UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"**Implementación de los requerimientos de Software para el Sistema de Registro al Concurso de Ingreso a la Educación Media Superior (COMIPEMS)"**

I N F O R M E D E A C T I V I D A D E S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

POR LA OPCIÓN TITULACIÓN POR TRABAJO PROFESIONAL

P R E S E N T A:

ARMANDO MARTÍNEZ ESTRADA

AVAL:

ING. ALBERTO GONZÁLEZ GUIZAR

Ciudad universitaria México, D.F. 2007

ÍNDICE

INFORME DE ACTIVIDADES

1 Nombre

Implementación de los requerimientos de Software para el Sistema de Registro al Concurso de Ingreso a la Educación Media Superior (COMIPEMS).

2 Objetivo

Implementar mejoras técnicas en las herramientas de software utilizadas en la actual infraestructura de red de los distintos centros de Registro del Concurso de Ingreso a la Educación Media Superior (COMIPEMS), con el fin de asegurar y custodiar el adecuado funcionamiento de los enlaces de comunicación entre el servidor de cada centro de registro y el servidor Central ubicado en el centro de computo de la Secretaria de Educación Publica (SEP), y de esta manera dar soporte a los procesos electrónicos de pre-Registro presencial, pre-registro en línea y registro del Concurso de Ingreso a la Educación Media Superior.

3 Antecedentes

3.1 Concurso de Ingreso a la Educación Media Superior

En Febrero de 1996 las autoridades educativas del gobierno federal y el Estado de México, junto con las instituciones públicas que ofrecen educación media superior acordaron realizar conjuntamente un concurso que permitiera la selección de aspirantes para sus planteles de la zona metropolitana, que se definió como el Distrito Federal y 22 municipios del Estado de México.

A partir de esto, se crea la Comisión Metropolitana de Instituciones Publicas de educación Media Superior (COMIPEMS), compuesta por nueve instituciones educativas que ofrecen programas de educación media superior pública en el Distrito Federal y en el Estado de México: Colegio de Bachilleres (COLBACH), Colegio Nacional de Educación Profesional Técnica (CONALEP), Dirección General del Bachillerato (DGB), Dirección General de Educación Tecnológica Agropecuaria (DGETA), Dirección General de Educación Tecnológica Industrial (DGETI), Instituto Politécnico Nacional (IPN), Secretaría de Educación del Gobierno del Estado de México (SE), Universidad Autónoma del Estado de México (UAEM), Universidad Nacional Autónoma de México (UNAM), que realiza un concurso anual permitiendo atender conjunta y de forma transparente a los aspirantes a la Educación Media Superior de la zona metropolitana.

La demanda para lugares en las instituciones de Educación Media Superior viene creciendo año con año, como se demuestra en la siguiente tabla.

EDICIÓN DEL CONCURSO	ASPIRANTES REGISTRADOS
1996	262,314
1997	238,956
1998	244,068
1999	247,691
2000	237,656
2001	245,823
2002	261,702
2003	276,490
2004	280,655
2005	287,886

Tabla 1. Cantidad de Aspirantes por año

Este crecimiento hace necesario automatizar los procesos de atención a los aspirantes (Pre-Registro en línea y presencial, Registro) y Publicación de Resultados del examen de Ingreso.

3.2 Concurso de Ingreso a la Educación Media Superior

Existen tres procesos durante la etapa de registro para el Concurso de Ingreso a la Educación Media Superior dirigidos a diferentes tipos de aspirantes como se describen a continuación:

3.2.1 Clasificación de los Aspirantes

a) *Aspirante Local*. Aquel que se registra en el concurso mientras cursa el tercer grado de secundaria en una escuela, pública o particular, ubicada en la Zona Metropolitana de la Ciudad de México, sin adeudar materias de primer o segundo grado.

b) *Aspirante egresado*. Aquel que cuenta con su Certificado de educación secundaria al momento de registrarse.

c) *Aspirante foráneo*. Aquel que se registra en el concurso mientras cursa el tercer grado de secundaria en una escuela, pública o privada, ubicada fuera de la Zona Metropolitana de la Ciudad de México, sin adeudar materias de primer o segundo grado.

d) *Aspirante INEA*. Aquel que se registra mientras finaliza su educación secundaria en el Instituto Nacional de Educación para Adultos, dentro o fuera de la Zona Metropolitana.

3.2.2 Procesos para la etapa de registro de los aspirantes al concurso

***Pre-registro presencial*.**

Los aspirantes egresados, foráneos e INEA, acudieron al centro de registro 01, para recibir los materiales para el proceso de registro siguiendo el calendario establecido; de acuerdo al tipo de aspirante en este proceso se presentaron diferentes documentos para completar esta etapa y de esta forma obtener un comprobante de pre-registro, permitiendo que ellos puedan posteriormente a través de Internet dar de alta sus opciones educativas y modificarlas.

Pre-registro en línea.

Los aspirantes egresados, foráneos e INEA pudieron realizar el pre-registro ingresando al portal de Internet http://comipems.org.mx, imprimiendo su comprobante de pre-registro y presentar la documentación correspondiente al tipo de aspirante en el centro de registro 01, de acuerdo con el calendario establecido. Esta información fue almacenada directamente en el servidor central de la COMIPEMS en la SEP, a través del sistema Web y el cual permite acceder desde cualquier computadora que cuente con Internet.

Registro

Una vez que finalizó el proceso de pre-registro, los aspirantes locales, foráneos egresados y del INEA, acudieron personalmente al centro de registro en la fecha que les corresponde, donde entregaron la documentación señalada en la convocatoria, además de que todos los aspirantes sin incluir los locales presentaron su comprobante de pre-registro.

Concluido el registro los aspirantes, recibieron un comprobante-credencial que indicaba lugar, fecha y hora donde tendrían que presentar el examen, además de las opciones educativas seleccionadas por el.

Los aspirantes foráneos, egresados y del INEA acudieron al centro de registro 01, mientras que los aspirantes locales se dirigieron al centro de registro que les correspondía según la ubicación de la escuela secundaria donde realizaron sus estudios.

4 Definición del problema ó contexto de la participación profesional

4.1 Concurso de Ingreso a la Educación Media Superior 2005

En el año 2005 la COMIPEMS se propuso la puesta en línea del proceso de Pre-Registro, así como la concentración de la información generada en dicho proceso y el del Pre-registro Presencial. Así mismo, se contemplo la interconexión de algunos Centros de Registro para el manejo de los Aforos.

Para llevar a cabo estas actividades se solicito el apoyo de la Dirección General de Servicios de Computo Académico (DGSCA), a través de la Dirección de Sistemas (DS) para brindar el soporte técnico a la Infraestructura y analizar los requerimientos necesarios para su implementación.

Para los tres procesos durante la etapa de registro del Concurso de Ingreso a la Educación Media Superior, contó con características particulares, como infraestructura de red, comunicación, dirigido a cierto tipo de aspirantes, pero son dependientes uno del otro y la importancia del éxito obtenido en cada uno de estos es primordial para la credibilidad, reputación y validez del Concurso.

4.2 Pre-registro presencial y en línea

La información que el aspirante proporciono al sistema informático durante el proceso de Pre-Registro Presencial, a través de las capturistas, era almacenada en el servidor del Centro 01, y replicada al servidor central ubicado en el centro de cómputo de la COMIPEMS ubicado en la SEP, a través de una conexión cifrada, de acuerdo con el esquema de red mostrado en la figura 1. Esta replicación se realizó con el fin de permitir posteriormente que los aspirantes consulten sus datos, agreguen y modifiquen sus opciones vía Internet.

Se contó con una Terminal conectada directamente al Servidor Central de COMIPEMS, funcionando como mesa de control manteniendo disponible la información, para los aspirantes que realizarán este tramite a través del sistema en línea (Pre-Registro en Línea) y desearán confirmar sus datos en el Centro de Registro 01 o para aquellos que perdieran su comprobante.

4.3 Registro

Anteriormente el proceso de asignación de Aforos se realizaba de forma manual, lo cual generaba un proceso lento e incrementaba la probabilidad de presentar errores, ya que esta información se manejaba en cada uno de los centros de registro de manera asíncrona y sin algún control automatizado, por lo que en el año 2005 la COMIPEMS decide centralizar el manejo de la información de los Aforos a través de un sistema que permitiera manejar de una forma mas eficiente esta información, disminuyendo así la probabilidad de que se presentara algún incidente.

Durante este proceso no existió replicación en la base de datos, el enlace fue utilizado para transferir los respaldos diarios de la Base de Datos a través del servicio SFTP, y la liberación de Aforos entre el Servidor de Web de la SEP y cada uno de los Centros de Registro.

5.3 Solución propuesta

La COMIPEMS estableció como requisito para la propuesta de infraestructura, el uso de tecnología Intel, por lo que no se hizo una evaluación del desempeño de otras tecnologías de procesadores, por lo que la propuesta tecnológica se baso únicamente en determinar las características requeridas para el soporte del procesamiento del volumen de datos.

5.4 Tendencia tecnológica y la ley de Moore

La evolución tecnológica constante en el hardware viene marcando las tendencias de las soluciones para aplicaciones de Tecnologías de la Información y Comunicaciones en los siguientes campos:

- Aumento en el poder de cómputo.
- Consolidación en el uso de servidores y medios de almacenamiento.
- Seguridad: antivirus, buenas prácticas, análisis de riesgos, seguridad de la información, concientización del personal en el tema.

Al respecto del primer punto el aumento en el poder de cómputo seguirá duplicándose según la Ley de Moore (2 años), cada 18 meses aproximadamente según la industria.

La tecnología de manufacturación de los microprocesadores permitirá hacerlos cada vez más pequeños, eficientes y con mejor rendimiento, con una mayor integración (dos, cuatro y ocho núcleos) en el mismo circuito, una mayor velocidad de transferencia con canales dobles de 1066 MHz y 1333 MHz para procesadores y memorias (DDR3), velocidades de 300 MBps para discos duros de tipo SATA 2 y SAS, el aumento en la capacidad de almacenamiento en discos duros (750 GB – 1 TB), el aumento en la capacidad de la memoria caché a nivel L2 (microprocesador) y L3 (tarjeta madre) ayudan a la consolidación del uso de los servidores y de los medios de almacenamiento.

La información se ha convertido en uno de los activos más importantes de las empresas y las organizaciones, ha tomado una gran importancia en la vida personal de cada individuo y por este motivo requiere ser protegida de forma apropiada.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que pueden aprovechar cualquiera de las vulnerabilidades existentes dentro y fuera de la organización para comprometer activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Estas amenazas muchas veces suponen un gran obstáculo para la continuidad del negocio o en caso extremo puede llegar a comprometer a la organización en cuestión de horas, simplemente por no contar con medidas que permitan: la detección de algún ataque, del acceso a la información de una persona no autorizada, de la recuperación o reparación de la información afectada, es decir, no se dispone una eficaz gestión de la Seguridad de la Información.

5.5 Actualización Tecnológica

Un factor importante a considerar durante la fase de adquisición o actualización de un equipo es su ciclo de vida, si bien este se reduce por los rápidos cambios tecnológicos, de 5 a 3 años, muchas personas no toman en cuenta factores que nos permitirían reducir costos en la planificación en dicha fase, como son el considerar los costos directos, es decir, aquellos ocasionados con la adquisición, instalación, operación, mantenimiento y actualización del equipo, y los costos indirectos, como la capacitación del personal para el manejo del equipo,

tiempos de caída, tiempo perdido del empleado por la mala utilización de la tecnología, depreciación del equipo, refacciones y tendencias futuras de la tecnología. Para lo cual se puede utilizar un método de estimaciones financieras propuesta por Gartner, conocido como Costo Total de la Propiedad (Total Cost of Ownership, TCO) que sirve para respaldar las decisiones de planeación y adquisición de recursos a mediano y largo plazo, reflejando los costos no sólo de adquisición sino de uso y mantenimiento.

Así mismo, no se realiza un análisis de requerimientos de los recursos en base al uso que se le dará al equipo y que serán cubiertos por el mismo, siendo otro factor a considerar.

Por último se debe considerar que la infraestructura tecnológica debe estar siempre alineada a los objetivos estratégicos de la organización, así como el uso de buenas prácticas (ITIL).

5.6 Tecnología de Procesadores

Las tecnologías de procesadores que se pueden encontrar en el mercado de los servidores para organizaciones medianas y grandes por parte de Intel son Xeon e Itanium, como se muestra en la descripción de los procesadores a continuación:

- *Pentium 4*. Diseñado para ofrecer desempeño a través de los distintos usos (tales como el procesamiento de imágenes, la creación de contenido de vídeo, juegos y multimedia en las aplicaciones de hogar y oficina digital) en los cuales los usuarios finales realmente pueden apreciar el desempeño.

- *Xeon*. Diseñado para servidores que cubren desde aplicaciones de propósitos generales, enfocados a la pequeña empresa, de bajo costo, hasta procesadores de gran estabilidad y desempeño, para procesar varias transacciones al mismo tiempo (como aplicaciones de bases de datos, de cadena de suministros y de inteligencia empresarial) así como virtualización y consolidación.

- *Itanium 2*. Diseñado para infraestructuras de TI de uso elevado de datos y alta disponibilidad. Estos procesadores brindan la confiabilidad típica de los sistemas mainframe con un desempeño y una escalabilidad excepcionales. Asimismo, proporcionan una flexibilidad inigualable con el desempeño económico, escalable y confiable que necesita para la base del centro de datos.

Así por ejemplo, dentro de las series de procesadores Xeon de Intel tenemos la siguiente clasificación según su uso:

Serie	Uso
3000 y 3200	Propósitos generales, enfocados a la pequeña empresa, de bajo costo, para las pequeñas empresas y para satisfacer las necesidades empresariales básicas de servidor.
5000	Soluciones empresariales, desde servidores de aplicaciones a servidores de correo electrónico pasando por servidores de Internet, de uso general potentes, densos y confiables. Diseñado para configuraciones dobles.
7000	Gran estabilidad y desempeño, para procesar varias transacciones al mismo tiempo (como aplicaciones de bases de datos, de cadena de suministros y de inteligencia empresarial) así como virtualización y consolidación, permitiendo incrementar el uso de los servidores del centro de datos. Diseñado para configuraciones de 4 hasta 32 procesadores dobles.

Tabla 2. Series de Procesadores Xeon.

5.7 Tecnología en Discos Duros para Servidores

A continuación se describen algunas tecnologías utilizadas en la arquitectura de un servidor dedicado.

- ***SCSI (Small Computer System Interface).*** Interfaz estándar en paralelo para unir dispositivos periféricos, que proporciona velocidades de transmisión de datos rápidas arriba de 80 MBps. Algunas de los tipos de interfaz SCSI existentes son:

  SCSI-1: Utiliza un canal de 8 bits, tiene un conector de 25 terminales y soporta velocidades de transferencia de 4 MBps (1986).
  SCSI-2: Idéntico al SCSI-1 pero con un conector de 50 terminales y soporta múltiples dispositivos.
  Wide SCSI: Utiliza un cable más ancho (168 hilos para 68 terminales) para soportar transferencias de 16 bits.
  Fast SCSI: Utiliza un canal de 8 bits, pero dobla la velocidad de reloj para soportar velocidades de transferencia de datos de 10 MBps.
  Fast Wide SCSI: Utiliza un canal de 16 bits y soporta velocidades de transferencia de datos de 20 MBps.
  Ultra SCSI: Utiliza un canal de 8 bits y soporta velocidades de transferencia de datos de 20 MBps.
  SCSI-3: Utiliza un canal de 16 bits y soporta velocidades de transferencia de datos de 40 MBps. También es llamado Ultra Wide SCSI.
  Ultra2 SCSI: Utiliza un canal de 8 bits y soporta velocidades de transferencia de datos de 40 MBps.
  Wide Ultra2 SCSI: Utiliza un canal de 16 bits y soporta velocidades de transferencia de datos de 80 MBps.

  En cuanto a medios de almacenamientos la tecnología SCSI permite un alto desempeño con velocidades de transferencia de datos superiores a los 80 MBps y una eficiencia mayor en términos de lecturas y escrituras, siendo una opción para sistemas de almacenamiento en servidores con aplicaciones NAS (Network Attached Storage) y SAN (Storage Area Network) o híbridas.

- ***SAS (Serial Attached SCSI***). Soporta arriba de 128 dispositivos de diferentes tamaños y tipos unidos utilizando cables más delgados y largos (hasta de 8 metros de largo), soporta una velocidad de transferencia full-duplex de 3 Gbps por cada canal. El ancho promedio de estos discos es de 2.5 pulgadas.

  Estos dispositivos pueden ser hot-plug y se pueden comunicar con dispositivos SATA y SCSI (el backplane de los SAS es idéntico al de los SATA), además de ser capaces de trabajar a velocidades de transferencia de 1.5 Gbps para sincronizarse con los dispositivos SATA.

  Los dispositivos SAS a diferencia de los SCSI tradicionales tienen dos puertos, cada uno de ellos reside en un dominio SAS diferente, lo que permite una redundancia para prueba de fallos, lo que permite seguir transmitiendo en caso de que uno falle a través de una ruta separada e independiente.

- ***SATA (Serial ATA y Serial Advanced Technology Attachmen***t). Este dispositivo crea una conexión punto a punto entre dos dispositivos a través de un cable de datos con 4 hilos, ideales para equipos PC que cumplan con el Factor de Forma Pequeña (SFF, Small Form Factor), la longitud del cable de conexión puede ser mayor de un metro a diferencia de los 40 cm. que tendrían los dispositivos IDE tradicionales de 40 u 80 hilos.

  La tecnología Ultra ATA soporta hasta dos dispositivos unidos a un canal vía un canal compartido, siendo conocidos como maestro y esclavo, a diferencia de la SATA en donde mediante una topología de punto a punto, es decir, cada origen es conectado a un destino, permitiéndole tener canales que trabajan independientemente.

Los dispositivos SATA tienen una velocidad de transferencia de 1.5 Gbps en un solo sentido por canal (protocolo half-duplex). Permite vía hardware la remoción en caliente (Hot Swap).

- ***Canal de Fibra (Fibre Channel, FC).*** Es una tecnología de interconexión Gigabit altamente confiable que permite comunicaciones concurrentes entre estaciones de trabajo, mainframes, servidores, sistemas de almacenamiento de datos y otros periféricos usando SCSI y protocolos IP. Provee sistemas de interconexión para topologías múltiples que pueden escalar a un sistema de ancho de banda total en el orden de un Terabit por segundo. Esta tecnología es utilizada en la actualidad en switchs, concentradores (hubs), sistemas de almacenamiento, dispositivos de almacenamiento y adaptadores, sin embargo, es una tecnología costosa.

  El canal de Fibra esta siendo proporcionado como una interfaz estándar de disco, la industria de fabricantes de RAID se ha enfocado a la utilización del Canal de Fibra en sus sistemas de almacenamiento. Es recomendable para ambientes que requieran de una transferencia de datos alta y eficiente.

5.8 Buenas prácticas sobre ITIL

Los líderes del proyecto se apoyaron en las buenas prácticas para la gestión de servicios de Tecnologías de la Información, en el estándar de ITIL, el cual esta enfocado a los procesos, la tecnología y requerimientos técnicos-operacionales de la organización.

Con referencia a estas buenas prácticas se pudo planificar la capacidad de la infraestructura con la que se contaba en ese momento y además de eso estimar el volumen de crecimiento para poder cubrir las demandas de disponibilidad para los concursantes.

5.9 Infraestructura del centro de cómputo de la SEP

En el Centro e cómputo de la SEP se disponía con los siguientes recursos para dar soporte a cada uno de los procesos.

- Servidor Web. 2 Procesadores Xeon a 2.8 GHz, Memoria RAM de 4 GB, Sistema Operativo Red Hat Enterprise Linux, 2 Discos Duros SCSI de 36 GB, Tarjeta Ethernet 10/100/1000, Servicio HTTP con Apache y PHP.
- Servidor de Bases de Datos. 2 Procesadores Xeon a 2.4 GHz, Memoria RAM de 1.2 GB, Sistema Operativo Red Hat Enterprise Linux, 2 Discos Duros SCSI de 36 GB, Tarjeta Ethernet 10/100/1000, servicio de bases de datos con PostgreSQL.

Se recomendó que estos servidores se escalaran en la memoria RAM hasta 8 GB, para soportar la carga de datos que se tuvo con la concurrencia de los procesos Pre-Registro en Línea y la replicación de la información de la base de datos del centro 01 durante el pre-registro presencial.

5.10 Infraestructura de los Centros de Registro

Para dar soporte a dichos procesos entre los diferentes centros de registro y el centro de cómputo de la SEP, proponiéndose lo siguiente para cada centro de registro:

- Servidor Web y de Base de Datos. Procesador dual Xeon 2.4 GHz, Memoria RAM de 4 GB, Sistema Operativo Red Hat Enterprise Linux, 2 Discos Duros SCSI de 36 GB, Tarjetas de Red 10/100/1000, Servicio HTTP con Apache y PHP, servicio de BD con PostgreSQL.
- Firewall. Procesador Pentium 4 a 2.4 GHz, Memoria RAM de 1GB, 1 Disco Duro de 80 GB, Sistema Operativo Red Hat, 2 Tarjetas Ethernet 10/100, firewall con ipchains.
- Conexiona Internet. Servicio ADSL, ancho de banda de 1 Mbps, dirección IP fija especificada por el proveedor.
- Mesa de Control. Se contara con una Terminal conectada directamente al Servidor Central de COMIPEMS, funcionando como mesa de control, para los aspirantes que realicen este tramite a través del sistema en línea, es decir realicen el proceso Pre-Registro en Línea, y deseen confirmar sus datos en el Centro de Registro 01 o pierdan su comprobante.

Se solicito dejar los servicios, mostrados en la Tabla3, habilitados en todos los servidores y evitar cualquier otro servició por seguridad.

Servicio	Servidor BD	Servidor Web
SMTP	☐	☑
SSHD. (Secure Shell) Permite conexiones de Terminal sobre un canal de transmisión seguro.	☑	☑
HTTP (Hyper Text Transfer Protocol)	☐	☑
STUNNEL. Permite creación de canales de transmisión seguros (cifrados)	☑	☐
PostgreSQL. Servidor de base de datos	☑	☐
CROND. Permite la ejecución de tareas programadas.	☑	☐

Tabla 3. Servicios por tipo de Servidor.

5.11 Arquitectura del centro de cómputo de la SEP

Durante el proceso de Pre-Registro Presencial y en Línea, fue necesario que el centro de computo de la SEP, permitiera únicamente la conexión de la Dirección IP_Centro_de_Registro proporcionada por el proveedor del servidor de Internet, con la intención denegar el acceso a cualquier otra dirección IP, y como consecuencia cualquier petición de conexión hacia el Centro de Computo de la SEP, como se muestra en la figura 1.

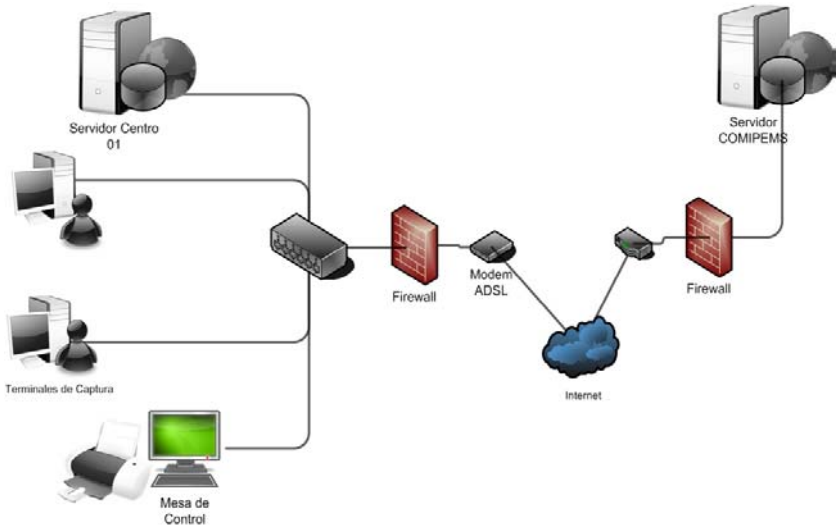

Figura 1. Enlace entre Centro de Registro 01 y Centro de Computo de la SEP

Además, fue necesario indicar en el Firewall de la SEP, la regla que permitiera las conexiones hacia el puerto SECURE_PG_PORT utilizado en la transferencia de datos cifrados de la base de datos, a través del software Stunnel, entre los Servidores del Centro de Registro 01 y el Servidor de la SEP; así como para el puerto SSH_PORT, para las conexiones entre Firewall del Centro 01 y los servidores la SEP.

Por motivos de monitoreo y administración remota de los servidores, a través del personal de la Dirección de Sistemas, fue necesario permitir las conexiones por el puerto SSH_PORT, para algunas direcciones IP pertenecientes a la Dirección de Sistemas

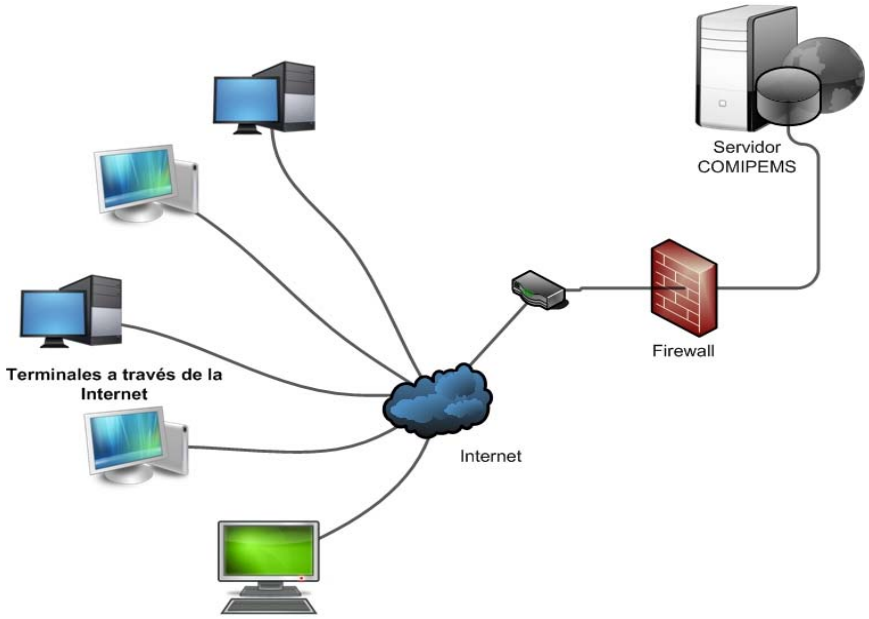

Figura 2. Topología de red del proceso de Pre-Registro en Línea

Para el caso de los centros de registro, donde se realizó la transferencia de los respaldo de bases de datos y fotografías, durante el proceso de Registro de Aspirantes, fue necesario permitir las conexiones entre el servidor del centro de computo de la SEP, con cada uno de los servidores de los centros de registro a través del puerto SSH_PORT. La topología de red que se tuvo para dicho proceso se muestra en la figura 3.

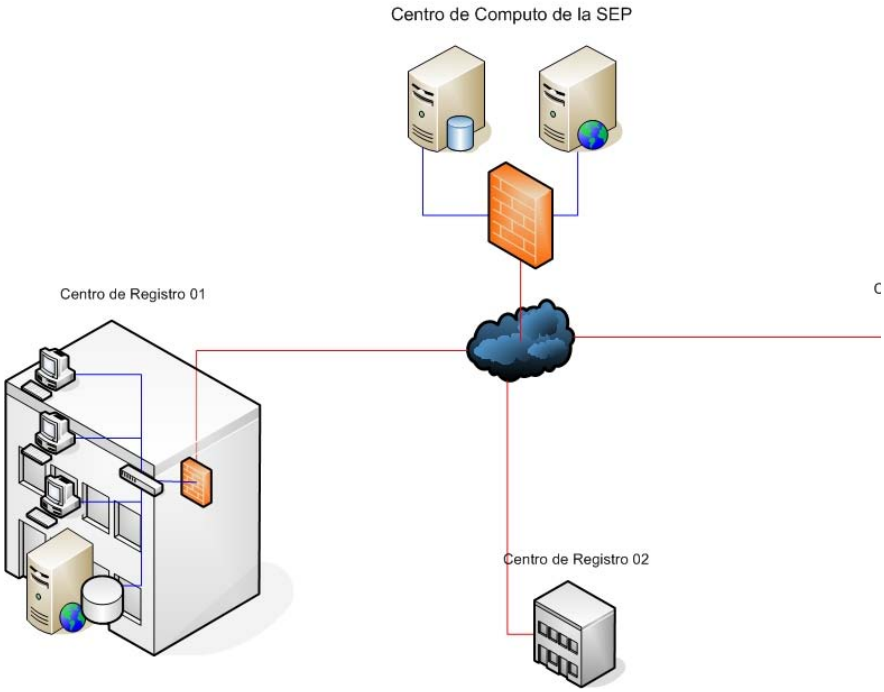

Figura 3. Topología de red del proceso de registro de aspirantes.

Fue requerido el apoyo del personal de redes de la SEP, para el monitoreo de su red durante el proceso de Pre-registro en línea con el fin de evitar y prevenir cualquier incidente.

5.12 Arquitectura del Centro de Registro

El Centro de Registro 01, Colegio de Bachilleres, a través del enlace establecido por una IP homologada especificada por el proveedor, se conectó a la Red Loca a través de un Firewall, con dos interfaces de red con sistema operativo Red Hat (Figura 4), cuyas reglas y

funcionamiento basadas en direcciones IP y puertos de servicios, posteriormente será descrito mas a detalle.

Las Terminales de Captura y Mesa de Control, todas ellas PC's; así como el Servidor, formaron parte de la Red Local del Centro de Registro 01, como se muestra en la Figura 4. A esta red se asignaron Direcciones IP privadas, cuya puerta de enlace con el exterior fue la interfaz Interna del Firewall, sin embargo no todas las PC's contaron con acceso a Internet.

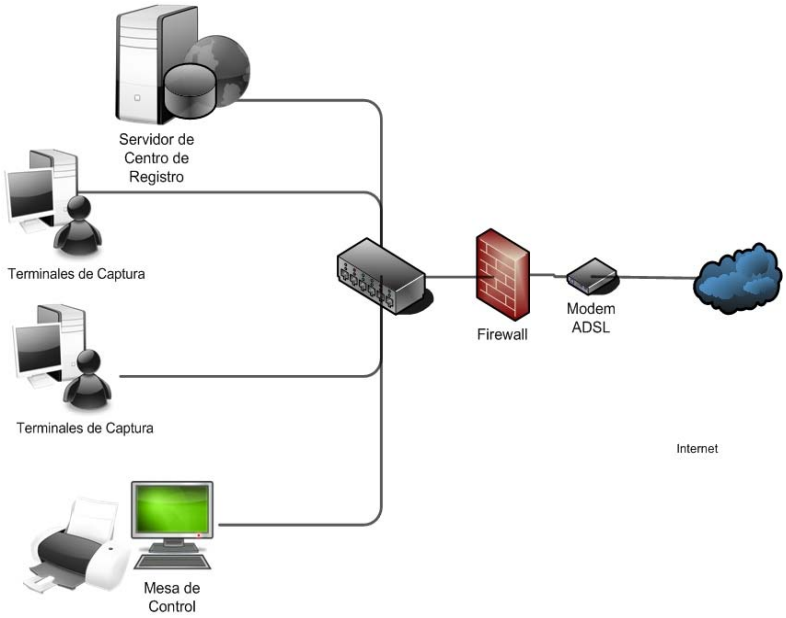

Figura 4. Red Local del Centro de Registro.

La Mesa de Control, fue una PC para consultar los datos de los aspirantes que habían realizado su pre-registro a través del sistema en línea, y deseaban confirmar la información que proporcionada. Esta información se presentó a través del sistema en Línea, por lo que la conexión con el centro de Cómputo de la SEP, se realizó a través de WEB.

Para los 39 centros de registro restantes se requirió de un enlace dedicado de 256 Kbps, como mínimo, para aquellos de mediana escala, afluencia de 9000 a 15000 aspirantes y un enlace de 128 Kbps para aquellos escala pequeña que recibían hasta 8000 aspirantes. Este enlace se utilizo durante el proceso de registro para transferir los respaldos de la BD cada día y para la liberación de Aforos entre el servidor de aplicación de la SEP y cada uno de los centros de registro.

5.13 Cálculo del ancho de banda

Para la arquitectura de red que se menciono anteriormente (ver figura 4), se utilizó un enlace dedicado, de 1 Mbps con dirección IP estática, ya que se requería para otorgar el acceso a los servicios dentro del centro de Cómputo de la SEP, con la finalidad de garantizar la conexión. El ancho de banda se obtuvo de la siguiente estimación.

Para la tarea de replicación de la información contenida en a Base de Datos, se obtuvo los cálculos del mínimo ancho de banda requerido (ver Tabla 3), para soportar tareas como la transferencia de datos durante el proceso de Registro.

Total de bits en tablas/registro	80 Kb
Numero de Terminales de Captura	68
Transmisión de los registros Concurrente	5.4 Mbps

Promedio de registro de aspirantes por día	8000
Transmisión por día	**634 Mb**

Tabla 4. Cálculo de Transmisión total por día para el centro 01.

Calculo de Ancho de Banda del Centro de Registro 01					
		Enlace [kbps]			
		1024	512	256	128
Transmisión por día	634 Mb	10.5 min.	20.5 min.	41.63 min.	82 min.

Tabla 5. Calculo de ancho de banda para el enlace SEP-centro registro 01

Con esto se recomendó un enlace de 512 Kbps como mínimo para el Centro de Registro, para el enlace entre los servidores de este centro y los del centro de cómputo de la SEP.

Para los centros de mediana escala, según las estadísticas reportadas por COMIPEMS, se registran aproximadamente año con año 600 alumnos, y con los datos de la tabla 6, se estimo que el ancho de banda que soporta la tarea de los respaldos por día de la base de datos requería el mínimo ancho ofrecido.

Total de bits en tablas/registro	80 Kb
Promedio de registro de aspirantes por día	1150
Transmisión por día	**10 Mb**

Tabla 6. Cálculo de transmisión total por día para centros de mediana escala

Calculo de Ancho de Banda de Centros de Registro de mediana concurrencia					
		Enlace [kbps]			
		1024	512	256	128
Transmisión por día	10 Mb	20 seg.	1 min.	2 min.	3 min.

Tabla 7. Cálculo de ancho de banda para el enlace SEP-centros de mediana escala

6. Participación profesional

6.2 Sistema operativo Red Hat Enterprise Linux

Red Hat Enterprise Linux (RHEL) es una distribución comercial Linux creada y soportada por la compañía Red Hat que ha creado una distribución del sistema operativo GNU/Linux.

La compañía se enfoca hacia el mercado de los negocios con la distribución Red Hat Enterprise Linux y la versión no comercial Fedora Core. Actualmente la nuevas versiones de Fedora se lanzan aproximadamente cada 6 meses, mientras las de RHEL cada 18 o 24 meses.

A continuación se muestran las Versiones de Red Hat Enterprise Linux:

- Red Hat Enterprise Linux 1.
- Red Hat Enterprise Linux 2.1 AS, publicada el 6 de mayo de 2002.
- Red Hat Enterprise Linux 3, publicada el 22 de octubre de 2003.
- Red Hat Enterprise Linux 4, publicada el 15 de febrero de 2005.
- Red Hat Enterprise Linux 5, publicada el 14 de marzo de 2007.

Características

Se vende bajo suscripción, y está certificado por los principales fabricantes de hardware y software, entre ellos tiene un nivel de seguridad certificado por Common Criteria.

Se cuenta con las siguientes ediciones:

EDICIÓN	DESCRIPCIÓN
AS (Advanced Server).	Soporta sistemas de misión crítica y high-end, disponible con los más altos niveles de soporte.
ES (Entry Server).	Solución para servidores pequeños y de mediano rango utilizados para la mayoría de las necesidades computacionales de los negocios de hoy día**.**
WS (Workstation)	Recomendable para estaciones de trabajo técnicas y para las necesidades de escritorio/cliente de una sola unidad, incluyendo desarrollo de software, escritorios de grandes capacidades, aplicaciones cliente de fines específicos y computación de alto rendimiento.
Red Hat Desktop	Ideal para los desarrollos de sistemas clientes en volúmenes. Disponible en paquetes de 10 y 50 unidades y enlazados con Red Hat Network Proxy o con Satellite Server.

Tabla 8. Ediciones de Red Hat Enterprise Linux

6.2 Instalación

La instalación se realizó desde los CD-ROM incluidos en la distribución y utilizando la Interfaz Gráfica de Usuario (GUI), el proceso fue sencillo y describe brevemente los pasos mas importantes, en las siguientes líneas.

Particionamiento de disco(s) personalizado. El particionamiento de discos permite dividir el disco en secciones, donde cada sección se tratara como un disco duro independiente. Existen dos formas en las que se puede realizar la partición de disco(s) durante la Instalación, el primero es el particionamiento automático, el cual realiza esta tarea únicamente con la selección de un esquema de los presentados por el instalador. El segundo, es el particionamiento manual con Disk Druid, en el cual es necesario crear/borrar/eliminar particiones en disco(s), como se muestra en la figura 5.

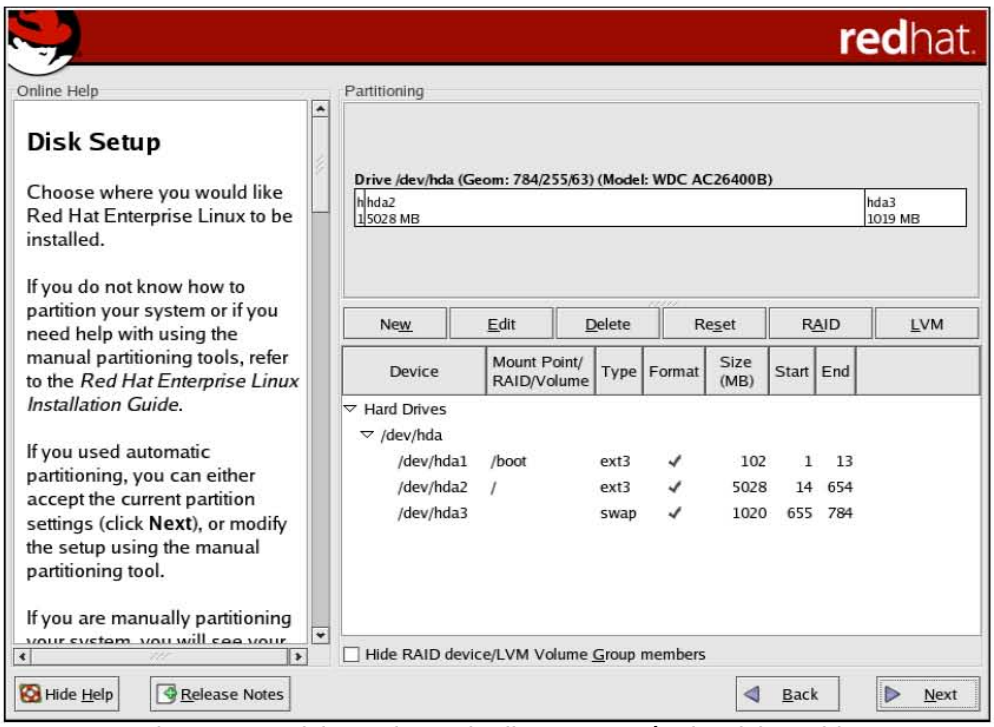

Figura 5. Particionamiento de discos a través de Disk Druid.

Configuración del gestor de arranque. Es posible inicializar el sistema sin la necesidad de contar con un diskette, instalando un gestor de arranque, el cual es el primer software que se ejecuta cuando se enciendo la computadora. Es responsable de la carga y transferencia del control al kernel del sistema operativo. El instalador del RHEL ofrece dos gestores de arranque GRUB por defecto y LILO. No se modificó la configuración por defecto del gestor de arranque, tampoco se estableció una contraseña para este.

Configuración de Red. El programa de Instalación detecta las interfaces de red con las que se cuentan, poniendo a disposición la posibilidad de modificar su configuración por defecto, la cual es por DHCP, para lo que se deben especificar los siguientes datos:

- Dirección IP.
- Nombre de la maquina.
- Puerta de enlace (Gateway).
- Servidores de nombres (DNS).

Configuración de firewall. Por defecto RHEL nos permite habilitar un nivel de firewall el cual rechaza conexiones a la maquina de acuerdo con el nivel especificado, excepto aquellas definidas por el mismo sistema como las peticiones al DNS. Se deshabilitó esta opción, debido a que la red de cada centro contaría con un firewall.

Selección del software a instalar. Por defecto RHEL ofrece un conjunto de paquetes que se instalaran, lo cuales dependen de la versión de RHEL, pero también permite personalizar la selección de los paquetes deseados, a través de una pantalla que ofrece diferentes grupos de paquetes y cada grupo tiene paquetes individuales a seleccionar.

3.2.3 Post Configuración

Una vez instalado el sistema operativo se prosiguió con la eliminación de algunos servicios que el sistema de Instalación habilitan por defecto para ello se utilizó la herramienta *chkconfig* que se describe a continuación.

Chkconfig. Provee un herramienta, en línea de comandos, para mantener los directorios /etc/rc[0-6].d, evitando así que los administradores manipulen directamente los enlaces simbólicos en estos directorios.

Tiene 5 diferentes funciones:

Sintaxis	Función
chkconfig --list [nombre]	Agregar nuevos servicios
chkconfig --del [nombre]	Remover servicios
chkconfig --list [nombre]	Mostrar la configuración de los servicios actuales
chkconfig [--level nivel] nombre <on|off|reset>	Modificar la configuración de servicios
chkconfig [--level levels] nombre	Mostrar la configuración de un servicio en particular

Tabla 9. Funciones de *chkconfig*

RPM. Gestor de paquetes, cuyas funciones son construir, instalar, verificar, actualizar, consultar y borrar paquetes de software individuales. Un paquete consiste en un conjunto de archivos, utilizado para la instalación y el borrado del conjunto de archivos. Además, gestiona una base de datos de todos los paquetes instalados en el sistema y sus archivos, la cual puede ser utilizada para actualizar el sistema.

A continuación, se mostraran los usos y opciones más comunes del gestor de paquetes rpm, los cuales se han obtenido del manual (man rpm).

Acción	Sintaxis
Instalación de un paquete	rpm -ivh nombre-archivo.rpm
Actualización de un paquete	rpm -Uvh nombre-archivo.rpm
Desinstalar un paquete	rpm -e nombre_paquete
Consulta si un paquete esta instalado	rpm -q nombre_paquete
Obtener información de un paquete instalado	rpm -qi nombre_paquete
Lista los archivos que contiene un paquete	rpm -ql nombre_paquete
Obtener el paquete al que pertenece un archivo	rpm -qf <path-to-filename>

Tabla 10. Uso común de RPM

3.3 Requerimientos de Software para el centro de Registro

Para la aplicación Web que dio soporte al sistema de pre-registro y registro de aspirantes, que fue accedida por las terminales de cada centro de registro a través de un navegador, fue necesario instalar en el servidor de cada centro de registro el siguiente software.

Software requerido
APACHE-HTTP
PHP
POSTGRESQL
VSFTP

Tabla 11. Software Requerido.

3.3.1 Automatización

Para la instalación de este software en los 39 servidores se utilizo el siguiente un CD-ROM que contiene un script de bash, el cual automatizó el proceso de instalación, así como la configuración de los servicios y base de datos. La instalación del software listado en la tabla 9 se realizó con la herramienta rpm, la cual utilizó los paquetes que se encontraban en el disco

que contenía dicho script. El proceso y los pasos consecutivos del script se describen a continuación.

Instalación de los paquetes de software. La instalación del software requerido para el soporte del sistema se realizo con la herramienta rpm, que como se describió en la tabla 8. Se instalaron los paquetes necesarios para tener los servicios Web, el lenguaje de programación PHP, PostgreSQL, FTP seguro y base de datos, por ejemplo:

rmp -ivh php-x.x.x.ent.i386.rpm

Configuración de los servicios. Se utilizaron los archivos de configuración que se encontraban en el CD-ROM de instalación para sustituir los archivos que por defecto crean los paquetes de instalación (rpm's), de tal forma que no se tuvo que modificar los archivos manualmente. Este proceso se realizó de la siguiente forma:

cp /media/cdrom/archivo_configuración.conf /apache/conf/

Instalación de librerías. Se realizo la instalación de librerías especiales necesarias para el sistema COMIPEMS, para ello se ejecutaron los comandos necesarios y específicos de cada librería.

Configuración y verificación del los niveles y servicios del sistema con la herramienta chkconfig. Con la ayuda de chkconfig se eliminaron los servicios innecesarios que por defecto la instalación del sistema operativo habilita. La eliminación de los servicios se realizó de la siguiente forma:

chkconfig –level 345 sendmail off

Verificación del software instalado. Para asegurar que los paquetes se hubieran instalado se obtuvo una lista de software instalado en el sistema con la siguiente instrucción, para cada paquete, de tal forma que si se obtiene la salida, de la especificación de paquete queda por entendido que ese paquete había sido instalado correctamente.

rpm -q http

Configuración de la base de datos PostgreSQL. Esta parte del script consistió en copiar el archivo de configuración del CD-ROM, establecer los permisos y el usuario correcto de dicho archivo, e iniciar la base de datos.

Instalación del Sistema COMIPEMS. Se instaló el sistema en su ubicación final, al descomprimir un paquete, como se muestra a continuación:

tar xvzf archivo.tar.gz

Creación e inicialización de la base de datos COMIPEMS. Una vez que se inicializó el sistema de bases de datos, fue posible ejecutar el archivo SQL, que contiene la base de datos del sistema. Este script se ejecutó de la siguiente forma.

su -c /tmp/initdb.sh postgres

3.4 Stunnel

Con Stunnel es posible cifrar con SSL (Secure Sockets Layer) conexiones TCP, en sistemas UNIX y Windows, asegurar demonios y protocolos, sin la necesidad de modificar el código de los demonios. El código fuente de Stunnel es distribuido bajo la licencia GNU GPL.

Stunnel no provee la funcionalidad SSL, por lo que aun se requiere una librería SSL funcionando dentro del sistema, como OpenSSL o SSLeay, para compilar el programa stunnel.

Esto significa que stunnel solo soporta las funciones que la librería SSL implementa, es decir, la compilación de estas librerías establece que algoritmos se usaran.

Stunnel hace posible el cifrado de conexiones de cualquier puerto simple TCP, estos son los servicios que solo utilizan un puerto y no utilizan mas de uno para otras funciones; por ejemplo HTTP, escucha y maneja todas sus conexiones a través de un solo puerto, pero FTP escucha generalmente por el puerto 21 para establecer las conexiones, pero utiliza otros puertos aleatorios para transferir datos.

3.4.1 Análisis

Stunnel puede desempeñar cualquiera de las siguientes funciones:

- Recibir datos no cifrados, cifrarlos y enviarlos a un servidor.
- Recibir datos cifrados, descifrarlos y enviarlos a un puerto arbitrario en esa u otra maquina.
- Iniciar un programa local (como lo hace inetd) para que este intercambie información con la maquina remota sobre un canal cifrado.

En sistemas UNIX, stunnel puede correr bajo inetd, como teltnetd o ftpd, o es posible que se ejecute como un servicio standalone.

Stunnel utiliza solo un programa binario stunnel, que puede ejecutarse de dos modos:
- Cliente. Stunnel escucha las conexiones descifradas y las reenvía a través de una conexión cifrada SSL a una máquina remota que ejecuta stunnel.
- Servidor. Stunnel escucha conexiones cifradas SSL, descifra y reenvía estas sesiones a un proceso.

3.4.2 Configuración

En versiones anteriores a la 4, las configuraciones se realizaban desde la línea de comandos, por ejemplo *stunnel -c -d rsync -r ssyncd -N ssync.* Mientras que para las versiones 4 y posteriores, stunnel utiliza un archivo de configuración: *stunnel.conf*, cuya ubicación por defecto es: */usr/local/etc/stunnel/stunnel.conf* si se instala desde el código fuente, pero si se utilizan paquetes binarios generalmente se encuentra en */etc/stunnel/stunel.conf*.

A continuación se muestra como se configura stunnel en las modalidades:

Servidor Stunnel

Para la configuración de stunnel en modo servidor se tiene los siguientes pasos:

Versiones anteriores a 4.0

Para las versiones anteriores a 4.0, stunnel se configuraba en la línea de comandos, donde se indican todos los parámetros, como se muestra a continuación:

stunnel -d <puerto_escucha> -r <redirecciona_a_ip>:<puerto> -p <certificado>

Versión 4.0 y mayores

- Es necesario que para la maquina que tendrá el rol de servidor se cuente con un certificado.
- Es opcional modificar el archivo /etc/services, agregando una línea para los puertos en los que stunnel escuchara las conexiones remotas, de tal forma que la línea de comandos sea manejada a través de estos identificadores y no por los puertos, por ejemplo:

  /etc/services
  ssyncd 273/tcp #Servicio rsync seguro

- Modificar el archivo de configuración /etc/stunnel/stunnel.conf de la forma indicada en la tabla 12, donde se le indica que utilice el certificado, ejecutarse en modo servidor, utilice el

servicio de TCPwrappers [servicio] como nombre de servicio TCPwrappers, escuchar los paquetes cifrados del puerto de y reenviar los paquetes descifrados a.

```
cert=/etc/stunnel/certificado.pem
client = no
[ssync]
accept=ssyncd
connect=rsync
```

Tabla 12. Archivo stunnel.conf en el servidor Stunnel

- El último paso es iniciar stunnel con el comando stunnel. No tiene importancia el orden de inicio de stunnel en modo servidor o cliente, ya que este no intentara iniciar un túnel hasta que no lo necesite. Si el certificado indicado esta protegido por contraseña, se solicitara cuando se inicia stunnel.
- Es recomendable verificar el inicio de los procesos mediante ps auxw y buscar el proceso stunnel.

Cliente Stunnel.- Para la configuración de stunnel en modo cliente se tiene los siguientes pasos:

Versiones anteriores a 4.0

Para las versiones anteriores a 4.0, stunnel se configura en la línea de comandos, donde se indican todos los parámetros, como se muestra a continuación:

stunnel -c -d [dirección_ip:]<puerto_escucha> -r <redirecciona_a_ip>:<puerto>

Versión 4.0 y mayores

- (Opcional) Añadir otra línea en /etc/services para definir un puerto de reenvío propio para stunnel.

  ssyncd 273/tcp #Servicio rsync seguro

- (Opcional) Si stunnel fue compilado con libwrap, también deberá añadirse la línea que permite las conexiones a este servicio, en el archivo /etc/host.allow, como se indica:

  /etc/hosts.allow
  ssync: ALL

- Modificar el archivo de configuración /etc/stunnel/stunnel.conf de la forma indicada en la tabla 11, donde se indica a stunnel ejecutarse en modo cliente a través del parámetro client, utilice el servicio [servicio] como nombre de servicio TCPwrappers, escuche las conexiones locales en el puerto accept y reenvié los paquetes descifrados a connect, como se muestra en la tabla 13.

```
client = yes
[ssync]
accept=rsync
connect=servidor:ssync
```

Tabla 13. Archivo stunnel.conf en el cliente Stunnel

- Iniciar Stunnel, ejecutando el comando stunnel.
- Como pruebas podemos ejecutar rsync normalmente con el comando rsync.
  $ rsync localhost::

Parámetro	Valor	Descripción
client	yes | no	Indica si stunnel se ejecutara en modo cliente, en caso contrario se ejecutara en modo servidor.
cert	/ruta.../nombre_archivo	Especifica la ruta del certificado.
[nombre_de_servicio]	Por ejemplo: ssync, 889	Indica el nombre de servicio a pasar por stunnel en las llamadas ala librería libwrap
accept	[IP:]puerto-de-servicio	Indica la dirección IP y puerto que escuchara stunnel. Puerto de servicio puede ser un puerto TCP numérico o un nombre de servicio declarado en /etc/services. En modo servidor indica donde se escucharan los paquetes cifrados y en modo cliente donde se escucharan los paquetes en claro.
connect	[IP:]puerto	Indica el puerto al que stunnel enviara los paquetes, en modo servidor envía los paquetes recibidos por el puerto accept (después de descifrarlos). En modo cliente, indica el puerto en el que el sistema remoto escucha las conexiones del túnel.
chroot	/ruta.../de../chrootjail	Indica a Stunnel que se ejecute dentro de una chroot jail, después de leer su archivo de configuración, pero antes de escribir su PID, analizando hosts.allow y hosts.deny.
setuid	nombre_usuario o UID	Indica el nombre o UID de la cuenta de un usuario no privilegiado, bajo en cual Stunnel funcionara.
setguid	nombre_grupo o GUID	Indica el nombre o GUID del grupo no privilegiado, bajo en cual Stunnel funcionara.

Tabla 14.Parámetros utilizados para configuración de Stunnel.

3.4.3 Implementación

Para el proceso Pre-Registro presencial de COMIPEMS descrito en los antecedentes, fue necesario permitir que los aspirantes consultarán sus datos, agregarán y modificarán sus opciones vía Internet, requiriendo tener cada registro que se obtuvo a través del pre-registro presencial, en el sistema en línea, por lo que se realizó una replicación de la base de datos de forma unidireccional, de maestro a esclavo a través de la sincronización de una tabla, del servidor del Centro de Registro 01 al servidor central de COMIPEMS en la SEP, de forma automática, como se muestra en la figura 6. La replicación de la base de datos en PostgreSQL se realizo con el software DBmirror.

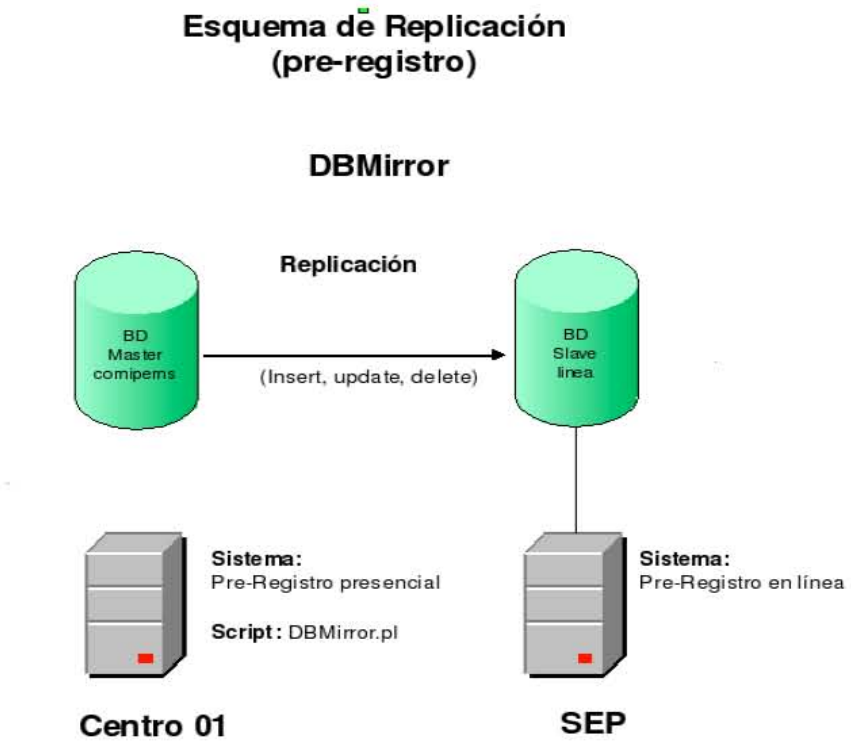

Figura 6. Esquema de replicación en el proceso de Pre-Registro.

Para realizar la replicación de los datos de pre-registro presencial del Centro 01 al centro de cómputo de la SEP, se ejecutaron los siguientes puntos:

- Configuración de DBMirror Maestro en el servidor Web del Centro 01, especificando la base de datos y tablas a replicar.
- Configuración de DBMirror Esclavo en el servidor de bases de datos en la SEP, indicando la base de datos y las tablas esclavas.
- Configuración del servicio de stunnel-servidor en el gateway del Centro 01, donde se procesa el cifrado y envió de datos al servidor de la SEP.
- Configuración del servicio de stunnel-esclavo en el servidor de bases de datos de la SEP, donde se hizo el descifrado de la información, siendo enviada a la misma maquina y procesada por DBMirror.
- Poner en marcha la replicación al ejecutar el comando: *./DBMirror archivo.conf.*
- La verificación de la replicación consistió en consultar el número de aspirantes pre-registrado en Centro 01, numero que coincidiría con el número de aspirantes pre-registrados presencialmente en la base de datos línea del servidor de la SEP.
- Para corroborar el cifrado de los datos solo bastó asegurar el paso de los datos por el canal establecido para ello con utilerías del sistema operativo, como:

  tcpdump -X port <puerto>

Descripción del proceso de replicación.

El proceso de replicación de la información transmitido por el software Stunnel, se explica a continuación y se muestra en la figura 7.

1. El servidor del centro de registro 01 realiza una petición al puerto local LOCAL_PG_PORT.
2. Esta petición viaja a través de la red interna del centro de registro 01 hasta su puerta de enlace que es el firewall.
3. En el firewall se encuentra un demonio stunnel-cliente escuchando peticiones por el puerto LOCAL_PG_PORT de su interfaz interna, por lo que todas las peticiones que intenten pasar por el puerto LOCAL_PG_PORT de esta son atendidas por el demonio de stunnel-cliente, cifrando los datos con SSL.

4. Stunnel envía los datos cifrados al servidor de base de datos de la SEP por el puerto SECURE_PG_PORT.
5. El servidor de bases de datos de la SEP acepta la petición a través del puerto SECURE_PG_PORT, donde se encuentra un stunnel-servidor.
6. Stunnel-servidor descifra los datos.
7. Stunnel-servidor envía los datos descifrados al puerto LOCAL_PG_PORT de la maquina local, es decir al puerto del servicio de bases de datos postgresql.

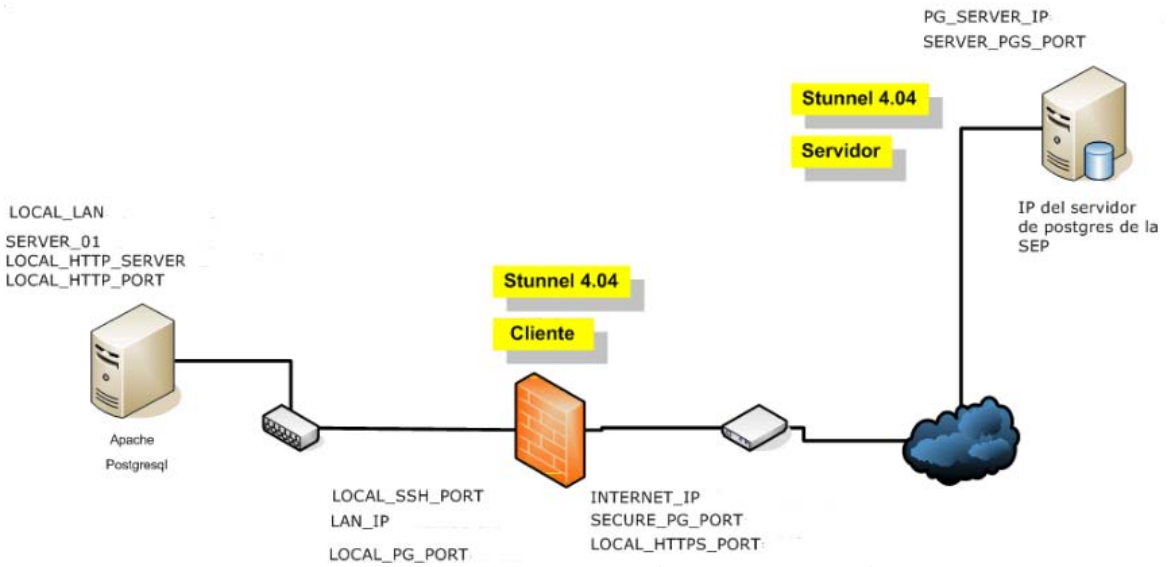

Figura 7. Esquema de stunnel durante la replicación de la información en el pre-registro.

3.4.3.1 Implementación Stunnel-Cliente en firewall del centro de registro 01

Para el centro de registro 01, se conservo el firewall con el sistema operativo Red Hat que fue utilizado en el Concurso del año 2005, por lo que el software stunnel con el que se contó en dicho sistemas fue anterior a la versión 4, esto nos llevó a que la configuración y ejecución de stunnel se realizó desde la línea de comandos, como se muestra a continuación:

stunnel -c -d <IP_LOCAL>:LOCAL_PG_PORT -r <IP_SERVIDOR_BD>:SECURE_PG_PORT

De esta forma, le indicamos a stunnel que cualquier conexión que intente realizar una conexión al puerto LOCAL_PG_PORT a través de la interfaz interna del firewall, cifra y envia los datos al la dirección IP del servidor de bases de datos de la SEP al puerto SECURE_PG_PORT.

3.4.3.2 Implementación Stunnel –Servidor

El servidor de bases de datos de la SEP, contaba con el sistema operativo Red Hat Enterprise Linux por lo que la versión del software stunnel fue mayor a la versión 4. La configuración realizada se muestra continuación.

```
cert=/etc/certs/stunnel.pem
```

chroot=/var/lib/stunnel
pid=/run/stunnel.pid
setuid=stunnel
setguid=stunnel
client=no
output=stunnel.log

[dbConecction]
accept=SECURE_PG_PORT
Connect= IP_SERVIDOR_BD:LOCAL_PG_PORT
Inicio del servicio:
stunnel /etc/stunnel/stunnel.conf

Verificación de stunnel funcionando:
netstat -ln

Ejecución de stunnel al inicio del sistema:
echo "stunnel /etc/stunnel/stunnel.conf" >> /etc/rc.local

Figura 8. Configuración de Stunnel-Servidor

3.4.3.3 Implementación en el proceso de registro

Durante el registro de aspirantes no se ejecuto la replicación de base de datos entre el centro de registro 01 y el servidor de base de datos de la SEP. Únicamente se crearon respaldos diarios de los registros de cada usuario a través de la transferencia de archivos vía ssh, o la entrega de estos respaldos al personal autorizado por COMIPEMS.

3.5 Cortafuegos (Firewall)

Un cortafuego (firewall) es un recurso de hardware o software utilizado en una red de computadoras, con el objetivo de controlar las comunicaciones, permitiendo o prohibiéndolas de acuerdo a las políticas definidas.

3.5.1 Análisis

Normalmente la ubicación de unos cortafuegos se encuentra en el punto de unión entre la red interna de la organización y la red externa, por lo que la red interna es protegida contra los accesos no autorizados, que puedan explotar vulnerabilidades de los sistemas internos.

Políticas de Cortafuegos.- Existen dos Políticas en la implementación de unos cortafuegos, las cuales definen la postura que tiene la seguridad de la red ante las comunicaciones entre la red interna y externa, estas políticas son:

- Restrictiva. Todo tráfico es denegado, por excepción del que se declara explícitamente.
- Permisiva. Todo tráfico es permitido, excepto el que explícitamente se niegue.

Ventajas

- Protege de intrusiones.
- Protección de información privada.
- Optimización de acceso.

Limitaciones

- No puede protegerse contra ataques que se encuentran fuera de su área de operación
- No puede protegerse de amenazas efectuadas por intrusos.
- No puede protegerse de ataques de Ingeniería Social.
- No es posible protegerse contra posibles ataques de la red interna como virus.
- No protege contra las vulnerabilidades de los servicios y protocolos para los que sea permitido el tráfico.

3.5.2 Clasificación

Existen tres principales tecnologías de firewall:

- Filtrado de paquetes (primera generación).-Se basa en permitir o denegar el tráfico basado en el encabezado de cada paquete. Como no guarda los estados de una conexión, es decir no tiene el concepto de una sesión.
- Filtrado por estado (Stateful Application inspection).- Permite abrir "Puertas" a cierto tipo de tráfico basado en una conexión y volver a cerrar la puerta cuando la conexión termina. Mantiene un registro de las conexiones, las sesiones y su contexto.
- Full application inspection (Application Gateway). - Es capaz de inspeccionar hasta el nivel de aplicación. No solo la validez de la conexión sino todo el contenido de la trama. Es considerado como el más seguro. Todas las conexiones van a través del firewall. Además no permite conexiones directas y soporta autenticación a nivel de usuario. Sin embargo, son más lentos por lo tanto se requiere mas cantidad de hardware para analizar el tráfico del canal.

3.5.3 Configuración

3.5.3.1 IPCHAINS

Linux *ipchains* es una modificación de la codificación de Linux IPv4 firewalling. Es necesaria para la administración de filtros de paquetes de IP en las versiones 2.1.102 de Linux o posteriores. Actualmente ipchains fue reemplazado por iptables desde la versión del kernel de Linux 2.4.
Las limitaciones del software son:

- No realiza transacciones con fragmentos, tiene contadores de 32-bit.
- No permite especificación de protocolos más que TCP, UDP o ICMP.
- No puede hacer grandes cambios atómicamente.
- No puede especificar reglas inversas.

Funcionamiento

Ipchains se basa en una lista (cadena) de reglas que determinan el comportamiento y las decisiones a tomar sobre paquetes cuando alcanzan un interfaz de entrada o salida. Inicialmente siempre hay cadenas de reglas que son las básicas y sobre las que se construye todo lo demás. Estas son:
- Entrada (Input).
- Salida (Output).
- Envío (Forward).

Con ellas hacemos respectivamente alusión a los paquetes que entran, a los que salen, y a los que se enrutan. Aparte de estas tres cadenas básicas se pueden definir otras por el usuario.

Cuando un paquete entra (al dispositivo de red) el kernel usa la cadena input para decidir su destino. Si sobrevive este paso, entonces el kernel decide dónde enviar el paquete. Si el destino es otra máquina, consulta la cadena Forward. Finalmente, justo antes de que el paquete salga, el kernel consulta la cadena output.

Una cadena es una lista de reglas. Cada regla dice 'si el encabezado del paquete se ve como esto, entonces esto es lo que deseo hacer con el paquete'. Si la regla no empareja con el paquete, entonces se consulta la próxima regla en la cadena. Finalmente, si no hay ninguna regla más por consultar, entonces el kernel consulta la política de la cadena para decidir qué hacer. En un sistema de seguridad-consciente, esta política normalmente le dice al kernel que rechace o deniegue el paquete.

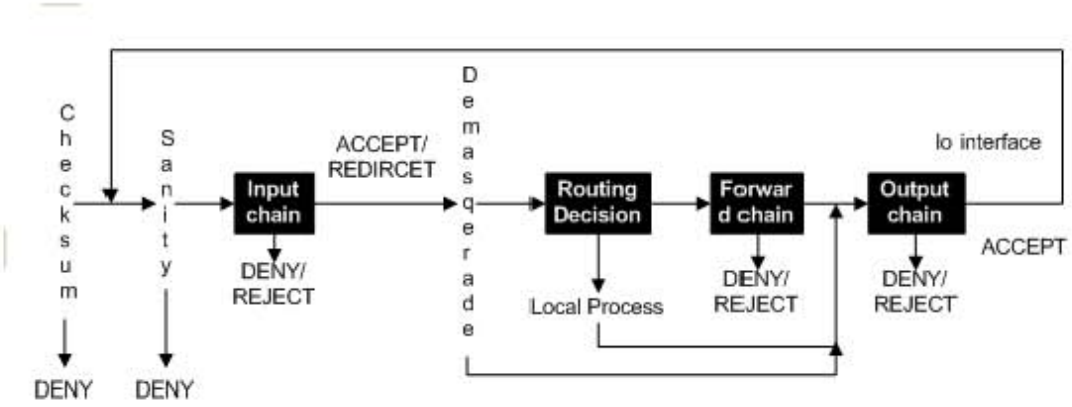

Figura 9. Diagrama de flujo de ipchains.

Los comandos para manipular las listas de reglas son (siempre en mayúsculas):

- N: Crea una nueva cadena de reglas.
- X: Borra una cadena de reglas que antes debe estar vacía.
- P: Cambia la política de la cadena de reglas. Esta puede ser ACCEPT, DENY, REJECT y MASQ (ésta solo valida en forward).
- L: Lista las reglas de la cadena de reglas.
- F: Borra todas las reglas.
- Z: Pone a cero todos los contadores de bytes en todas las reglas de la lista.

Los comandos para manipular las reglas que están dentro de la cadena:

- A: Añade una nueva regla a la cadena (la añade al final).
- I: Inserta una regla en una posición indicada.
- R: Reemplaza una regla.
- D: Borra una regla.

Las reglas suelen seguir la sintaxis*: ipchains -(ADIR) opciones -j (salto) , done:*

- salto: Si el paquete coincide con la susodicha regla se saltará a donde indique -j que puede ser aceptar, denegar, rechazar u otra cadena definida por el usuario. De todas formas no es imprescindible el -j.
- opciones:
    - -s (origen) y -d (destino) dirección IP, puede expresarse de las siguientes formas: dirección_IP, nombre_host, dirección_IP/bits_significativos.
    - -p especifica el protocolo. El protocolo puede ser el valor numérico del protocolo IP o un nombre para los casos especiales de `TCP ', `UDP ' o `ICMP '.
    - puerto o rango_puertos. El puerto o rango de puertos se especifica después de las opciones s y/o d dejando con un espacio en blanco. El puerto es posible especificarlo usando el nombre y el rango se hace como puerto_inicial:puerto_final.
    - -i especifica el interfaz por el que entra el paquete (en input) o sale (en output y forward). Se pueden especificar interfaces inexistentes. Se permite el uso del comodín ``+" para designar un conjunto de interfaces.
    - -y referencia a los paquetes SYN que son los que se usan para iniciar una conexión. Con ! se hace referencia a los que no son para iniciar una conexión.
    - -f la regla solo se aplicará al segundo y demás fragmentos de un paquete, no se permite especificar puertos.
    - -j especifica el objetivo de la regla que puede ser: ACCEPT, REJECT y DENY (deniegan), MASQ (aplica masquerade a un paquete, solo válida en forward), REDIRECT (redirecciona a otro puerto o máquina, RETURN (aplica la política por defecto). Se puede especificar otra cadena de reglas definidas por el usuario con lo que se aplicarán las reglas de esa cadena y luego se volverá al original. Si no se especifica -j, la regla solo realizará una actualización de la cuenta, esto es, se pueden contar el número de paquetes que cumplen la regla sin tomar acción sobre ellos (también se cuentan cuando se usa -j).
    - l si un paquete coincide con la regla se registra en el syslog.
    - -v en conjunción con -L aumenta la información ofrecida.

3.5.3.2 Netfilter/Iptables

Netfilter es un conjunto de herramientas que se incluyen en el núcleo de Linux que interceptan y manipulan los paquetes de red, además son utilizadas también por el componente que realiza traducción de direcciones de red (Network Address Transaltion, NAT) y por cualquier otro componente que provee compatibilidad hacia tras con ipchains. Iptables es la herramienta del espacio de usuario con la que el administrador crea las reglas para el filtrado de paquetes y realizar NAT. Mientras ipchains e ipfwadm combina el filtrado de paquetes y NAT, Netfilter separa la operación de los paquetes en tres partes:

- Filtrado de paquetes (packet filtering)
- Seguimiento de conexiones (Connection Tracking)
- Traducción de direcciones de red (Network Address Transaltion, NAT)

Funcionamiento

El administrador del sistema define las acciones que se realizarán con los paquetes de red a través de la indefinición de reglas, que el framework de netfilter permite crear. Las cadenas se agrupan en tablas, donde cada tabla esta asociada con un tipo diferente de procesamiento de paquetes. Cada cadena contiene una lista de reglas, es decir, en iptables las reglas se agrupan en cadenas. Cada regla detalla que paquetes la cumplen y el destino que indica que acción se tomara con los paquetes que la cumplen. Todo paquete en la red recorre por lo menos una cadena y cada regla de dicha cadena es examinada para comprobar si cumple el paquete su definición:

- Si el datagrama cumple con la definición de la regla, el recorrido se detiene y se aplica la acción al paquete, dictada por el destino e la regla.
- Si el paquete alcanza el fin de la cadena predefinida sin haber cumplido la definición de una regla, la política de destino de la cadena dicta que acción se tomara para el paquete.
- Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido con alguna regla, o si esta cadena del usuario esta vacía, el recorrido continúa con la cadena que hizo la llamada, lo que es conocido como RETORNO DE DESTINO IMPLICITO (implicit target RETURN).

Tablas

Existen tres tablas ya incorporadas, que contiene cadenas predefinidas. Es posible crear y eliminar cadenas. Por omisión, al inicio todas las cadenas están vacías, además de tener una política de destino permisiva. Las tablas son las siguientes:

Tabla de Filtros (filter table). Todo paquete pasa por la tabla de Filtros, que se encarga de bloquear o permitir el paso de estos paquetes.

Tabla de Traducción de Direcciones de Red (NAT Table). Responsable de configurar la reglas de modificación de direcciones y/o puertos de los paquetes. En toda conexión el primer paquete pasa a través de esta tabla, donde se determina como se modificaron todos los paquetes de dicha conexión

Tabla de Destrozo (mangle table). Cualquier paquete pasará por esta, que es responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad de servicio. Esta tabla esta diseñada para acciones avanzadas, por lo que contiene todas las cadenas predefinidas.

Destinos de las Reglas

El destino de una regla puede ser el nombre de una cadena definida por el usuario o uno de los definidos por iptables, que son ACCEPT, DROP, QUEUE, RETURN, REJECT, LOG, ULOG, DNAT, SNAT o MASQUERADE. Cuando este destino es el nombre de una cadena definida por el usuario, el paquete se dirige a esa cadena para ser analizado. Si el paquete no aplica para ninguna de las reglas de la cadena definida por el usuario, el procesamiento del paquete

continua a partir del punto de llamada de la cadena del usuario. Este llamado de cadenas no tiene algún límite de anidado.

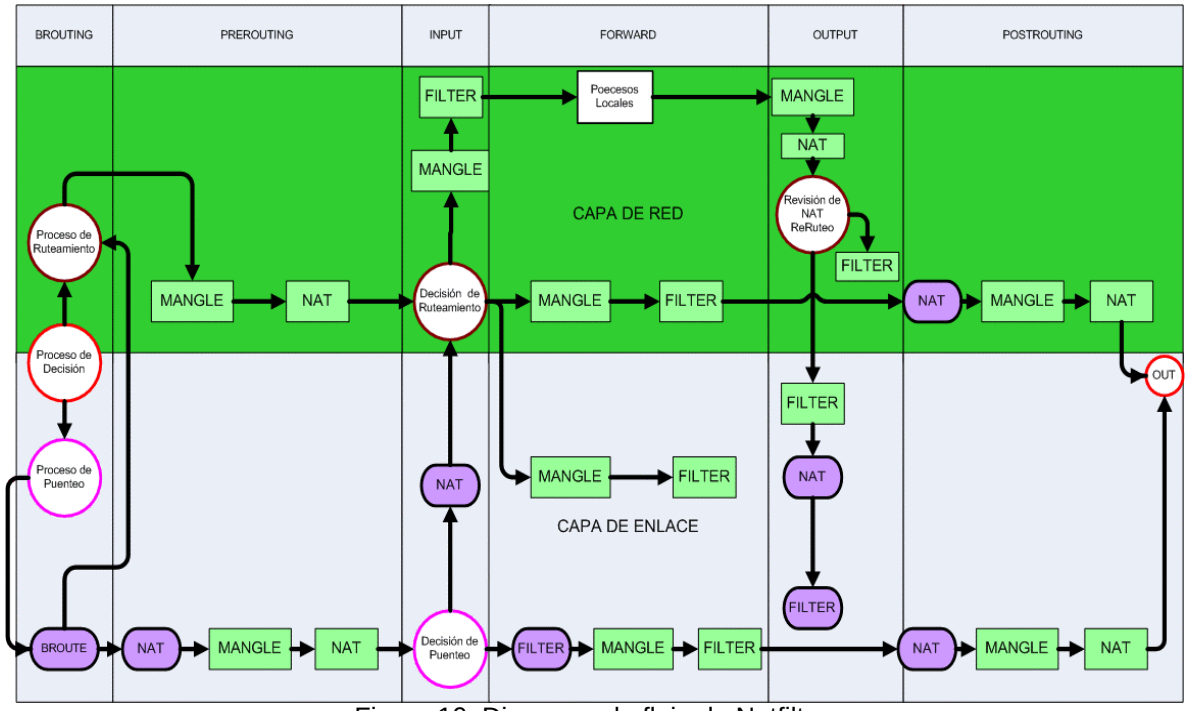

Figura 10. Diagrama de flujo de Netfilter.

Seguimiento de Conexiones

El seguimiento de conexiones (connection tracking) le permite al núcleo llevar una estadística de todas las conexiones o sesiones lógicas de red y de este modo relacionar todos los paquetes que pueden llegar a formar parte de esa conexión. La traducción de dirección de red (NAT) depende de esta información para traducir todos los paquetes relacionados de la misma manera, además que iptables puede utilizar esta información para actuar como unos cortafuegos stateful. El seguimiento de conexiones clasifica cada paquete en uno de los siguientes estados:

- NEW. Intentando crear una conexión nueva.
- ESTABLISHED. Fragmento de una conexión ya existente.
- RELATED. Relacionada, pero no comienza de una conexión existente.
- INVALID. No es fragmento de una conexión existen e es incapaz de crear una conexión nueva.

Iptables

Iptables es la herramienta que le permite al administrador del sistema configurar las tablas, cadenas y reglas de netfilter, y solo puede ser ejecutado por el superusuario. La sintaxis detallada del comando esta documentada en su página de manual.

iptables { -A | --append | -D | --delete } *cadena especificación-de-regla* [*opciones*]
Agrega o elimina una regla de la cadena especificada.
iptables { -R | --replace | -I | --insert } *cadena numregla especificación-de-regla* [*opciones*]
Reemplaza una regla existente o inserta una regla nueva en la cadena especificada.
iptables { -D | --delete } *cadena numregla* [*opciones*]
Elimina una regla del índice numérico especificado en la cadena especificada.
iptables { -L | --list | -F | --flush | -Z | --zero } [*cadena*] [*opciones*]
Lista las reglas en una cadena, Tira (elimina) todas las reglas de una cadena, o Pone en cero el byte y los contadores de paquetes de una cadena.
iptables { -N | --new-chain } *cadena* iptables { -X | --delete-chain } [*cadena*]

Crea una cadena definida por el usuario o elimina una cadena existente definida por el usuario.
iptables { -P | --policy } *cadena destino*
Especifica la política de destino para una cadena.
iptables { -E | --rename-chain } *nombre-de-cadena-viejo nombre-de-cadena-nuevo*
Renombra una cadena definida por el usuario.

Tabla 15. Sintaxis utilizada para Iptables.

-t tabla	El comando se aplique a la *tabla* especificada.
-v	Produce una salida con detalles
-n	Produce una salida numérica
--line-numbers	Se agrega números (posición en la cadena) de línea al comienzo de cada regla.
-j *destino*	Especifica el destino de una regla.
-i [!] *in-interface*	Nombre de una interfaz a través de la cual un paquete va a ser recibido.
-o [!] *out-interface*	Nombre de una interfaz a través de la cual un paquete va a ser enviado.
-p [!] *protocoló*	*Matchea* paquetes del nombre de protocolo especificado.
-s [!] *origen*[/*prefijo*]	*Matchea* paquetes IP viniendo de la dirección de origen especificada.
-d [!] *destino*[/*prefijo*]	*Matchea* paquetes IP yendo a la dirección de destino especificada.
--dport [!] [*puerto*[[:*puerto*]]	*Matchea* paquetes TCP o UDP destinados a los puertos o rango de puertos.
--sport [!] [*puerto*[[:*puerto*]]	*Matchea* paquetes TCP o UDP que vienen de los puertos o rango de puertos.
--tcp-flags [!] *mask comp*	*Matchea* paquetes TCP que tienen marcadas o desmarcadas ciertas banderas del protocolo TCP.
[!] --syn	*Matchea* paquetes TCP que tienen la bandera SYN marcada y las banderas ACK, FIN y RST desmarcadas.

Tabla 16. Opciones más comunes para Iptables.

3.5.3.3 Firewall-Puerta de Enlace (Gateway)

La arquitectura de red que se implemento en los diferentes centros de registro puede generalizarse como se observa en el figura 4, sin embargo en este apartado nos interesa describir la estructura ofrecida para la salida a Internet y su configuración, ya que fue un punto importante para los procesos involucrados como la replicación de datos y la administración de aforos, así como para la administración remota. En la figura 11, se muestra la arquitectura de red para la salida de Internet que desarrollada en años anteriores, por lo que el trabajo consistió en entender la configuración que se tenia, analizar y actualizar o bien migrar el firewall a un sistema Red Hat Enterprise Linux.

La figura 11 muestra que el punto de unión entre las dos redes: Internet y la red local, a través un módem ADSL proporcionado por el proveedor del servicio de Internet, que proporcionó el servicio de Internet a una maquina que funciona como firewall y para controlar el trafico entre ambas redes.

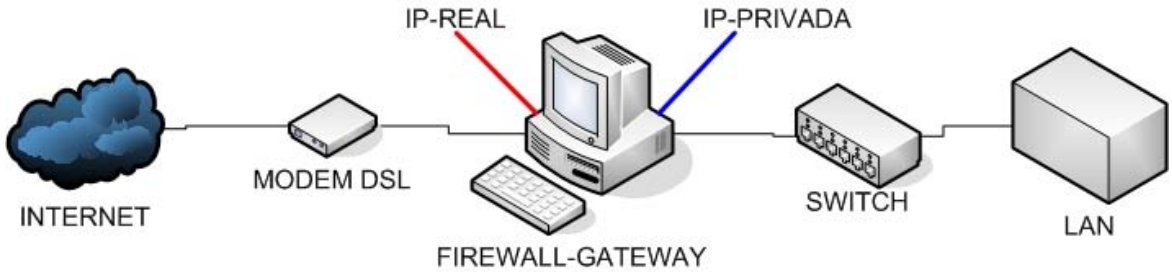

Figura 11. Puerta de Enlace en los centros de registro.

Instalación y configuración del Firewall

Para la instalación y configuración del sistema que funciona como firewall se realizaron los siguientes pasos, que se describirán mas adelante.

- Instalación del sistema operativo.
- Configuración de las interfaces de red.
- Configuración de la tabla de ruteo.
- Habilitar ip-fowarding.
- Creación del script de configuración del firewall.
- Automatización de la configuración del firewall.

Instalación del sistema operativo

Se instalo el sistema operativo Red Hat Enterprise Linux, donde se siguieron los pasos descritos anteriormente para la instalación de los servidores, con la diferencia que en la selección de los paquetes, se selecciono la opción de software mínimo, evitando así la instalación de cualquier otro software incensario, los cuales consumen mas recursos del sistema.

Configuración de las interfaces de red

La configuración se realizó mediante la modificación de sus correspondientes archivos ubicados en la ruta /etc/sysconfig/network-scripts, cada uno de estos archivos de configuración controlan la operación de un dispositivo de interfaz de red particular. Estos archivos habitualmente se conocen como ifcfg-<device>, donde <device> hace referencia al nombre del dispositivo que controla el fichero de configuración.

Para configuración del firewall una tarjeta de red se conectó a la red local del centro de registro mientras otra tarjeta de red hacia la acometida del módem ADSL. La primera tarjeta de red (eth0) se configuró con una IP de la red local del centro de registro y la segunda tarjeta de red (eth1) con la IP provista por el ISP, como se muestra en la tabla 17. Teniendo de esta forma que cualquier equipo que necesitará tener salida a Internet, deberá pasar a través del firewall.

/etc/sysconfig/network-scripts/ifcfg-eth0	/etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth0 IPADDR=192.168.1.1 NETMASK=255.255.255.0 BROADCAST=192.168.1.255 GATEWAY=192.168.1.1 ONBOOT=yes	DEVICE=eth0 IPADDR=132.248.63.205 NETMASK=255.255.255.0 BROADCAST=132.248.63.255 GATEWAY=132.248.63.1 ONBOOT=yes

Tabla 17. Configuración de las tarjetas de red para el firewall

Configuración de la tabla de ruteo.

Una puerta de enlace (gateway) es normalmente un equipo configurado para dotar a las máquinas de una red local conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT), la cual le permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP).

Para ello, las máquinas de la red deben tener una tabla de ruteo donde indiquen a quién dirigirse para enviar paquetes a cierta red. En Linux, esta tabla de ruteo se integra en el kernel y se administra con la utilidad route. La tabla está compuesta por una serie de reglas que se revisan por orden. Con estas reglas podemos especificar que camino o ruta seguir para mandar un paquete a cierto host o a cierta red. Se pueden hacer algunas tareas de registro y seguridad usando tablas de ruteo, pero su utilidad principal será enlazar nuestras sub-redes.

En caso de que no exista alguna de estas entradas o sea necesario borrar, se realiza con el comando:

 # route {add|del} -net [red] netmask [mascara de red] gw [gateway] dev [dispositivo]

Tabla de ruteo del firewall. Esta sirve para decidir cuándo el tráfico de red esta dirigido hacia la LAN y cuando estaba dirigido hacia Internet. Para ver los valores actuales de la tabla de ruteo, hay que utilizar el comando:

 # route –n

Kernel routing table

Destination	Gateway	GenMask	Flags	Mss Window	Use	Iface
23.42.2.0	*	255.255.255.0	U	15000	15	eth0
192.168.1.0	*	255.255.255.0	U	15000	15	eth1
127.0.0.1	*	255.0.0.0	U	15000	2	lo
default	*	*	UG	15000	72	eth0

De tal forma que los paquetes, con destino a la red 23.42.2.0/255.255.255.0 son destinos que se envían por la interfaz eth0. Los paquetes con destino a la red 192.168.1.0/255.255.255.0 (es decir las maquinas que tengan dirección IP en el rango 192.168.1.0 a 192.192.168.1.254) son destinos locales que se envían por la interfaz eth1. Los paquetes con destino para la dirección 127.0.0.1 son para la maquina local que son manejados por la interfaz local (lo). Finalmente los paquetes que cuyo destino no sea clasificado dentro de las reglas anteriores/o conocido por defecto serán enviados al Gateway, el cual se indica por la bandera G en la columna Flags. En este caso podemos observa que no existe una entrada para el gateway por defecto por lo que es posible agregar una puerta de enlace por defecto con el siguiente comando:

#route add deafult gw <ip>

Habilitar ip_forwarding

Consistió en habilitar la capacidad de reenvío (forwarding) de paquetes TCP/IP en la configuración de red. Específicamente en el archivo /proc/sys/net/ipv4/ip_forward al dar el valor de 1 a la variable del sistema net.ipv4.ip_forwarding, cuyo valor es almacenado en dicho archivo:

 # echo 1 > /proc/sys/net/ipv4/ip_forward

O bien, a través del archivo /etc/sysctl.conf modificando la variable net.ipv4.ip_forwarding de valor 0 a 1:

net.ipv4.ip_forward = 1

Una vez realizado este cambio, fue necesario reiniciar el servicio de red y comprobar que se realizados los cambios con lo siguientes comandos:

 # service network restart
 # cat /proc/sys/net/ipv4/ip_forward (cuya salida deberá ser 1)

Configuración de un cliente para trabajar con la puerta de enlace (gateway)

Para los clientes Windows fue necesario acceder a las propiedades de la interfaz de red a través del panel de control, mientras que para los clientes Linux, bastó con especificar la dirección IP de la interfaz interna del gateway en el parámetro GATEWAY de los archivos de configuración según la distribución de Linux que se utilice.

3.5.4 Implementación

3.5.4.1 Firewall Centro 01

Cuando se comenzó el proyecto se tenía el firewall del centro de registro 01 con el sistema operativo Red Hat y con la herramienta ipchains. Este sistema se dejo intacto y solo se tomo como referencia para realizar una actualización de este esquema para los otros centros de registro, para los cuales se cambió por el sistema Red Hat Enterprise Linux y por lo tanto iptables, lo cual se detallara mas adelante.

Análisis de la configuración del firewall con ipchains del centro de registro 01

A continuación se describe el proceso de la creación del firewall a través de la declaración de reglas con la ayuda de ipchains, para analizar cada una de las reglas que contiene el script se ha separado por secciones y funcionalidad, no sin antes mencionar que antes de la declaración de las reglas existe un conjunto de declaraciones de variables, cuyo fin fue agilizar la actualización y el entendimiento de las reglas a través de palabras y no de números.

- Acceso al servicio SSH del firewall para direcciones IP determinadas. Este conjunto de reglas permitieron el uso de conexiones ssh hacia al firewall, pero solo para ciertas direcciones IP que definen en la variable TRUSTED_IPS.

  ipchains -A input -p tcp -s 0.0.0.0/0 22 -d $INTERNET_IP -j ACCEPT
  for i in $TRUSTED_IPS
  do
  ipchains -A input -p tcp -s $i -d $INTERNET_IP $LOCAL_SSH_PORT -j ACCEPT
  done

- Salida a Internet para direcciones IP determinadas. Con este conjunto de reglas se otorgó acceso a Internet para ciertas IP definidas en la variable INTERNET_OUT_IPS para realizar cualquier conexión hacia Internet, para los protocolos TCP y UDP a través del ENMASCARAMIENTO.

  for i in $INTERNET_OUT_IPS
  do
  ipchains -A forward -p tcp -s $i -d 0.0.0.0/0 -j MASQ
  ipchains -A input -p all -s $i -d 0.0.0.0/0 -j ACCEPT
  ipchains -A input -p tcp -s 0.0.0.0/0 -d $i -j ACCEPT
  ipchains -A forward -p udp -s $i -d 0.0.0.0/0 -j MASQ
  done

- Acceso a los servicios SSH y POSTGRESQL del servidor interno del centro desde el firewall. Estas reglas permitieron realizar conexiones tcp desde el firewall a los puertos de los servicios SSH y POSTGRESQL del servidor interno del centro de registro.

  ipchains -A input -p tcp -s $SERVER_01 -d $LAN_IP $LOCAL_SSH_PORT -j ACCEPT
  ipchains -A input -p tcp -s $SERVER_01 -d $LAN_IP $LOCAL_SSH_PORT -j ACCEPT

- Conexiones a los servicios POSTGRESQL(seguro), HTTP y SSH del servidor interno hacia servidor de la SEP. Estas reglas permitieron realizar conexiones desde la interfaz Interna del firewall para servicios POSTGRESQL, HTTP y SSH hacia los servidores de aplicación y base de datos de la SEP.

  ipchains -A input -p tcp -s $REMOTE_HTTP_CLIENT -d $INTERNET_IP $SEP_HTTP_PORT -j ACCEPT
  ipchains -A input -p tcp -s $LAN_IP -d $LOCAL_HTTP_SERVER $LOCAL_HTTP_PORT -j ACCEPT
  ipchains -A forward -p tcp -s $SERVER_01 -d $SERVER_PG_SEP $SECURE_PG_PORT -j MASQ
  ipchains -A input -p tcp -s $SERVER_PG_SEP $SECURE_PG_PORT -d $INTERNET_IP -j ACCEPT
  ipchains -A forward -p tcp -s $SERVER_01 -d $SERVER_PG_SEP 22 -j MASQ
  ipchains -A input -p tcp -s $SERVER_PG_SEP 22 -d $INTERNET_IP -j ACCEPT

- Conexión segura de POSTGRESQL y SSH del servidor del centro de registro al servidor de base de datos de la SEP. Estas reglas permitieron las conexiones entre lo servidores con el objetivo de que se realizarán las conexiones necesarias para la replicación y consulta de la Base de Datos, así como para la administración remota a través del servicio SSH.

ipchains -A forward -p tcp -s $SERVER_01 -d $SERVER_PG_SEP $SECURE_PG_PORT -j MASQ
ipchains -A input -p tcp -s $SERVER_PG_SEP $SECURE_PG_PORT -d $INTERNET_IP -j ACCEPT
ipchains -A forward -p tcp -s $SERVER_01 -d $SERVER_PG_SEP 22 -j MASQ
ipchains -A input -p tcp -s $SERVER_PG_SEP 22 -d $INTERNET_IP -j ACCEPT

- Conexión de la Mesa de Control hacia el servidor de aplicación (Web) de la SEP. Estas reglas habilitaron las conexiones entre la mesa de control ubicada en el centro de registro y el servidor de la SEP, únicamente para el servicio Web, por lo que la mesa de control solo puede acceder a la pagina Web del servidor central.

  ipchains -A forward -p tcp -s $PC_01 -d $SERVER_HTTP_SEP $SEP_HTTP_PORT -j MASQ
  ipchains -A input -p tcp -s $SERVER_HTTP_SEP $SEP_HTTP_PORT -d $INTERNET_IP -j ACCEPT

Eliminar todas las conexiones restantes. Todas las conexiones que no coincidieron con ningunas de las reglas anteriores fueron rechazadas.

ipchains -A input -l -s 0.0.0.0/0 -d $INTERNET_IP -j REJECT

3.5.4.2 Firewall Iptables para el centro de registro

Una vez se realizó la investigación, se actualizo el script para la configuración del firewall de ipchains a iptables, conservando el mismo orden de declaración de reglas con algunas mejoras y observaciones como se describe a continuación. Además se realizo un esquema (ver figura 12) del firewall, en especial del firewall del centro de registro 01, el cual se replico a los centros e registro facilitando la implementación del firewall.

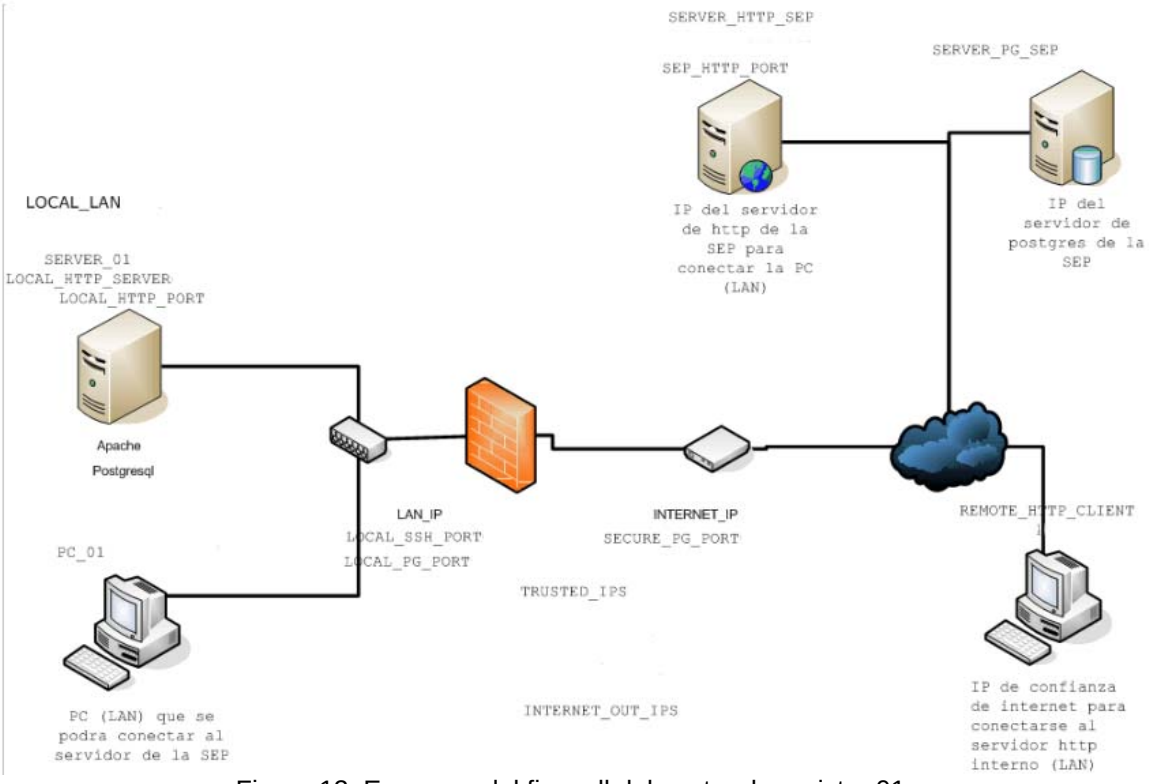

Figura 12. Esquema del firewall del centro de registro 01.

En resumen el funcionamiento y el orden de declaración de las reglas es el mismo que se muestra en el firewall implementado con ipchains, aunque se llevaron a cabo algunas mejoras técnicas, corrigieron algunos errores, como por ejemplo:

- El acceso a la interfaz externa del firewall a través de ssh no estaba restringido únicamente a las IP's establecidas en la variable TRUSTED_IPS, ya que en el script que se tenia de ipchains se tenia una regla que antecedía al ciclo for que permitía el acceso a cualquier IP a través del servicio SSH.

  ```
  for i in $TRUSTED_IPS
  do
    iptables -A INPUT -p tcp -s $i -d $INTERNET_IP --dport $LOCAL_SSH_PORT -j ACCEPT
  done
  iptables -A INPUT -p tcp -s 0.0.0.0/0 -d $INTERNET_IP --dport $LOCAL_SSH_PORT -j DROP
  ```

- Una vez que se permitían las conexiones para cierto tipo de servicio, inmediatamente se negaban aquellas reglas que no cumplían dichas reglas con el fin de evitar acceso no autorizados, como se muestra a continuación:

  ```
  iptables -A INPUT -p tcp -s $SERVER_01 -d $LAN_IP --dport $LOCAL_PG_PORT -j ACCEPT
  iptables -A INPUT -p tcp -s 0.0.0.0/0 -d $LAN_IP --dport $LOCAL_PG_PORT -j DROP
  ```

- Se habilito el uso de bitácoras, lo cual facilitó la posibilidad de conocer a mayor detalle el funcionamiento del firewall, así como las conexiones entrantes y salientes que se realizan a través del firewall.

  ```
  iptables -A FORWARD -j LOG --log-level info
  ```

3.5.4.3 Automatización de la configuración

Debido a que fue necesario repetir la instalación y la configuración del firewall en diferentes centros de registro, se realizo un script que interactuara con el administrador y que a través de preguntas concretas obteniendo la información necesaria para configurar el firewall.

A continuación se muestra el proceso que realizó el script en bash que permitió:

- Eliminar servicios innecesarios a través del comando chkconfig, por ejemplo:

  chkconfig --level 0123456 cups off

- Obtener información como la dirección IP pública, puerta de enlace de la dirección IP homologada, dirección IP de local y dirección IP de la LAN, a través de preguntas en el shell que almacenaban las direcciones IP en variables, por ejemplo:

  ```
  echo -n " ¿Cual es la IP de la Red LOCAL (IP LAN) ?  "
  read LOCAL_LAN
  ```

- Configuración de las tarjetas de red, al editar los archivos de configuración /etc/sysconfig/network-scripts/ifcfg-eth0 y /etc/sysconfig/network-scripts/ifcfg-eth1, con la información proporcionada anteriormente, por ejemplo:

  ```
  echo "DEVICE=eth1" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "BOOTPROTO=static" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "IPADDR=$LAN_IP" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "NETMASK=255.255.255.0" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "NETWORK=$LOCAL_LAN" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "BROADCAST=$BROADCAST" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "GATEWAY=$LAN_IP" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  echo "ONBOOT=yes" >> /etc/sysconfig/network-scripts/ifcfg-eth1
  ```

- Reinicio del servicio de red con el objetivo de actualizar la configuración de las tarjetas de red y probar la salida a Internet.

- Obtener la información necesaria para la configuración del firewall, de igual forma como se obtuvo la información para la configuración de las tarjetas de red, en esta sección se obtiene la información como direcciones IP de la SEP, puerto local de Postgres, etc, por ejemplo:

  echo -n " ¿Cual es el Puerto de Postgres por el que escucha la Interfaz Externa del Firewall?"
  read SECURE_PG_PORT

- Creación del script del cortafuegos “cortafuegos.sh” al vaciar la información recaba en el archivo, así como agregar este script al scritp rc.local del sistema con el fin de que este se ejecute siempre que el sistema se inicie, por ejemplo:

  echo "# IP para la interfaz de red del firewall que tendrá salida a Internet." >> /root/firewall.sh
  echo "INTERNET_IP=$INTERNET_IP" >> /root/firewall.sh
  cat "sh /root/firewall.sh" >> /etc/rc.local

- Configuración de stunnel en modo cliente y la verificación de la disponibilidad de este servicio, con algunos comandos como:

  stunnel /etc/stunnel/stunnel.conf
  ps -fea | grep stunnel | grep -v grep
  netstat -ln | grep $SECURE_PG_PORT

3.6 Capacitación y Soporte

Una vez que se implemento la solución especificada en cada uno de los centros de registro, forme parte del equipo de personas que capacito a un grupo de personas para dar soporte en cada uno de los centros de registro, los temas principales de esta capacitación en los que participé fueron:

- Instalación y configuración del sistema operativo
- Manejo y reporte de incidentes durante el proceso de registro.
- Conexiones seguras con Stunnel.

Así como también forme parte del grupo que dio soporte durante los procesos de pre-registro presencial y registro, en el centro de registro 01, donde se tenían días con hasta 8000 aspirantes.

7 Resultados y aportaciones

Administración de los servidores

Este proyecto se basó en el mantenimiento y la mejora técnica de la infraestructura existente en la SEP y en el Centro de Registro 01, por tanto no fue necesario involucrarme en las fases tempranas (Inicio, Planeación y Análisis), ya que me incorporé en donde tuve que asimilar los conocimientos de muchos de los procedimientos y procesos sobre el funcionamiento de la aplicación, los cuales ya habían sido definidos. Algunos inconvenientes que se presentaron fue la documentación de dichos procedimientos, además el personal involucrado de otras versiones del proyecto que había desarrollado e implementado dicha solución, ya no se encontraba laborando en la Dirección de Sistemas.

La asimilación de estos conocimientos, me permitió definir los puntos de mejora y las posibles actualizaciones, para posteriormente definir con los requerimientos de Software y hardware, considerando que los tiempos planeados para dicha fase de diseño tenía poca holgura, ya que los calendarios de inicio del proceso de registro habían sido publicados por la SEP.

Una vez definidos los lineamientos de trabajo, participe en la impartición de cursos y formación de recursos humanos para la capacitación del personal de apoyo que se distribuiría en cada unos de los 37 centros de registro. La capacitación se dividió en dos diferentes rubros: Instalación y configuración del sistema operativo, Manejo y reporte de incidentes durante el proceso de registro y Conexiones seguras con Stunnel.

Dentro de la fase de implementación estuve encargado de:

Instalación, configuración, actualización y automatización del firewall.

Una vez analizado el funcionamiento del firewall implementado en el centro de registro 01, tuve que instalar el sistema operativo con una nueva versión, así como el cambio del software encargado del filtrado de los paquetes de red: NetFilter. Posteriormente programé un script el cual permitiría automatizar la configuración del firewall, ya que sería necesario agilizar esta tarea que se llevaría a cabo en cada uno de los centros de registro.

Automatización del enlace de conexión por medio de Stunnel

Para lograr la automatización del enlace de conexión por medio de una VPN se utilizó el stunnel, lo cual involucró manejar dos tipos de versiones dado las limitaciones de tiempo. Además una de las ventajas que nos ofrece este software fue proteger de forma cifrada los datos que se enviaban al Servidor Central de la SEP. Una de las mejoras que podría realizarse a dicho proceso, sin embargo no se realizo por cuestiones de tiempo, es que en el esquema de replicación de información la información viaja cifrada, gracias al software Stunnel, pero la maquina stunnel en modo cliente podría autenticar el certificado, de tal forma que se asegure que la comunicación sea entre las partes concordadas y de esta manera evitar problemas de seguridad como spoofing.

Instalación, Configuración, Aseguramiento de los servidores

En la fase de post implementación, mi trabajo consistió en la administración de los recursos y servicios ofrecidos por los servidores involucrados en los proceso de pre-registro y registro, cuidando, previniendo y solucionando los problemas que se presentaban en dichos procesos, particularmente fui asignado al centro de registro 01 la mayor parte del tiempo, donde la asistencia de aspirantes era mayor 2000 aspirantes por día, aproximadamente; así como al monitoreo de los servidores del centro de computo de SEP algunos días.

Además de eso, si se presentaba algún error inesperado dentro de la aplicación tenía ayudar a rastrear el error junto con el departamento de desarrollo para su inmediata corrección.

Una de mis aportaciones como miembro del departamento de Servidores fue la generación de registros y bitácoras sobre cada una de las actividades que realice, como parte de la documentación generada por este proyecto, como un futuro apoyo en otros posibles proyectos o servicios.

8 Conclusiones

En particular el haberme involucrado en este proyecto me permitió darme cuenta de la importancia que tiene la ingeniería del Software en proyectos tan grandes como lo fue este, entendiendo cual es la importancia de la generación de la documentación desde tempranas fases de un proyecto.

La implementación de las mejoras técnicas detectadas en el proceso de Pre-registro y registro permitió que estos procesos, se realizaran sin ningún incidente relevante para la octava edición del concurso de Comipems, generando credibilidad a dicho concurso, ya que se obtuvieron evidencias.

También es importante mencionar que después de dicho proyecto he sido contratado en la Dirección de Sistemas, cuyas actividades por cuestiones de tiempo no me fue posible describir, pero he tenido la oportunidad de participar en:

- Mantenimiento, actualización y mejoramiento de la infraestructura tecnológica en el Area de administración de Servidores, dando soporte principalmente a servicios de Correo Electrónico, Web, Bases de Datos.
- Administración de servidores UNIX y Windows Server.
- Participación de proyectos externos en los que participa la Dirección de Sistemas, donde tengo el rol de Administrador de Servidores.
- También he tenido la oportunidad de participar en la impartición de cursos de la Dirección General de Servicios de Computo Académico, específicamente para cursos de Lenguajes de Programación C y Java Básico.
- Además, he participado activamente el plan de becarios de la Subdirección de Sistemas, impartiendo cursos para los becarios.

9 Bibliografía

- Dirección de sistemas, UNAM- GGSCA, Proyectos, Fecha de Consulta: 14 de abril de 2007, Disponible en: http://www.sistemas.unam.mx/proyectos.html
- COMIPEMS, Fecha de Consulta: 14 de abril de 2007, Disponible en: www.comipems.org.mx
- Michael D. Bauer, “Seguridad en Servidores Linux”, Anaya Multimedia-O'Reilly, 2005, Ed. 1, pp 185-210.
- IPTABLES Manual práctico, Fecha de consulta 23 de Marzo de 2007, Disponible en: http://www.pello.info/filez/firewall/iptables.html
- Linux IPCHAINS-COM, Fecha de Consulta: 30 de Marzo de 2007, Disponible en: http://people.netfilter.org/~rusty/ipchains/spanish/HOWTO.html.
- Netfilter/iptables, Fecha de Consulta: 30 de Marzo de 2007, Disponible en: http://es.wikipedia.org/wiki/Netfilter/iptables.
- Cortafuegos (informática), Fecha de Consulta: 30 de Marzo de 2007, Disponible en: http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29.
- Paul Russell, traducido por Herman Rodríguez, IPCHAINS, Wikipedia, Fecha de Modificación: 27 de Enero de 2007, Consulta: 24 abril 2007, disponible en: http://es.wikipedia.org/wiki/Ipchains.