mes 8
- Documentación – meses 1 al 8

8.6.3.6 Metodología de Trabajo

Se utilizara una metodología evolutiva.

8.6.3.7 Formación ofrecida al estudiante

Conocimiento y experiencia de desarrollo sobre Wan, particularmente cuando los recursos disponibles y la calidad y ancho de banda de las comunicaciones no son las mejores.
Confrontación con los costos reales de un sistema, como por ejemplo los asociados al deployment y mantenimiento.

8.6.3.8 Bibliografía específica

8.6.4 Recursos Informáticos

8.6.4.1 Hardware

Amplia gama de equipamiento informatico desde workstatión a servidores.
Infraestructura de telecomunicaciones (lineas directas, discadas, 0800, adsl, etc.)

8.6.4.2 Sistema Operativo

Windows NT, Windows 2000

8.6.4.3 Lenguajes

Genexus, o Visual Basic.

8.6.4.4 Herramientas

Internet Information Server, MSSQL.

8.6.4.5 Otros

8.6.5 Conocimientos previos del estudiante

8.6.5.1 Exigidos

Experiencia en proyectos de mediano porte

8.6.5.2 Recomendados

Conocimientos de redes.

8.7 Ampliación de proyecto

A continuación se introducirá el documento que amplio los objetivos del proyecto al comienzo del mismo, se considera pertinente su inclusión por dos motivos a saber, el primero porque da una idea de la evolución del proyecto y como este se vio afectado por los cambios en la infraestructura de comunicaciones y el segundo porque los objetivos planteados en el mismo pueden ser retomados a la hora de retomar el estudio de las soluciones para una Wan desconexa tal y como planteamos en el capitulo de contingencias.

8.7.1 Introducción

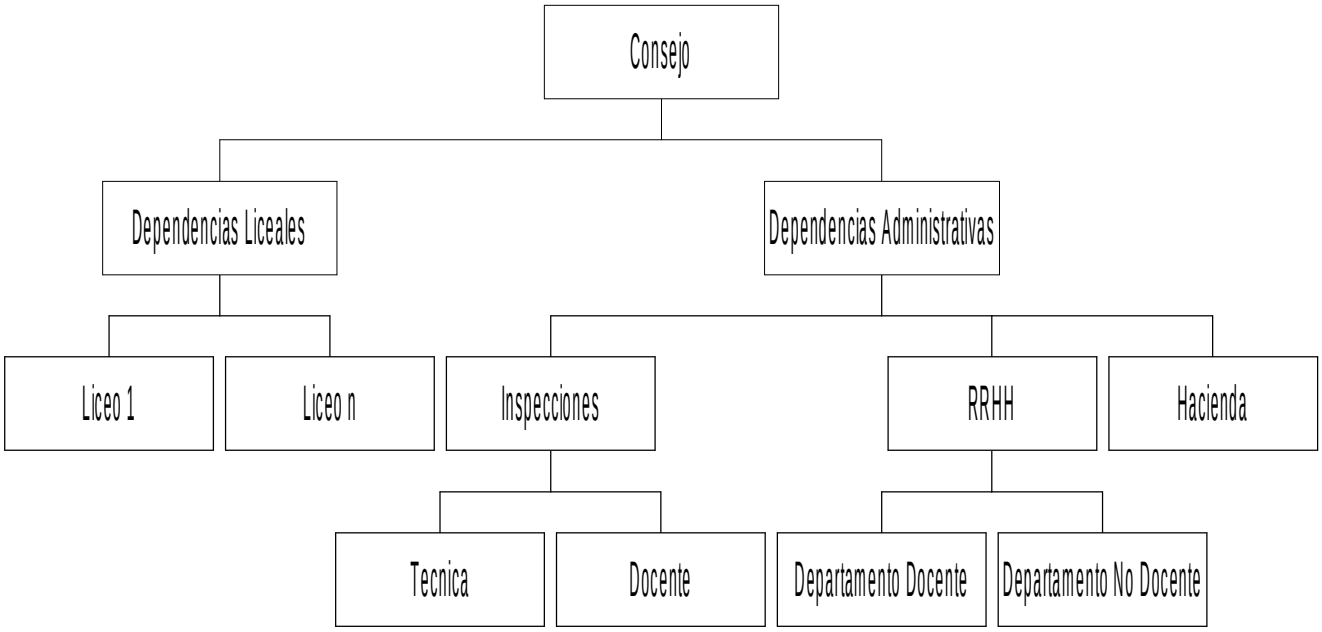
El presente documento expone, amplía y concreta los requerimientos incluidos en el documento "Control y seguimiento de gastos en centros educativos", tratado y aprobado por el Consejo de Educación Secundaria en la Sesión Nº 26 de fecha 4 de junio del año 2003.

El objetivo de dicho proyecto es el de obtener una infraestructura que permita la instalación el monitoreo y uso de aplicaciones distribuidas en todas las dependencias del Ente, incluidas las Liceales.

Finalmente se espera implementar una aplicación concreta (Seguimiento de gastos) a los efectos de probar la adaptabilidad y funcionamiento en la práctica de la estructura finalmente recomendada.

8.7.1.1 Estructura organizacional del Consejo

El consejo de Educación Secundaria tiene una estructura arborescente con dos ramas principales, institutos Liceales y Dependencias Administrativas.



A su vez, el "árbol" del CES es una rama del árbol mas grande conformado por la ANEP en su totalidad, donde encontramos Inspecciones regionales, RRHH de la ANEP, etc, que también tienen necesidades compartidas con distintas hojas del CES.

En definitiva tenemos un gran árbol distribuido en todo el país, la mejor forma de implementar diversas soluciones informáticas sobre todo este árbol, es el objeto principal de este proyecto.

8.7.1.1.1 Comunicaciones e infraestructura existente

De hecho hoy no hay una solución integral de comunicaciones en el ámbito del CES. Existe una red LAN sobre TCP/IP con servidores NT, que cubre las oficinas centrales y a través de líneas dedicadas o fibra óptica varias dependencias centrales del Consejo.

A su vez, esta red esta conectada por intermedio de una línea de 2 MB/s al Centro de Cómputos de CoDiCen, donde se obtiene la conexión a Internet (Línea de 512 kb/s) y la interconexión con las restantes ramas de la ANEP.

Los liceos aun tiene líneas discadas, las cuales en principio utilizarían el 0800-ANEP para interconectarse a la LAN del CES.

Hoy en día el resto del árbol "ANEP", coexiste sobre las mismas líneas de comunicación física (es decir todos compartimos la salida a Internet ☺) pero no existe interconexión lógica, dificultando la implementación de soluciones globales.

8.7.1.1.2 Objetivo

Obtener una forma estandarizada de instalar aplicaciones (distribuidas o no) en uno o varios nodos, permitiendo que las mismas sean mantenidas (en la medida de lo posible y teniendo en cuenta la naturaleza de la propia aplicacion) y monitoreadas en forma remota desde un nodo particular (p.e el nodo CES).

Se debe cuidar de proveer además una metodología para que permita la comunicación de datos entre nodos de distintos niveles (p.e de nodos descendientes a ancestros o entre nodos hermanos, etc) teniendo en cuenta aspectos tales como la centralización de datos en un nodo particular (base de datos central) o bien la distribución de datos en los distintos nodos de forma que sea visible a otros nodos (base de datos distribuida), lo cual implica utilizar técnicas de sincronización, replicación u otras.

En definitiva se propone realizar un estudio que brinde un marco general que permita el desarrollo de aplicaciones, su instalación, mantenimiento y monitoreo y como se realiza el flujo de datos entre las mismas, considerando distintas formas de almacenamientos de datos (bases de datos centralizada, distribuida, etc), lo cual implica el estudio y coordinacion de aspectos relativos a las comunicaciones (autenticacion, certificacion, etc...), plataformas a utilizar, tipo de aplicaciones a desarrollar, formas de comunicacion, hardware a utilizar, configuraciones, etc..

Tendiendo a dar una solucion global que cubra distintos aspectos y que constituya un marco general que pueda ser adaptado a distintas aplicaciones a desarrollarse en el futuro.

Obtener una forma de instalar, monitorear y usar apliaciones distribuidas entre los nodos y hojas del árbol, proveyendo métodos para asegurar el viaje de datos entre nodos de distintos niveles, con centralización de datos o sin ella de acuerdo al caso concreto.

Probar los mecanismos propuestos con el sistema de control de gastos liceales.

Abstrayendo el objetivo, diríamos que dado una estructura pasible de ser representada por un grafo conexo buscamos un modelo escalable que resuelva los problemas de seguridad, flujo de datos y soporte presentados.

Entendemos por:

- *Problemas de seguridad, aquellos que quedan determinados por los presentados para garantizar la confidencialidad, autenticidad y disponibilidad de los datos.*
- *Flujo de datos, aquí esperamos que el modelo permita la comunicación de un nodo cualquiera a múltiples nodos receptores, de un nodo cualquiera a un único nodo receptor y viceversa, de uno o múltiples nodos emisores a un único nodo receptor.*
- *Por soporte entendemos la instalación, monitoreo y mantenimiento de la infraestructura informática de forma remota.*

Entendemos por escalable, que el modelo propuesto sea capaz de evolucionar y crecer para soportar los cambios en las necesidades expuestas en las consideraciones anteriores, así como también la evolución tecnológica en materia de comunicaciones.

8.7.1.1.3 Motivación

Hay dos grandes motivaciones:

- Cada vez mas la vida de una organización recae en la información, y hoy en día la única alternativa practica es contar con sistemas de información que alcancen a la totalidad de la organización. Pero estos sistemas, ya sean workflow, aplicaciones clásicas, mail, etc, requieren de una infraestructura para funcionar, estudiar las alternativas existentes para brindar la mejor infraestructura para el caso propuesto es el objeto de este proyecto.

- En esta misma organización hubo grandes proyectos informáticos que han fracasado, o no han alcanzado completamente sus objetivos por no disponer de estructuras eficientes que permitieran la recolección de datos.

8.7.2 Alternativas

Se deben investigar, analizar y finalmente recomendar el uso de las tecnologías detalladas a continuación, así como su forma de uso y estandarización.

8.7.2.1 Alternativas en comunicaciones

- 0800
- Wan (ADSL, ISDN, Frame Relay, etc)
- Internet
  - Mail
  - FTP

8.7.2.2 Tecnologías de seguridad a implementar

- Autentificación
- Certificación
- Firewall
- Sistemas de detección de intrusos
- Antivirus
- Proxy
- Filtrado de paquetes
- Zonas desmilitarizadas
- Grupos de usuarios

8.7.2.3 Estándares de configuración a utilizar

- Configuración de TCP/IP a nivel de direcciones IP y Ruteo
  - DHCP
  - Ip's Fijas
  - Subredes
- Configuración de DNS
- Estándares de Seguridad

8.7.2.4 Plataforma a utilizar

Determinación de

- Sistema Operativo
- Entorno de desarrollo recomendado
- Base de datos
- Herramientas de seguridad

8.7.2.5 Aplicaciones

- Aplicaciones Web
  - ASP
  - Web Services

- Aplicaciones "Windows Clásicas"
  - Instalación remota
  - Monitoreo
  - Sincronización de datos

- Mecanismos de actualización remota

- Bases de datos centralizada

8.7.2.6 Topología

Estructura de alcance regional con nodos departamentales o regionales.

8.7.2.7 Plan de Contingencia

¿Qué pasa si se cae la ADSL que une Salto con Montevideo?

¿Qué soluciones alternativas brindamos o sugerimos?

8.7.2.8 Varios

Interconexión entre distintas plataformas o tecnologías.

8.7.2.9 En resumen

Buscamos una solución muy escalable que se adapte a los requerimientos de la organización presentes y futuros, y que sea fácilmente adaptable a la hora de implementar nuevas aplicaciones que alcancen a todos los puntos de la organización (o a un subgrupo de la misma), sin necesidad de tener que "reinventar la rueda" para cada proyecto informático.

Obviamente la solución buscada, tocara todos los aspectos enumerados anteriormente, comparándolos y determinando las recomendaciones y soluciones que mas se adapten a la realidad organizacional.

8.7.3 Prototipado

Finalmente mediante la creación de la aplicación de control de gastos en liceos, buscaremos probar en la practica la solución propuesta, si bien desde el punto de vista conceptual es una aplicación simple la misma cuenta con :

- Alcance nacional, más de 270 centros liceales.
- Variedad en la infraestructura de comunicaciones.
- Los datos deben viajar de las hojas al nodo principal y ocasionalmente viceversa.
- Se debe proveer un adecuado plan de contingencia, por ejemplo si nos orientamos a una solución Web, debemos proveer una solución alternativa a la conexión principal del liceo.
- Instalación y monitoreo remoto

8.7.4 Cronograma

12-6-2003

Obtención de apoyo oficial a nivel de Alta Gerencia y mandos medios.

Relevamiento primario

(ETAPA CUMPLIDA)

17-7-2003

Reperfilamiento del proyecto

Obtención de consenso en la organización.

25-7-2003

Investigación y documentación de tecnologías disponibles

Relevamiento de la infraestructura existente

9-2003

Análisis del primer prototipo de la arquitectura propuesta (a nivel de conectividad)

Análisis de impacto

La actual infraestructura de la ANEP, ¿permite la solución en materia de ruteo?, ¿Plataforma de servidores?, ¿ancho de banda disponible?

10-2003

Sucesivos refinamientos de la solución básica

Análisis y documentación de soluciones en materia de seguridad

A la red propuesta tendrán acceso 15.000 funcionarios y unos 200.000 alumnos (pequeños hackers en potencia☺), ¿qué haremos para protegernos?. Y si la solución pasa por Internet, ¿cómo sabremos que alguien es quien dice ser?

11-2003

Análisis de infraestructura a nivel de:

Web
Base de datos
Entorno de desarrollo

Aquí debemos responder a la pregunta, ¿cómo trabajaremos sobre esa infraestructura?, ¿Utilizaremos servidores Web?, ¿Bases de datos? ¿cómo replicaremos o sincronizaremos nuestros datos?, ¿Web services?, ¿aplicaciones Win?

12-2003

Monitoreo e instalación remoto

¿Cómo lograremos mantener todo esto andando sin necesidad de recorrer todo el país cada vez que hay que actualizar la aplicación?

¿Cómo sabremos si la aplicación funciona en cada uno de los puntos en los que esta instalada?

¿Cómo instalaremos cada nuevo sistema?

1,2-2004

Implementación de la Aplicación Prototipo

3-2004

Finalización del proyecto

9 Bibliografía

[1] Redes de computadoras, Andrew S. Tanenbaum, Prentice Hall, ISBN 968-880-958-6

[2]http://www.windowstimag.com/atrasados/2000/44_julago00/articulos/comparativa.htm ,articulo de comparación de herramientas de control remoto, accedido 10/1/2004

[3]Virtual Network Computing, IEEE Internet Computing Volume 2, Number 1 January/February 1998

[4] http://www.uk.research.att.com/archive/vnc/sshvnc.html, accedido 10/2/2004

[5] Fundamentals of database systems, Elmasri, R y Navathe. Addison-Wesley, ISBN 0-8053-1753-8

[6] http://www.monografias.com/trabajos15/datos/Bddistribuidas.shtml, 1/2/2004

[7] Microsoft Corporation, Libros en pantalla de SQL Server 7.0.

[8] Análisis y perspectivas del nuevo sistema de sueldos, García, Nieves y Nossar, Consejo de Educación Secundaria, documento interno ANEP 2002

[9]Internetworking Lans, Robert Davison Nathan Muller, Artech House, ISBN 0-89006-598-5

[10]Intranets, Gordon Benett, Prentice Hall, ISBN 84-89660-65-4

[11]Redes de Computadores, protocolos Normas e Interfaces, Uyless Black, Ra-Ma, ISBN 970-15-0329-5

[12]Distributed Networks, Uyless Black, Prentice Hall, ISBN 0-8359-1209-4-025

[13]Local and Metropolitan Area Network, William Stallings, Prentice Hall ISBN 0-13-190737-9

[14] http://www.monografias.com/trabajos13/gpts/gpts.shtml, 4/2/2004

[15] http://aptrix2.ancel.com.uy/ancel/ancel_site.nsf/Content/gsm, 10/3/2004

[16] http://www.casadomo.com/revista_domotica_metodos.asp?TextType=3304, 20/2/2004

[17] http://www.casadomo.com/revista_domotica_metodos.asp?TextType=3313, 20/2/2004