ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

IMPLEMENTACIÓN DE SEGURIDADES LÓGICAS BASADO EN EL MODELO OSI, PARA LA RED DEL CYBER CAFÉ W&M SOBRE LA PLATAFORMA LINUX

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

IZA CARATE MIRYAN DORILA

Latacunga, julio del 2006

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por Iza Carate Miryan Dorila, bajo nuestra supervisión.

_____

Ing. Raúl Rosero

DIRECTOR

_____

Ing. Raúl Cajas

CODIRECTOR

AGRADECIMIENTO

Mi profundo agradecimiento y reconocimiento, por los conocimientos impartidos a quienes aportaron su sabia experiencia, de manera desinteresada e incondicional, para la culminación del presente trabajo de investigación ya que sin su ayuda no hubiese sido posible llegar a feliz término.

De manera especial no quiero dejar de reconocer su labor fecunda y próspera por el apoyo recibido de mis queridos maestros Ing. Raúl Rosero e Ing. Raúl Cajas, quienes en su destacada labor docente han formado personas y profesionales con espíritu emprendedor.

Además al Ing. Orlando Chamorro, quien me brindó sus conocimientos en el desarrollo del presente trabajo, gracias por sus conocimientos compartidos.

A mi noble Institución ESPE Sede Latacunga, en sus aulas adquirí la sapiencia impartida por tan notable cuerpo docente que de igual manera aportaron en mi formación estudiantil y profesional, infinitas gracias por haberme dado la posibilidad de formarme íntegramente como persona adquiriendo valores y virtudes humanas que solo allí pude encontrar.

DEDICATORIA

Éste trabajo lo dedico con mucho amor a mis padres, hermanos, y muy especialmente a mi esposo, quien me respaldo en momentos de dificultad y desmayo, por su apoyo siendo él la motivación para alcanzar éste objetivo como primer paso para mi vida profesional.

Y a Dios por darme la gracia y poner en mi camino a las personas ideales que son testigos de mi lucha constante por superarme, y que de ellos aprendí para proseguir en el camino de la vida.

Miryan

CONTENIDO

Pág.

CAPITULO III: REDES SEGURAS USANDO EL SISTEMA GNU/LINUX

CAPITULO IV: ANÁLISIS Y DIAGNOSTICO DE LA RED DE LA ESCUELA POLITÉCNICA DEL EJERCITO SEDE LATACUNGA.

CAPITULO V: IMPLEMENTACIÓN DE SEGURIDADES EN LA RED DE LA ESCUELA POLITÉCNICA DEL EJERCITO SEDE LATACUNGA

GRÁFICOS

Pág.

TABLAS

Pág.

CAPITULO I

SEGURIDAD LÓGICA

1.1 SEGURIDAD LÓGICA

Es importante recalcar que la mayoría de daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra la información por él almacenada y procesada. El activo más importante que posee una empresa es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la **Seguridad Lógica** consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo".

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.2 CONTROL DE ACCESO

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardas la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

1.2.1 IDENTIFICACIÓN Y AUTENTICACIÓN

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina **IDENTIFICACIÓN** al momento en que el usuario se da a conocer en el sistema; y **AUTENTICACIÓN** a la verificación que realiza el sistema sobre esta identificación.

Basándose en la seguridad física, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
2. Algo que la persona **POSEE:** por ejemplo una tarjeta magnética.

3. Algo que el individuo **ES** y que los identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. Algo que el individuo es capaz de **HACER:** por ejemplo los patrones de escritura.

Para cada una de estas técnicas cale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single log-in" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

1. Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

2. Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
3. Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoria o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
4. Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
5. Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
6. Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
7. Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando “bombas lógicas” o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

   Para evitar estas situaciones, es recomendable anular los permisos de accesos a las personas que se desvincularán de la organización, lo antes posible. En caso de despido,

el permiso de accesos debería anularse previamente a la notificación de la persona sobre la situación.

1.2.2 ROLES

El acceso a la información también puede controlarse a través de la función o rol de usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

1.2.3 TRANSACCIONES

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

1.2.4 LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

1.2.5 MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **LECTURA:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **ESCRITURA:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **BORRADO**: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **CREACIÓN:** permite al usuario crear nuevos archivos, registros o campos.
- **BÚSQUEDA:** permite listar los archivos de un directorio determinado.

1.2.6 UBICACIÓN Y HORARIO

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

1.2.7 CONTROL DE ACCESO INTERNO

1.2.7.1 PALABRAS CLAVES (PASSWORDS)

Generalmente se utilizan para realizar a autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resulta de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

- **SINCRONIZACION DE PASSWORDS:** consiste en permitir que un usuario acceda con el mismo password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario. Sin embargo, estudios hechos muestran que las personas

normalmente suelen manejar una solo password para todos los sitios a los que tenga acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

- **CADUCIDAD Y CONTROL:** este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwrods, y un período máximo que puede transcurrir para que éstos caduquen.

1.2.7.2 ENCRIPTACIÓN

La información encriptada solamente puede ser desencriptada por quienes poseen la clave apropiada. La encripatación puede proveer de una potente medida de control de acceso.

1.2.7.3 LISTAS DE CONTROL DE ACCESOS

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recursos del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

1.2.7.4 LIMITES SOBRE LA INTERFASE DE USUARIO

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase se usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

1.2.7.5 ETIQUETAS DE SEGURIDAD

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

1.2.8 CONTROL DE ACCESO EXTERNO

1.2.8.1 DISPOSITIVOS DE CONTROL DE PUERTOS

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

1.2.8.2 ACCESO DE PERSONAL CONTROLADO O CONSULTORES

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

1.2.8.3 ACCESOS PÚBLICOS

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través de correo electrónico) deben tener en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

1.2.9 ADMINISTRACIÓN

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimiento, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que producirá una eventual exposición de la misma a usuarios no autorizados.

Asé los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

1.2.9.1 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS

1.2.9.1.1 ORGANIZACIÓN DEL PERSONAL

Este proceso lleva generalmente cuatro pasos:

1. **Definición de puestos:** debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
2. **Determinación de la sensibilidad del puesto:** para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
3. **Elección de la persona para cada puesto:** requiere considerar los requerimientos de experiencia y conocimientos técnico necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.
4. **Entrenamiento inicial y continuo del empleado**: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

1.3 NIVELES DE SEGURIDAD INFORMÁTICA

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abraca los subniveles B1, C2, C1 y el D.

1.3.1 NIVEL D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

1.3.2 NIVEL C1: PROTECCIÓN DISCRECIONAL

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este “super usuario”; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumera los requerimientos mínimos que debe cumplir la clase C1:

- **Acceso de control discrecional**: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismo privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- **Identificación y Autenticación**: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

1.3.3 NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requieren que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tiene la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

1.3.4 NIVEL B1: SEGURIDAD ETIQUETADA

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el diseño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.)

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

1.3.5 NIVEL B2: PROTECCIÓN ESTRUCTURADA

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado para almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

1.3.6 NIVEL B3: DOMINIOS DE SEGURIDAD

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser los suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

1.3.7 NIVEL A: PROTECCIÓN VERIFICADA

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y

el hardware con protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.4 TIPOS DE ATAQUES Y VULNERABILIDADES

La identificación de las vulnerabilidades permite conocer los tipos de ataque que podrían ser efectuados, así como también sus consecuencias. Se realizará una descripción general de los principales tipos de ataque.

1.4.1 INGENIERÍA SOCIAL.

Consiste en persuadir a los usuarios para que ejecuten acciones o revelen la información para superar las barreras de seguridad.

1.4.2 NEGACIÓN DE SERVICIO (Denial of service, DoS)

Es un tipo de ataque cuya meta fundamental es la de impedir el uso legítimo o negar el acceso a un recurso determinado.

1.4.3 CRACKING DE PASSWORDS

Existen dos métodos:

Diccionario: Consiste en efectuar encriptaciones de palabras (posibles claves) y comparar estas encriptaciones con el original.

Fuerza Bruta: Consiste en realizar todas las combinaciones posibles de un conjunto de caracteres. En el siguiente cuadro se ve el tiempo de búsqueda de una contraseña de acuerdo a la longitud y tipo de caracteres utilizados.

Long. en caracteres	26 (letras minúsculas)	36 (letras y dígitos)	52 (letras mayúsculas y minúsculas)	96 (Todos los caracteres)
6	50 min.	6 horas	2.2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10.5 meses	17 años	219 años
9 10	21 meses 45 años	32.6 años 1159 años	881 años 45838 años	2287 años 21 millones de años

Tabla 1.1 Tiempo para hallar una clave valida. (100.000 claves por segundo)

1.4.4 E-MAIL BOMBING Y SPAMMING

El e-mail bombing consiste en enviar muchas veces el mismo mensaje a una misma dirección. El spamming, que es una variante del e-mail bombing, se refiere a enviar el email a centenares o millares de usuarios.

Trayendo al usuario inconveniente por perdida de tiempo al tener que escoger entre correo invalido y el "spam", además puede ocasionar que el usuario deje de recibir correo por desbordamiento del espacio en la cuenta electrónica.

1.4.5 ESCANEO DE PUERTOS

Existen herramientas para verificar los servicios que presta una máquina por medio de la revisión de los puertos abiertos.

1.4.6 BUFFER OVERFLOWS

Es posible corromper la pila de ejecución escribiendo más allá de los límites reservados para un programa en ejecución. La pila es una estructura last-in, first out (último en entrar, primero en salir) en la que los datos sucesivos se "colocan encima" de los anteriores. Los datos se sacan después en orden inverso de la pila.

Los errores de programación que causan el desbordamiento son:

Combinaciones no esperadas: Los programas usualmente son construidos usando muchas capas de código, todas las capas se colocan encima del sistema operativo, Un mal diseño de una capa puede causar que entradas pertenecientes a la capa superior de la aplicación sea mandada directamente al sistema operativo y ejecutado.

Entradas anormales: La mayoría de los programas manejan parámetros o valores suministrados como entradas validas. Si un programador no considera un tipo de entrada que el programa no puede manejar, ocasionará el daño de los datos de la aplicación.

Condiciones de carrera: "Situación en la que dos o más procesos leen o escriben en un área compartida y el resultado final depende de los instantes de ejecución de cada uno. Cuando esto ocurre y acciones que deberían ser particulares no lo son, existe un intervalo

de tiempo en el que un atacante puede obtener privilegios y violar la seguridad del sistema".

1.4.7 TRANSMISIÓN EN TEXTO PLANO

Servicios como el Telnet, FTP y http no utilizan ningún método de encriptación de la información enviada (recibida) al (del) cliente, dándole la posibilidad a un tercero de interceptar el tráfico y comprender los datos de la transferencia.

1.4.8 PROGRAMAS DAÑINOS (CREADOS INTENCIONALMENTE)

Son programas diseñados para atacar al sistema o para conseguir información sensible. Su funcionamiento está basado en el aprovechamiento de errores en los servicios o en partes inseguras del sistema.

1.4.9 SNIFFERS

"Los sniffers operan activando una de las interfaces de red del sistema en modo promiscuo. En este modo de configuración, el sniffer almacenará en un log todo el tráfico que circule por la tarjeta de red, ya sea destinado o generado por el propio sistema o desde/hacia cualquiera de los sistemas existentes en el entorno de red compartido. Asimismo, pueden ser instalados tanto en sistemas como en dispositivos de red.

La utilización de un sniffer permite la obtención de una gran cantidad de información sensible enviada sin encriptar, como por ejemplo usuarios, contraseñas, direcciones de correo electrónico, etc. El análisis de la información transmitida permite a su vez extraer relaciones y topologías de las redes y organizaciones.

Aparte de los programas independientes existentes para ésta tarea, los sistemas operativos poseen sniffers en las distribuciones comerciales, típicamente utilizados por el administrador de red para resolver problemas en las comunicaciones".

1.5. SISTEMA DETECCIÓN DE INTRUSOS (IDS) (INTRUSION DETECCTION SYSTEM)

La detección de intrusos es una tecnología que intenta identificar intrusiones que sean realizadas contra una red de computadoras. Para descubrir posibles intrusiones en su

sistema informático, un administrador puede hacer uso de un sistema de detección de intrusos (IDS's).

Para realizar su labor, muchos IDS's basan sus operaciones en el análisis de un seguimiento realizado sobre el sistema operativo. Los datos así obtenidos constituyen una "huella" del uso del sistema a lo largo del tiempo. A partir de esta información, los IDS's calculan métricas sobre el estado global del sistema y deciden si en un determinado momento el sistema está sufriendo algún tipo de intrusión.

Los IDS's también pueden realizar su propio sistema de monitoreo, manteniendo un conjunto de estadísticas que ofrecen un perfil del uso del sistema. Las estadísticas citadas pueden ser obtenidas de varias fuentes como pueden ser: el uso de la CPU, las entradas y salidas a disco, el uso de memoria, las actividades realizadas por los usuarios, el número de logins intentados, etc. Estos datos deben ser actualizados continuamente para reflejar el estado actual del sistema y, a partir de un modelo interno, el IDS determinará si una serie de acciones constituyen una intrusión o un intento de intrusión. El modelo interno mencionado puede describir un conjunto de escenarios de intrusión o posibles perfiles de un sistema sin intrusiones.

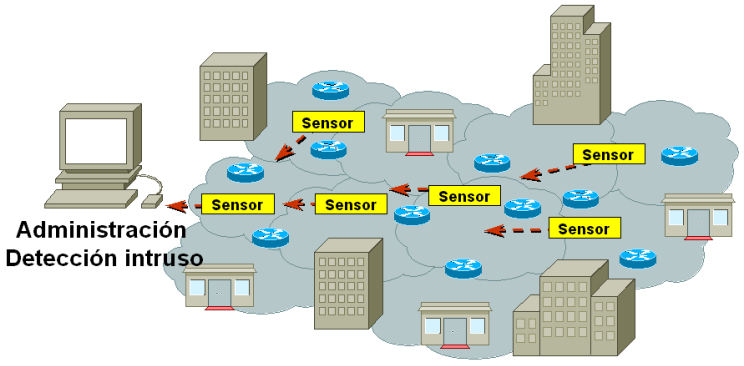


Figura 1.1. Ejemplo de detección de intrusos en red

CLASIFICACIÓN DE LOS IDS'S

- **IDS BASADOS EN HOSTS:** Este tipo de IDS's monitorizan log's de eventos de actividades sospechosas procedentes de diversas fuentes. Estas herramientas son especialmente útiles para detectar intrusiones iniciadas por usuarios habituales en el sistema o usuarios que se infiltran a través de la red. Los fallos son detectados muy rápidamente lo que hace a estas herramientas de detección muy populares. Abacus Project, Kane Secure Enterprise KSE, RealSecure OS Sensor o Intruder Alert son ejemplos de productos de este tipo.
- **IDS BASADO EN RED (NIDS):** Básicamente es un sniffer –monitoriza el tráfico de la red y además detecta tráfico no deseable (actuando en consecuencia). Algunos productos de este tipo son snort, Defense Worx IDS, Network Flight Recorder, RealSecure, SHADOW.
- **IDS HÍBRIDO:** Consiste en la combinación de los dos anteriores proporcionando una máxima cobertura, no obstante, esto supone un gasto importante, por lo que se suele reservar para servidores críticos. En el futuro se estima que serán los utilizados. Pertenecen a este tipo productos como CentraxICE, CyberCop Monitor o RealSecure Server Sensor.
- **HONEYPOTS:** Un honeypot es un sistema que simula uno o varios host's vulnerables, por lo que tales host's resultarán un objetivo apetecible para cualquier atacante. De este modo, si poseemos un punto vulnerable en nuestro sistema, el intruso perderá tiempo en el honeypot dándonos un margen de tiempo para resolver la parte del sistema que realmente se encuentre en estado crítico. Algunos productos son BackOfficer Friendly, Spectre, CyberCop Sting o Mantrap.
- **VERIFICADORES DE INTEGRIDAD DE FICHEROS:** Cuando un sistema es atacado, el intruso a menudo alterará ciertos ficheros clave para poder acceder posteriormente y evitar que sea detectado.. De este tipo de IDS's existen Tripwire, Veracity, Fcheck o chrootkit entre otros.
- **IDENTIFICACIÓN DE PUERTOS:** Examina los puertos en activo y para cada nuevo puerto encontrado, determina si es peligroso. Algunos productos de este tipo son Intrusion Vision, Intruder Alert o NetForensics.

Actualmente existen sobre 88 productos IDS distintos, por lo tanto, a continuación se introducirán funciones y características generales de los dos tipos de IDS's más populares: los basados en host y los basados en red.

1.5.1 IDS BASADO EN RED (NIDS)

Para realizar su labor, NIDS analiza paquetes de red en bruto buscando una firma procedente de algún atacante. Para determinar si una firma pertenece a un atacante se compara con un modelo de posibles atacantes. Este reconocimiento se realiza en tiempo real y normalmente se realiza con un módulo de reconocimiento de ataques IDS. Para realizar este reconocimiento se usan cuatro técnicas que son las siguientes:

- Mediante patrones o emparejamiento de expresiones.
- Frecuencia o sobrepaso de un determinado umbral.
- Relación mutua entre pequeños eventos.
- Detección de estadísticas "anormales".

De todas ellas, la técnica más usada es la basada en patrones, también denominada análisis de firmas o detección de abusos. Dicha técnica está programada para interpretar una serie de paquetes como un ataque. El IDS busca una subcadena dentro del flujo de datos que llega a través de los paquetes de red y cuando encuentra una cadena que se corresponde con ella, advierte de una intrusión. Por ello es de gran importancia disponer de una lista de firmas de ataques totalmente actualizada.

En el momento que descubre un ataque, reacciona ante el mismo del modo que su capacidad (variará de unos productos IDS a otros) y la política de administración del sistema le permita. Las capacidades de IDS incluyen acciones como enviar alertas a la consola, registrar eventos, enviar e-mails, eliminar conexiones (TCP reset), reconfigurar un firewall o un enrutador, o usar una "trampa" SNMP.

La mayor parte de los sistemas IDS basados en red sitúan un agente o sensor en el segmento de la red que desea ser monitorizada.

Este agente enviará de vuelta los datos recogidos a la consola de la computadora encargada de monitorizar todos los agentes utilizados. Los datos intercambiados entre la

consola y los agentes deben estar encriptados para prevenir un ataque de intercepción o de inhabilitación de un agente (por ejemplo un intruso podría hacerse pasar por la consola anulando la labor del agente).

La computadora que se use como IDS ha de cumplir una serie de requisitos como son tener instalado una tarjeta de red para monitorizar la red o el segmento de red que se desee mantener seguro, rapidez de procesador para procesar los datos enviados por todos los agentes en un tiempo corto y capacidad de almacenamiento en disco para mantener los log's y datos recibidos de los agentes –además del paquete de software IDS-. Las tarjetas de interfaz de red de los agentes (NIC) deben correr en modo promiscuo. Esto permite a las computadoras agentes ver todo el tráfico de paquetes en el segmento de red en el que se encuentre.

La consola y el agente pueden correr en la misma máquina, no obstante, numerosos vendedores no recomiendan esto debido a que se puede sobrecargar los recursos del ordenador, especialmente en redes muy ocupadas.

Los agentes (o sensores) IDS deben ser situados en el/los lugar/es más adecuado/s para la detección de intrusiones en la red, pero no existe unanimidad de opinión sobre la localización más adecuada de los agentes. En determinadas empresas se prefiere la ubicación de los agentes dentro del firewall debido a que se deben detectar los ataques que entran por el firewall. En otras en cambio, se decide poner fuera del firewall (en lo que se conoce como zona delimitada o DMZ) para detectar los ataques contra el propio firewall; por supuesto, esto deja al agente en situación de poder ser atacado y su mantenimiento será probablemente muy tedioso. Muchos firewalls permiten crear túneles seguros o redes virtuales privadas (VPN) que permiten acceso seguro al agente. Normalmente habrá que configurar un túnel por el número de puerto que el IDS use para la comunicación entre agente y consola.

Otra opción puede consistir en poner un agente fuera y otro dentro de la zona custodiada por el firewall, con lo que se obtiene una gran capacidad de detección; esto permite tener pleno conocimiento de los dos "lados" del firewall. Además, también se podría saber si existe alguien fuera que no logra entrar debido a una mala configuración del firewall.

1.5.2 IDS BASADO EN HOST

Surgieron como una manera automatizada de examinar los log's de los ordenadores, lo cual resulta en numerosas ocasiones definitivo para detectar hackers, de hecho, el famoso hacker kevin Mitnick fue cazado por un ingeniero que chequeó los log's de su ordenador; sus ataques hubiesen sido detectados tanto por el IDS basado en host's como por el basado en red.

En sistemas que corren con Windows NT, los IDS's basados en host's monitorizan el sistema, los eventos y los log's de seguridad que posee el sistema; en sistemas con Unix, monitorizan el syslog. Cuando se añade una entrada en el log, el IDS comprueba que dicha entrada no coincida con un patrón de ataque. Algunos IDS's también comprueban si ha habido algún cambio en determinados ficheros del sistema usando checksum's, y si es así envían una notificación. Adicionalmente, también pueden monitorizar los puertos del ordenador en el que están, tomando medidas cuando hay accesos a determinados puertos.

Cuando detectan una intrusión pueden hacer varias acciones: registrar el evento causante, enviar un aviso a la consola, iniciar una "trampa" SNMP, finalizar el login del usuario o inhabilitar la cuenta del usuario.

1.6 POLÍTICAS DE SEGURIDAD

Hoy es imposible hablar de un sistema cien por ciento seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hacheadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. "Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo que puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Existen organizaciones que han desarrollado documentos, directrices y recomendaciones que orientan el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de las mismas.

En este sentido, las Políticas se Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos.

1.6.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

El proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Es imposible proponer un documento establecido, lo que debe hacer el usuario o una organización para lograr una mayor Seguridad Informática posible. Lo que si es posible proponer lineamientos generales que se deben seguir para lograr un documento con estas características. La Seguridad Informática es el resultado de la innovación tecnológica, a la par del avance tecnológico.

Según Julio C. Ardita: "Una política de seguridad funciona muy bien en EE.UU., pero cuando estos manuales se trajeron a América Latina fue un fracaso."

Una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está permitido en el área de seguridad durante la operación general del sistema.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero ante todo una política de seguridad es una forma de comunicarse con los usuarios, siempre hay que tener en cuenta que la seguridad comienza y termina con personas, y debe:

- Ser holística (cubrir aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.

- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad ha de contemplar los elementos claves de seguridad: integridad, disponibilidad, privacidad y adicionalmente control, autenticidad y utilidad.

1.6.2 EVALUACIÓN DE RIESGOS

El análisis de riesgos supone más que el hecho de calcular la disponibilidad de que ocurran cosas negativas.

- Se debe obtener una evaluación económica del impacto de estos sucesos.
- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles.
- Se debe conocer qué se quiere proteger, donde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos.

1.6.3 ESTRATEGIA DE SEGURIDAD

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles. El plan de seguridad debe incluir una estrategia Preactiva y otra Reactiva.

La estrategia PROACTIVA, o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La estrategia REACTIVA o estrategia posterior al ataque ayudará al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan

de contingencia desarrollado en la estrategia Preactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- **Lo que no se permite expresamente esta prohibido**: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- **Lo que no se prohíbe expresamente está permitido**: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás si lo estarán.

1.6.3.1 IMPLEMENTACIÓN

La implementación de medidas de seguridad, es un proceso Técnico – Administrativo. Este proceso abarca toda la organización, sin exclusión alguna, debe estar apoyado por la Gerencia, ya que sin su apoyo, las medidas tomadas no tendrán fuerza necesaria.

La implementación de Políticas de Seguridad, trae varios problemas que afectan el funcionamiento de la organización. La implementación conlleva a incrementar la complejidad en la operación de la organización tanto técnica como administrativamente.

Es indispensable notificar a los involucrados en las nuevas disposiciones, y darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una Política de Seguridad deberá abarcar:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.

- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias del no cumplimiento de la política.
- La política debe especificar que las cosas ocurran, las sanciones que se puedan imponer. No deberá especificar con exactitud qué pasará o cuando algo sucederá.
- Explicaciones comprensibles sobre el porque de las decisiones tomadas.
- Debe ser un documento dinámico de la organización, debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes.

El siguiente diagrama indica como realizar una Política de Seguridad:

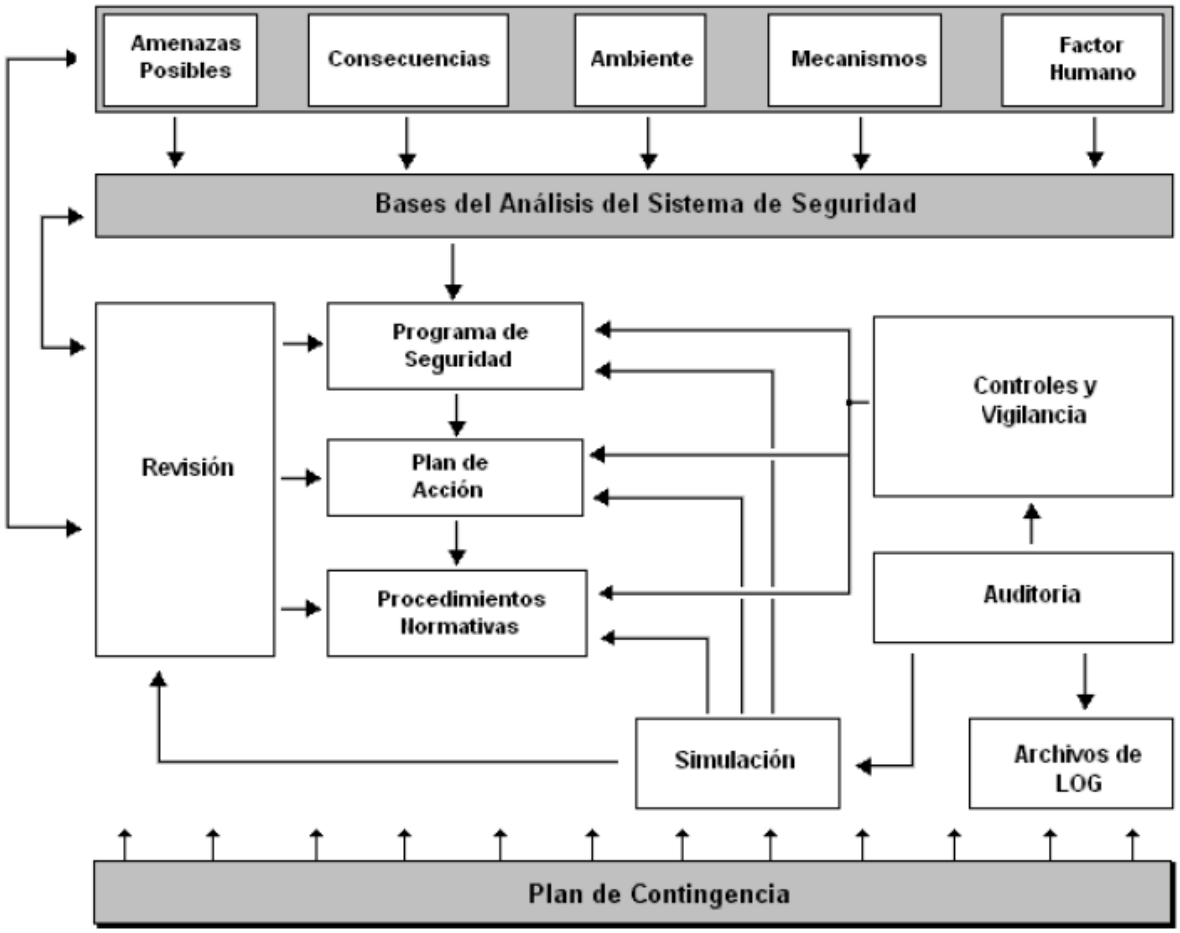


Figura 1.2: Diagrama de Política de Seguridad

1.6.3.2 AUDITORIA Y CONTROL

La Auditoria son los "ojos y oídos" de la dirección. La Auditoria consiste en contar con los mecanismos para determinar que es lo que sucede en el sistema, que es lo que hace cada uno y cuando lo hace.

El objetivo del control es contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

1.6.3.3 PLAN DE CONTINGENCIA

Consiste en los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea una parte, la capacidad funcional del sistema. El Plan de Contingencias debe incluirse en el Plan de Recuperación de Desastres.

La RECUPERACIÓN, es la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la capacidad de volver a la situación anterior, habiendo recuperado el máximo posible de los recursos e información.

1.6.3.4 EQUIPOS DE RESPUESTA A INCIDENTES

Es aconsejable formar un equipo de respuestas a incidentes, el mismo que debe estar implicado en trabajos preactivos del profesional de seguridad, se debe considerar:

- El desarrollo de instrucciones para controlar incidentes.
- Creación del sector del responsable, generalmente Administrador de seguridad.
- Identificación de herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas se Seguridad Informática.
- Realización de investigaciones acerca de virus.
- Ejecución de estudios relativos a ataques al sistema.

1.6.3.5 BACKUPS

El Backup de archivos permite tener integra y disponible la información para cuando sucedan accidentes. Es necesario realizar un análisis Costo/Beneficio para determinar que información será almacenada.

1.6.3.6 PRUEBAS

Las pruebas y el estudio de sus resultados, se lleva a cabo después que se han puesto en marcha las estrategias reactiva y preactiva. Estas pruebas no se deben llevar a cabo en los sistemas de producción real.

Si es posible se deben comprobar y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad que se van a implementar.

CAPITULO II

2. SERVICIOS Y PROTOCOLOS POR CAPAS DE RED – MODELO OSI

Una de las necesidades más acuciantes de un sistema de comunicaciones es el establecimientos de estándares, sin ellos sólo podrían comunicarse entre si equipos del mismo fabricante y que usaran la misma tecnología.

La conexión entre equipos electrónicos se ha ido estandarizando paulatinamente siendo la redes telefónicas las pioneras en este campo.

La ISO (International Organisation for Standarisation) ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación. Tampoco existe ningún sistema de comunicaciones que los siga estrictamente, siendo la familia de protocolos TCP/IP la que más se acerca.

El modelo OSI describe siete niveles para facilitar las interfaces de conexión entre sistemas abiertos.

Nivel	Nombre	Función	Dispositivos y protocolo
1	Físico	Se ocupa de la transmisión del flujo de bits a través del medio.	Cables, tarjetas y repetidores (hub). RS-232, X.21.
2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos.	Puentes (bridges). HDLC, LLC, Ethernet, PPP
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red.	Encaminador(router). IP, IPX, ARP, RIP
4	Transporte	La función de este nivel es asegurar que el receptor reciba exactamente la misma	Pasarela (gateway). UDP, TCP, SPX.

		información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.	
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	NFS - Linux
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Pasarela. Compresión, encriptado, VT100. JPG – MP3
7	Aplicación	Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un fichero). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el fichero).	X.400, FTP, TELNET, HTTP, Correo electronico.

Tabla 2.1

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas datos de control.

De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. La forma, pues de enviar información en el modelo OSI tiene una cierta similitud con enviar un

paquete de regalo a una persona, donde se ponen una serie de papeles de envoltorio, una o más cajas, hasta llegar al regalo en sí.

Emisor	Paquete	Receptor
Aplicación	C7 Datos	Aplicación
Presentación	C6 C7 Datos	Presentación
Sesión	C5 C6 C7 Datos	Sesión
Transporte	C4 C5 C6 C7 Datos	Transporte
Red	C3 C4 C5 C6 C7 Datos	Red
Enlace	C2 C3 C4 C5 C6 C7 Datos	Enlace
Físico	C2 C3 C4 C5 C6 C7 Datos	Físico

Tabla 2.2

C7-C2 : Datos de control específicos de cada nivel.

Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos protocolos. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario reescribir todo el conjunto.

En las familias de protocolos más utilizadas en redes de ordenadores (TCP/IP, IPX/SPX, etc.) nos encontraremos a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

2.1 SEGURIDAD A NIVEL DE CAPAS

El desarrollo de protocolos está basado en los servicios definidos en las capas de comunicación del modelo estandar OSI-ISO [Briscoe, 2000], para entender

apropiadamente las características de los protocolos de seguridad y su intervalo de aplicación, se ha elaborado una marco de trabajo que esquematiza una relación entre los servicios y las capas de protocolos. En la Tabla 2.3 puede observarse que los servicios de seguridad pueden aplicarse completamente en la capa 7, parcialmente en las capas 3 y 4, mucho menos ingerencia en las capas 1 y 2, y prácticamente ninguna función en las capas 5 y 6.

Servicio	**Capas de comunicación**						
	1	2	3	4	5	6	7
Autenticación de entidad extremo (Peer Entity)	-	-	✓	✓	-	-	✓
Autenticación del origen de los datos	-	ND	✓	✓	-	-	✓
Servicios de Control de acceso	-	ND	✓	✓	-	-	✓
Confidencialidad de la conexión	✓	✓	✓	✓	-	-	✓
Confidencialidad orientada a no conexión	-	✓	✓	✓	-	-	✓
Confidencialidad de un campo selectivo	-	-	-	-	-	✓	✓
Confidencialidad del flujo de trafico	✓	-	✓	-	-	-	✓
Integridad orientada a no conexión	-	ND	✓	✓	-	-	✓
Integridad de un campo selectivo	-	-	-	-	-	-	✓
Origen, no repudio	-	-	-	-	-	-	✓
Recepción, no repudio	-	-	-	-	-	-	✓

Tabla 2.3: Relación de servicios a Capas de Protocolos.

2.1.1. SEGURIDAD EN LA CAPA FÍSICA

En esta capa se tiene una dependencia significativa de la tecnología de red que se utilice. El equipo y todo lo demás cambia si hay modificación de tecnología de comunicación: Ethernet, SDH, SONET, etc. Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico), no se provee servicio, pero se da soporte a las capas superiores para control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es individual o a nivel de circuitos conmutados. En la Figura 2.1 se esquematiza un escenario común de componentes de capa física, se distinguen con la letra S aquellos componentes con capacidad de protección de datos y cifrado, y con la letra D aquellos que son los puntos débiles por proteger.

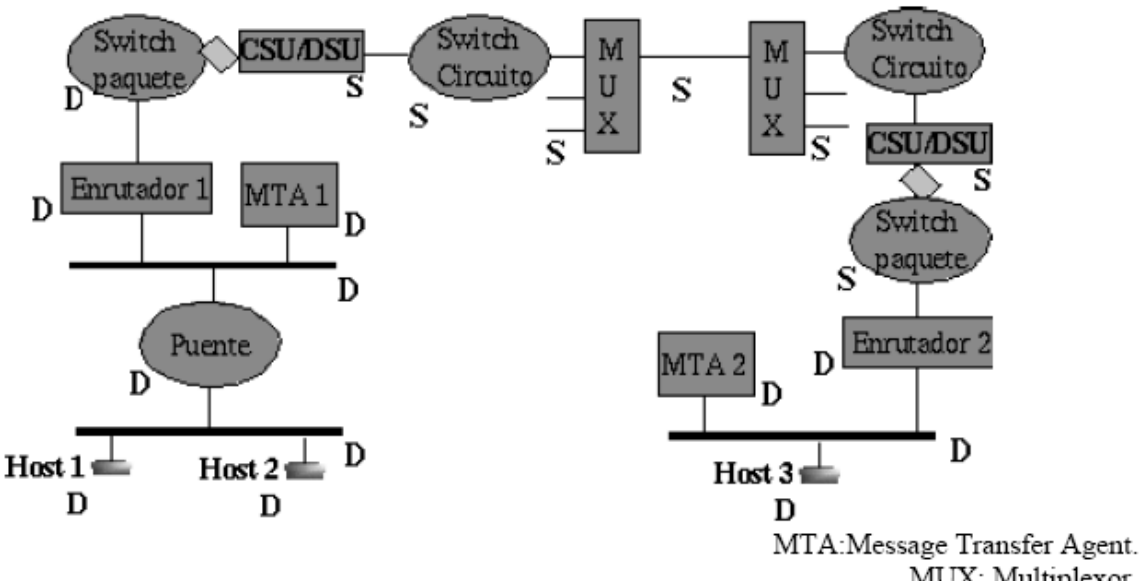


Figura 2.1: Ejemplo de seguridad en la capa física en una red de paquetes

2.1.2. SEGURIDAD EN LA CAPA DE ENLACE

En esta capa se tiene una dependencia ligera de la tecnología (IEEE LANs) y del conjunto de protocolos que se utilice. Los servicios de seguridad son: confidencialidad, control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es en los hosts individuales y en los segmentos de la LAN. En la Figura 2.2 se esquematiza un escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

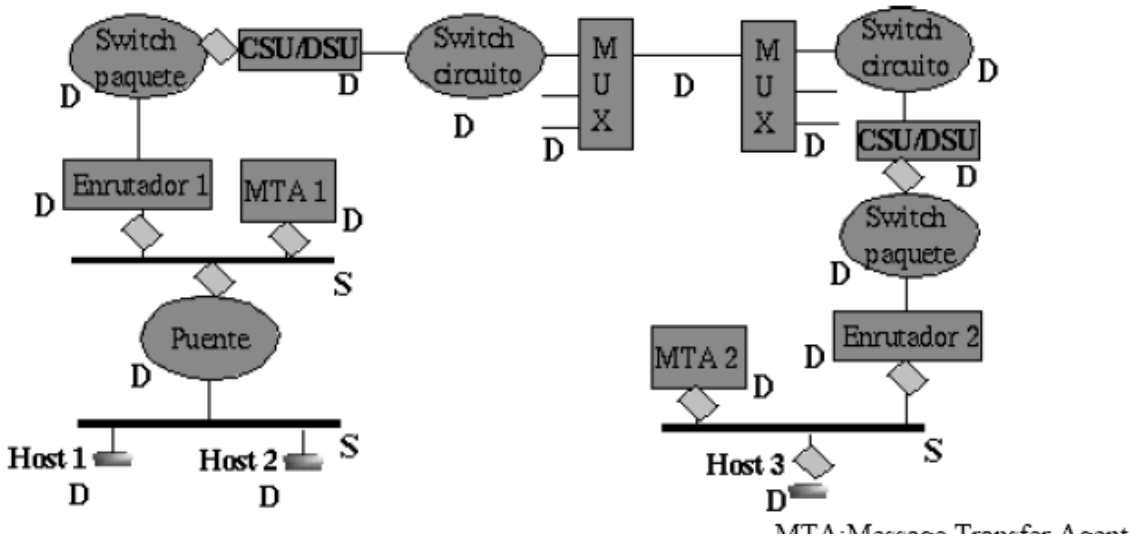


Figura 2.2: Ejemplo de seguridad en la capa de enlace en una red de paquetes

En la Figura 2.3, se muestra la conjunción de los ejemplos de la capa 1 y 2, se aprecia su complemento y necesidad de aplicación de seguridad en las capas superiores.

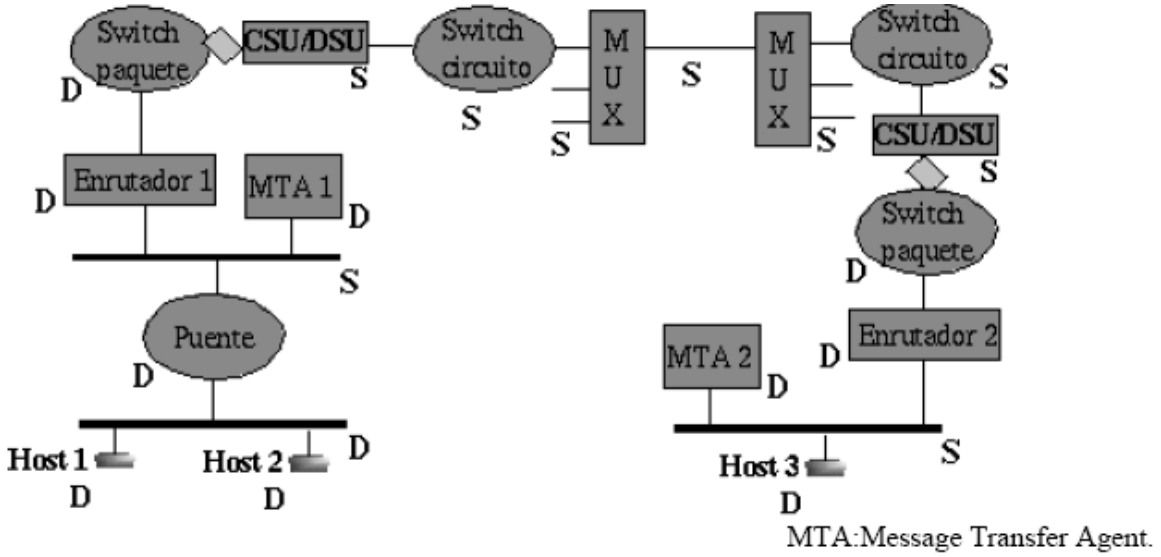


Figura 2.3: Ejemplo de seguridad en las capas física y de enlace en una red de paquetes

2.1.3. SEGURIDAD EN LA CAPA DE RED (INFERIOR)

En la subcapa inferior de esta capa se tiene una alta dependencia de la tecnología de red y menor sobre el conjunto de protocolos que se utilicen. Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control

de acceso, autenticación del origen de los datos e integridad orientada a conexión y a no conexión (dependiente de la red). La granularidad de protección radica en los hosts (por conexión) y en el enrutador (LAN). En la Figura 2.4 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

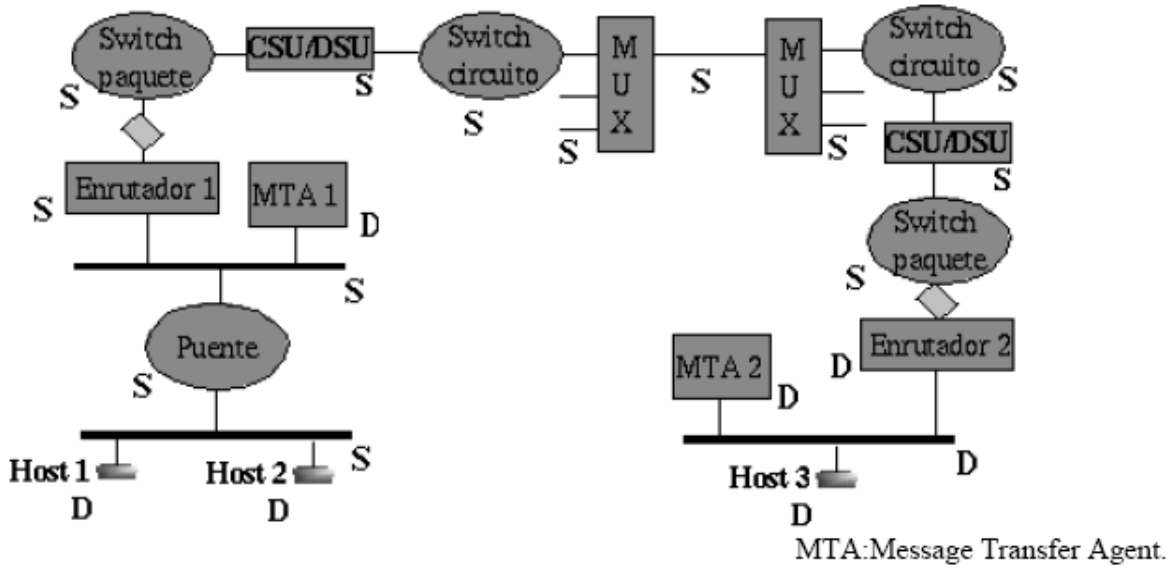


Figura 2.4: Ejemplo de seguridad en la capa de red (inferior) en una red de paquetes

2.1.4. SEGURIDAD EN LA CAPA DE RED (SUPERIOR)

En la subcapa superior de esta capa no se tiene dependencia de la tecnología de red, aunque sí moderada sobre el conjunto de protocolos que se utilicen (el tunelaje de IP disminuye esto considerablemente). Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del origen de los datos e integridad orientada a no conexión y a secuencia parcial. La granularidad de protección radica en los hosts, en la red o seguridad de calidad de servicio (QoS). En la Figura 2.5 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger

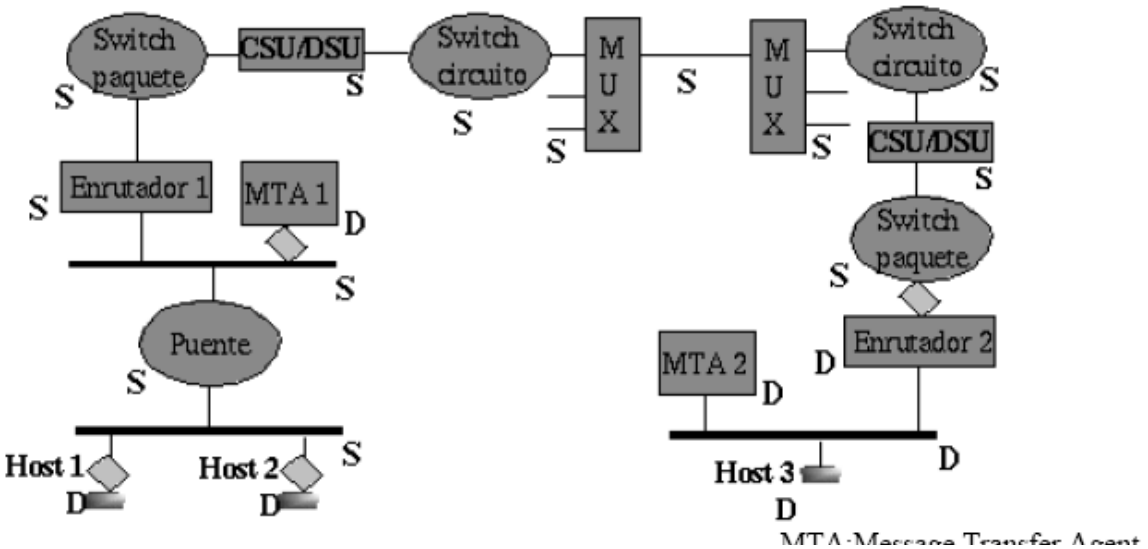


Figura 2.5: Ejemplo de seguridad en la capa de red (superior) en una red de paquetes

2.1.5. SEGURIDAD EN LA CAPA DE TRANSPORTE

En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice. Los servicios de seguridad son: confidencialidad, control de acceso, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a no conexión e integridad orientada a conexión con recuperación de datos. La granularidad de protección radica en los hosts por conexión. En la Figura 2.6 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquellos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

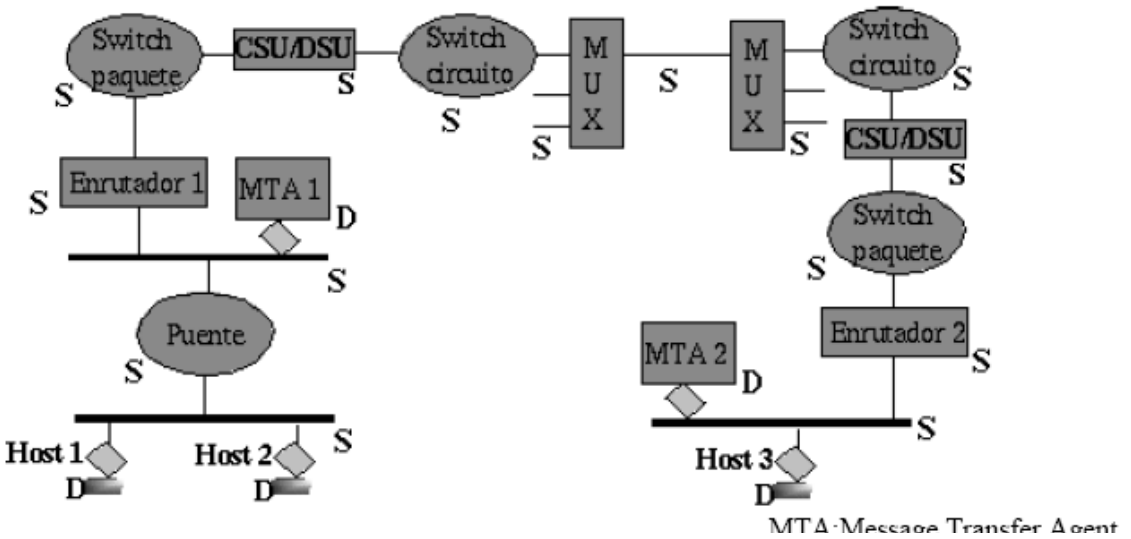


Figura 2.6: Ejemplo de seguridad en la capa de transporte en una red de paquetes.

2.1.6. SEGURIDAD EN LA CAPA DE SESIÓN

En esta capa no se tiene dependencia de la tecnología de red. La dependencia es significativa sobre las aplicaciones. Los servicios de seguridad son: integridad orientada a conexión, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a conexión y control de acceso. La granularidad de protección radica en las sesiones. El escenario de componentes y riesgos para esta capa es igual al de la capa de transporte mostrada en la Figura 6.

2.1.7. SEGURIDAD EN LA CAPA DE APLICACIÓN

En esta capa no se tiene dependencia de la tecnología de red. La dependencia es significativa sobre las aplicaciones. Los servicios de seguridad son: confidencialidad (orientado a conexión, a no conexión, o a un campo selectivo), autenticación del origen de los datos, autenticación de la entidad extremo, integridad (orientada a conexión y a no conexión, con opción a recuperación) y no repudio (en el origen y recepción). La granularidad de protección radica en los usuarios, aplicaciones y PDUs (Protocol Data Unit). En la Figura 2.7 se esquematiza el escenario común de componentes, y se distinguen de acuerdo a los servicios de esta capa, con la letra S aquéllos componentes considerados seguros, con la letra D aquellos puntos débiles por proteger.

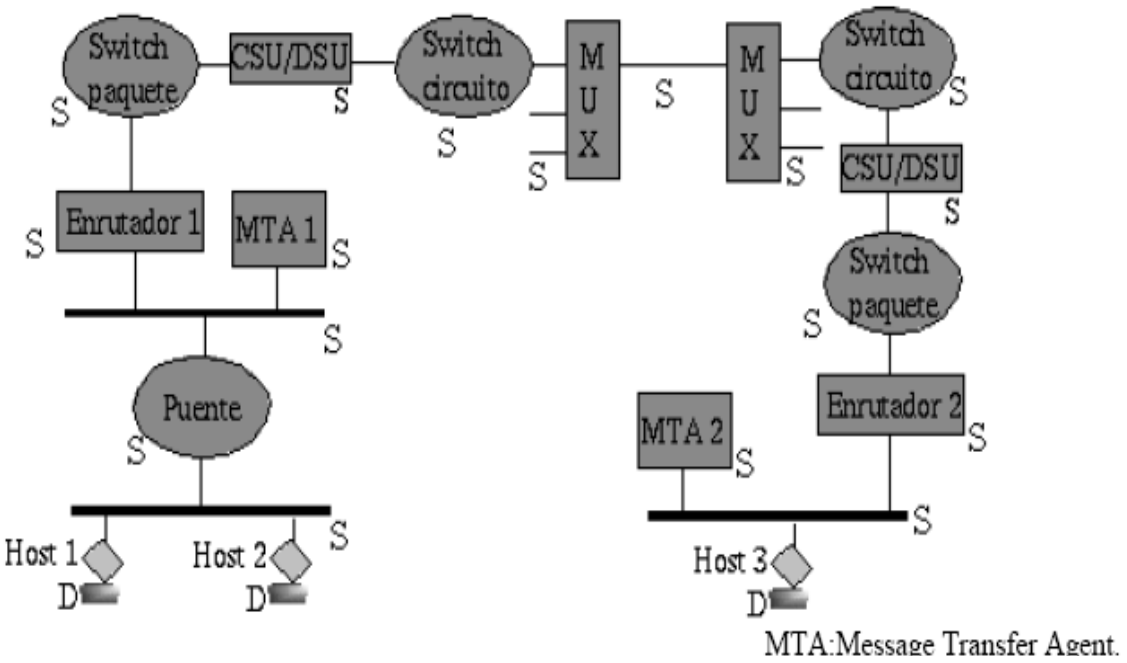


Figura 2.7: Ejemplo de seguridad en la capa de aplicación en una red de paquetes

2.2. PROTOCOLOS

Reglas para suministrar un lenguaje formal que permita que todos los equipos, sin importar su tecnología, puedan comunicarse entre si.

Uno de los más importantes protocolos es el TCP/IP, el cual "proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP / IP Proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto"1. Este protocolo hoy en día permite la utilización de dive rsos servicios en la red como: transmisión de correo electrónico, transferencia de archivos, Web, etc.

- **LOS PUERTOS**

Un puerto se representa por un valor de 16 bits que indica al servidor a cual servicio se le esta haciendo una petición.

Por convención, los puertos se encuentran divididos en tres rangos:

- Del 0 al 1023: Puertos denominados “Well Known”. Su uso por convención requiere de privilegios de Superusuario.
- Del 1024 al 49151: Registrados y asignados dinámicamente.
- Del 49152 al 65535: Puertos privados.

La tabla que se muestra a continuación presenta un listado de algunos de los puertos más utilizados:

Puerto	Aplicación	Descripción
21	FTP	Control Transferencia Archivos
22	SSH	Servicio Remoto vía SSL
23	Telnet	Servicio Remoto
25	SMTP	Envío de mails
53	DNS	Servidor de Nombres de Dominios
79	Finger	Información de usuarios
80	WWW- HTTP	World Wide Web
110	POP3(PostOffice)	Recepción de mail
137	NetBios	Intercambio de datos en red
443	HTTPS	http seguro vía SSL
5432	PostgreSQL	Base de Datos

Tabla 2.4

TABLA DE PUERTOS DE RED

En la actualidad LINUX orientan su utilización a ofrecer servicios a la red y uno de los problemas que podemos tener son justamente estos servicios. Los servicios son puertas con las cuales los usuarios (clientes) u otros servicios pueden interactuar. Cuántas más puertas tengamos en una casa menos segura es esta.

Estos servicios se dan en unos puertos determinados. A cada puerto se le nombra por un número pudiendo ir desde 1 hasta 65536. Veamos cuales son esos servicios

(algunos abiertos por defecto), a que puertos se asocian, que hacen y con cuales nos debemos quedar.

Servicio/Puerto/Protocolo	Descripción	Localización
echo/7/tcp-udp	Todo lo que se mande a ese puerto lo devuelve.	inetd.conf
daytime/13/tcp-udp	Devuelve la hora y fecha del sistema	inetd.conf
ftp/21/tcp	Servidor FTP	inetd.conf
telnet/23/tcp	Permite conectarnos y abrir una consola remotamente	inetd.conf
smpt/25/tcp	Gestiona la distribución de correo de la máquina	/etc/rc.d
timeserver/37/tcp-udp	Devuelve la hora del sistema	inetd.conf
named/53/tcp-udp	Servidor de nombres (DNS)	/etc/rc.d
gopher/70/tcp	Sistema de indexación de los servidores FTP	inetd.conf
finger/79/tcp	Devuelve la información sobre los usuarios del sistema	inetd.conf
http (www)/80/tcp	Servidor www	/etc/rc.d
pop2/109/tcp	Servidor de correo pop versión 2	inetd.conf
pop3/110/tcp	Servidor de correo pop versión 3	inetd.conf
rpcbind/111/tcp-udp	Servidor de RCP (portmapper)	/etc/rc.d
auth(ident)/113/tcp	Identifica y registra a los usuarios que hace uso de servicios tcp	inetd.conf
innd/119/tcp	Servidor de News	/etc/rc.d
netbios/137-138-139/tcp-udp	Servidor Samba. Windows para Workgroups	/etc/rc.d
imap2/143/tcp	Servidor de correo Imap versión 2	inetd.conf
login/513/tcp	Permite logias remotos (rlogin) a usuarios autorizados	inetd.conf
shell/514/tcp	Permite shells remotos (rshell) a usuarios autorizados	inetd.conf
syslog/514/udp	Registra todos los sucesos del sistema y los guarda en logs	/etc/rc.d

Servicio/Puerto/Protocolo	Descripción	Localización
lpd/515/tcp	Servidor de impresión	/etc/rc.d
uucp/540/tcp	Antiguo protocolo de comunicación de unix	inetd.conf
mountd/635/udp	NFS mount daemon	/etc/rc.d
nfsd/2049/udp	Sistema de ficheros de red de Unix	/etc/rc.d
x-windows/6000	Acepta conexiones de servidores X autorizados	host-

Tabla 2.5

Solo deberemos dejar abiertos aquellos puertos que vamos a usar. Si por ejemplo no necesitamos un servidor FTP, deberíamos desactivar estos servicios.

CAPITULO III

3. REDES SEGURAS USANDO EL SISTEMA GNU/LINUX

El sistema operativo libre GNU/Linux se usa en las soluciones de seguridad de redes aquí presentadas por varias razones: se tiene acceso al código fuente, y esto permite encontrar soluciones a los posibles problemas; usándolo en simples computadoras personales permite contar con soluciones de software, en vez de hardware que es muy caro, de ruteadores y cortafuegos; y otro punto mas importante, la arquitectura de GNU/Linux (tiene el subsistema de control de red dentro del mismo núcleo del sistema operativo) lo hace muy eficiente en los servicios de red, tanto como para rivalizar con el hardware especializado de ruteadores y cortafuegos.

Su gratuidad, flexibilidad, potencia, apertura, facilidad para obtención de herramientas y otras muchas virtudes hacen de Linux la elección cada vez más frecuente entre los administradores de sistemas a la hora de decidirse por una u otra plataforma.

Aunque Linux es un sistema muy robusto e incorpora las características de seguridad comunes a todos los sistemas tipo Unix, a pesar de todo resulta fundamental dedicar cierto tiempo y recursos para conocer cuáles son sus debilidades y vías frecuentes de ataque y adoptar posteriormente las medidas más eficaces para contrarrestarlas. A menudo un sistema operativo es tan seguro como la astucia y habilidad de su administrador.

Lo primero que tenemos que tener en mente es que no existe nada como un sistema completamente seguro. Todo lo que puede hacer es aumentar la dificultad para que alguien pueda comprometer su sistema. En el caso medio del usuario de Linux en casa, no se requiere demasiado para mantener alejado al cracker. Para usuarios con grandes requisitos (bancos, compañías de telecomunicaciones, etc.) se requiere mucho más trabajo.

Otro factor a tener en cuenta es que cuanto más incremente la seguridad del sistema, más intrusiva se vuelve la seguridad, en otras palabras, el sistema puede perder funcionalidad y resentirse la comodidad. Es necesario decidir en qué medida el sistema es utilizable y en qué medida es seguro para ciertos propósitos. Por ejemplo, puede necesitar

que cualquiera marque a su modem para que éste devuelva la llamada a su casa. Esto es más seguro, pero si alguien no está en casa hace más difícil que se pueda conectar. También se puede configurar el sistema Linux sin conexión a Internet, pero esto dificulta que pueda navegar por las webs. Si el sitio es medio-grande, se deberá establecer una "Política de Seguridad" que indique qué niveles requiere el sitio y qué medidas de evaluación se realizan.

Es necesario listar todos aquellos recursos (servidores, servicios, datos y otros componentes) que contengan datos, den servicios, formen parte de la infraestructura de tu compañía, etc.

3.1 REDES MILITARIZADAS

Zona militarizada: Máxima seguridad, sólo ingresarán los usuarios de Intranet

El interior es el área de confianza de la internetwork. Los dispositivos que están en el interior forman la red privada de la organización. Estos dispositivos comparten unas directivas de seguridad comunes con respecto a la red exterior (Internet). Sin embargo, resulta muy habitual que un firewall segmente el entorno de confianza. Si un departamento, como Recursos Humanos, tiene que ser protegido del resto de usuarios de confianza, se puede utilizar un firewall.

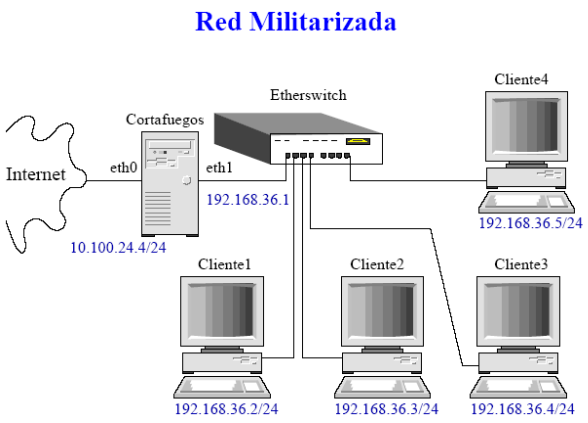


Figura 3.1

3.2 REDES DESMILITARIZADAS

Zona desmilitarizada: Nivel intermedio de seguridad, accederán también los usuarios de Extranet.

La DMZ es una red aislada, a la que pueden acceder los usuarios del exterior. Es necesario configurar el firewall para permitir el acceso desde el exterior o el interior hasta la DMZ. La creación de una DMZ posibilita que una empresa ponga la información y los servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado. Esto permite el acceso a los usuarios del exterior, sin permitir el acceso al interior. Los hosts o servidores que residen en la DMZ suelen denominarse hosts bastión. En este caso, un host bastión es un host que está actualizado con respecto a su sistema operativo y las modificaciones experimentadas por este último. El hecho de que esté actualizado generalmente lo hará menos vulnerable a los ataques, ya que el fabricante habrá establecido o "parcheado" todos los defectos conocidos. El host bastión es un host que sólo ejecuta los servicios necesarios para realizar sus tareas de aplicación. Los servicios innecesarios (y a veces más vulnerables) son desactivados o eliminados.

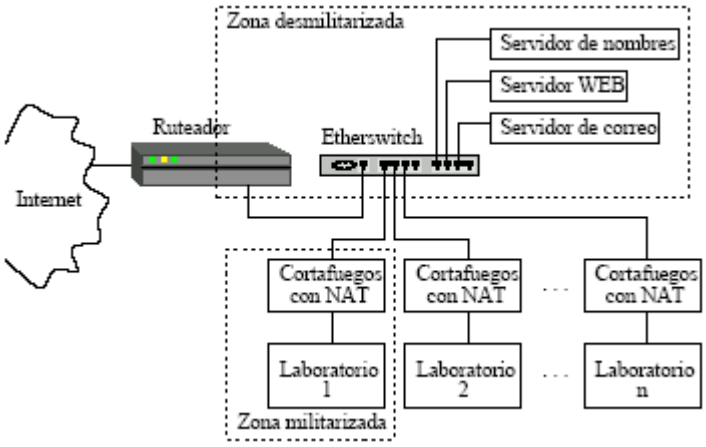


Figura 3.2

- La red DMZ es una red pequeña y aislada situada entre la red privada e Internet
- La red DMZ está configurada de modo que:
  - Los sistemas de Internet y de la red privada pueden acceder a un número limitado de sistemas de la red DMZ.

– La transmisión directa de tráfico a través de la red DMZ está prohibido

Zona pública: Sin medidas de seguridad, en este esquema lo representa todo Internet.

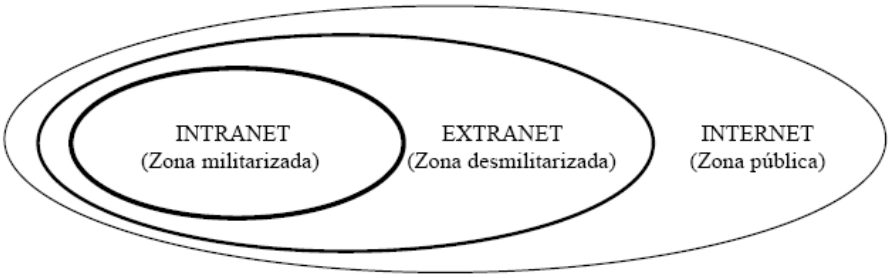


Figura 3.3

3.3 ARQUITECTURA GNU/LINUX

3.3.1 NOCIONES DE SISTEMA OPERATIVO LINUX

Linux es un sistema operativo basado en Unix que se distribuye bajo licencia GNU. Este sistema operativo ha sido diseñado y programado por multitud de programadores alrededor del mundo y su núcleo sigue en continuo desarrollo.

ARQUITECTURA DE GNU/LINUX

- Linux no es un bloque monolítico
- Varios componentes trabajan en conjunto, diseñados por personas diferentes y conjuntados en distribuciones
- Solo del exterior el núcleo Linux parece una unidad
- Existe una diferencia entre el núcleo y las aplicaciones

El sistema de archivos de Linux tiene una estructura definida según su propósito:

/etc	Archivos de configuración
/var	Datos volátiles y directorios de spooling
/usr	Programa y librerías accesibles por el usuario
/usr/bin	Herramientas de uso general (editores, correos, compiladores)
/usr/sbin	Utilizado para herramientas de administración que no sean esenciales (cron, lpd)
/usr/local	Contiene la mayor parte de elementos de software que se añade de forma no estándar (bin, lib, etc, man)

/usr/share/man	Páginas manuales
/usr/share/doc	Documentos variados sobre el software instalado
/mnt	Punto de montaje temporal de dispositivos
/tmp	Archivos temporales del sistema
/home	(creado por defecto) Directorios de todos los usuarios
/dev	Archivos de interfaz de dispositivos
/boot	Archivos estáticos para el arranque del sistema
/lib	Compartidas esenciales. Módulos de núcleo
/bin	Comandos básicos
/root	Directorio de la cuenta de administrador
/proc	Información asociada con el núcleo que se está ejecutando
/sbin	Comandos básicos para la administración del sistema

Tabla 3.1 Estructura de directorios.

COMPONENTES DEL NÚCLEO

- Administración memoria principal
- Acceso a los periféricos
- Administración del espacio en disco duro
- Administración de los programas y los procesos
- Administración de los derecho de acceso

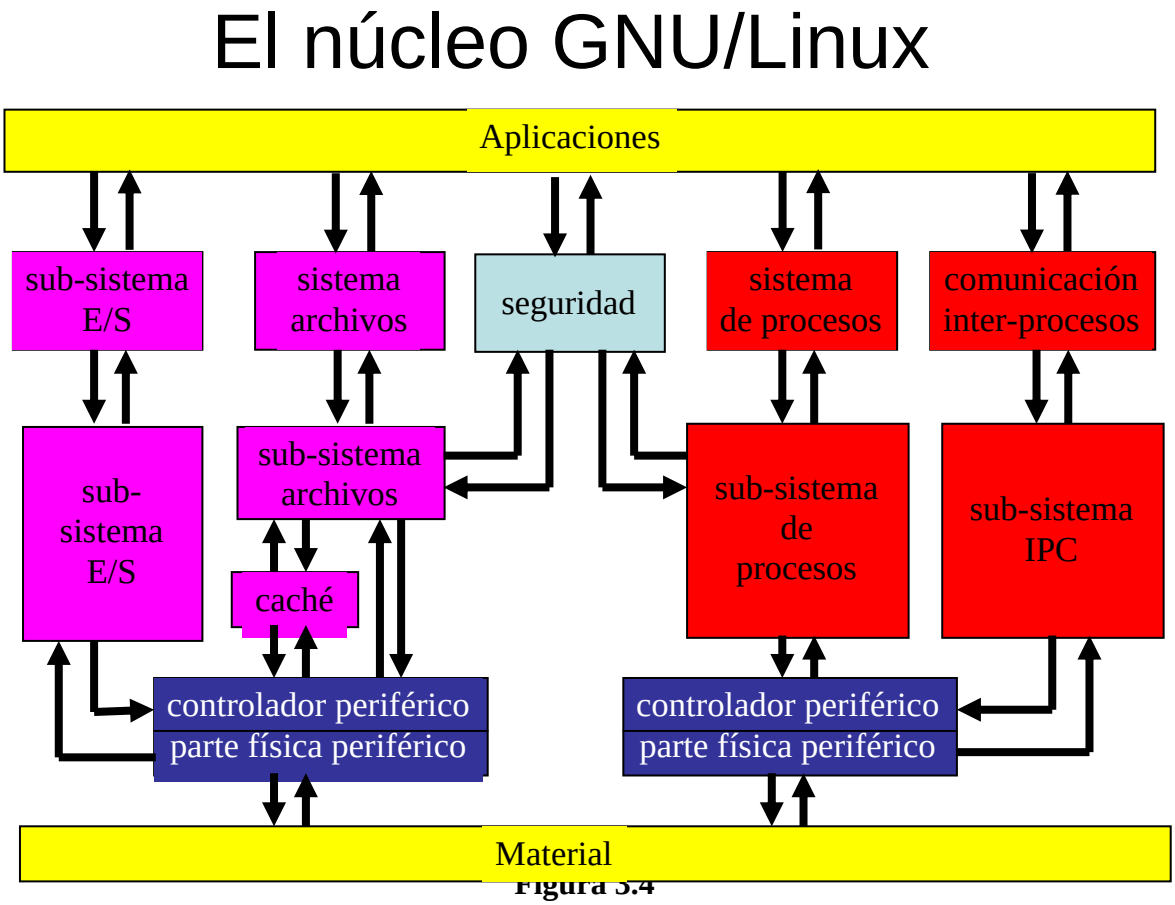


Figura 3.4

3.4 PUERTOS (GATEWAYS)

Un Gateway es un server, que proporciona a clientes conectividad hacia el mundo exterior, estén o no dentro de una red.

Este server, puede ser cualquier tipo de máquina, con cualquier sistema operativo que sea capaz de proveer funcionalidades de router y firewall

Un gateway o puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading, usada muy a menudo para dar acceso a

Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

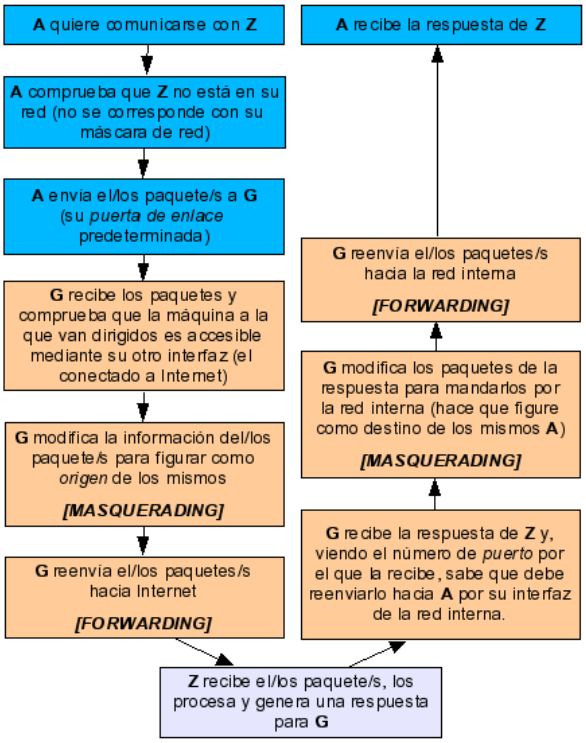


Figura 3.5

3.5 CORTAFUEGOS (FIREWALLS)

Se puede definir de una forma simple un sistema firewall, como aquel sistema o conjunto combinado de sistemas que crean una barrera segura entre 2 redes.

El firewall es un sistema que refuerza las políticas de control de acceso. Estas políticas regulan el tráfico entre una red interna (de confianza) y otra red externa (de dudosa confianza). Normalmente, los firewall se utilizan para proteger a las redes internas del acceso no autorizado vía Internet o mediante otra red externa.

La función del firewall, por tanto, es bloquear el tráfico no autorizado entre un sistema de confianza y un sistema de dudosa confianza.

Un firewall es, a menudo, instalado en el punto donde una red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del firewall, así puede determinar si dicho tráfico es aceptable de acuerdo a sus políticas de seguridad.

Aunque el propósito principal de los firewall es mantener a los intrusos fuera del alcance de la información que es propiedad de un ente determinado, ya sea un usuario, una empresa o un gobierno, su posición dentro del acceso a distintas redes le vuelve muy útil para controlar estadísticas de situaciones como usuarios que intentaron conectarse y no lo consiguieron, tráfico que atravesó la misma, etc. Esto proporciona un sistema muy cómodo de auditar la red. Algunas de sus funciones son las siguientes:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques
- Dividir una red en zonas con distintas necesidades de seguridad
- Auditar el acceso a la red.

Algunos firewall solamente permiten tráfico de correo a través de ellos, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otros firewall proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión. Generalmente, los firewalls están configurados para proteger contra "logins" sin autorización. Esto ayuda principalmente a prevenir actos de vandalismos en máquinas y software de nuestra red. Redes firewalls más elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior comunicarse libremente con los usuarios del exterior. Los firewall pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello.

Hay una serie de asuntos básicos que hay que tratar en el momento de que una persona adquiere la responsabilidad de diseñar, especificar e implementar o supervisar la instalación de un firewall en una empresa:

1. Reflejar la política con la que la compañía u organización quiere trabajar con el sistema: ¿Se destina el firewall para denegar todos los servicios o solo algunos?, ¿se va a emplear el firewall para proporcionar un método de medición y auditoria de los accesos no autorizados a la red?

2. Determinar el nivel de vigilancia, redundancia y control que queremos. La seguridad total es imposible, así que tendremos que establecer un nivel de riesgo aceptable. Para ello se pueden establecer una lista de comprobación de los que debería ser vigilado, permitido y denegado.
3. El tercer asunto es financiero. Es importante intentar cuantificar y proponer soluciones en términos de cuánto cuesta comprar o implementar tal cosa o tal otra. A veces lo realmente necesario no es gastarse mucho dinero en un firewall muy potente, sino perder tiempo en evaluar las necesidades y encontrar un firewall que se adapte a ellas.

3.5.1 TIPOS DE FIREWALLS

Existen tres tipos fundamentales de firewalls, pudiendo catalogarse en función al nivel en el que se encuentren. Esto no siempre es cierto ya que un firewall, para ser completo, deberá estar presente en todos los niveles.

1) FILTRADOR DE PAQUETES (PACKET FILTER)

Va a analizar la información contenida dentro de los paquetes IP antes de permitirles el acceso o no al ordenador. Para ello va a coger los paquetes IP y les va a aplicar unas reglas de filtrado. Normalmente se implementa mediante un router con 2 interfaces de red: uno de cara al interior y otro de cara al exterior.

El filtrado de paquetes se puede basar en cualquiera de los siguientes criterios:

- Protocolos utilizados
- Dirección IP de origen y de destino
- Puerto TCP-UDP de origen y destino

Una tabla de reglas de filtrado podría tener la siguiente forma:

Origen	Destino	Tipo	Puerto	Acción
192.169.0.0	*	*	*	Deny
*	10.10.11.0	*	*	Deny
192.168.0.0 *	* 10.10.10.0	* *	* *	Allow Deny
*	*	*	*	Deny

Tabla 3.2 Filtrado de Paquetes

Si al Firewall donde está definida esta política llega un paquete proveniente de la red 192.169.0.0, su paso sería bloqueado sin importar su destino. Igual sucede si llega información a la subred 10.10.11.0, su paso sería bloqueado sin importar su origen.

El orden de análisis de la tabla es muy importante para poder definir una buena política de seguridad. En la tabla anterior por ejemplo, podemos ver qué sucede si llega un paquete desde la red 192.168.0.0 a la subred 10.10.10.0. Una de las reglas dice que todos los paquetes provenientes de la red 192.168.0.0 son permitidos, mientras que la siguiente regla indica que cualquier paquete que llegue a la subred 10.10.10.0 debe ser bloqueado. Si la tabla es leída de arriba hacia abajo, el paquete podría pasar, ya que la tabla es consultada hasta que se encuentra una regla que se ajuste a la cabecera del paquete. Si la tabla es consultada de abajo hacia arriba, el paquete sería bloqueado. Es por esto que las reglas de filtrado deben ser muy claras y sencillas.

2) PASARELAS A NIVEL DE APLICACIÓN

Es el extremo opuesto a los filtradores de paquetes. En lugar de filtrar el flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado en cada uno de ellos. Es probablemente el sistema más seguro, ya que no necesita utilizar complicadas listas de acceso y centraliza en un solo punto la gestión del servicio, además de que nos permitirá controlar y conocer información de cada uno de los servicios por separado.

3) PASARELAS A NIVEL DE RED

Se basan en el control de las conexiones TCP y su manera de actuar es la que sigue: por un lado reciben las peticiones de conexión a un puerto TCP y por el otro se establecen las conexiones con el destinatario deseado si se han cumplido las restricciones de acceso establecidas.

3.6 BLOQUEO DE SERVICIOS INDESEABLES CON IPTABLES

- **UTILIZACIÓN DEL IPTABLES**

El filtrado de paquetes está incluido en el kernel de Linux. Para poder utilizar iptables, se debe compilar el kernel con la opción CONFIG_NETFILTER activada.

IPtables es un sistema de firewall vinculado al kernel. Un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación, iptables esta integrado con el kernel, es parte del sistema operativo. ¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas. Para ellos se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas.

Iptables maneja las reglas de filtrado de forma dinámica. Esto significa que cada máquina sea reiniciada, las reglas se borrarán. Por este motivo, se recomienda crear un script que se ejecute al iniciar el sistema para que éstas vuelvan a ser definidas.

Una vez creadas las reglas, pueden ser grabadas por medio de la orden iptablessave y pueden ser recuperadas con iptables-restore.

El núcleo de Linux agrupa las diferentes reglas definidas por el administrador en tres listas denominadas chains: INPUT, OUTPUT y FORWARD. Cuando un paquete es recibido, el sistema utiliza en primer lugar las reglas de la lista INPUT para decidir si la acepta o no. Si las reglas definidas en esta lista indican que el paquete puede ser aceptado, se comprueba dónde debe ser enrutado. Si el destino es una máquina diferente a firewall, se aplican las reglas de la lista FORWARD para reenviarlo a su destino.

La lista OUTPUT se utiliza antes de enviar un paquete por una interfaz de red, para decidir si el tráfico de salida es permitido o no.

Si el paquete no cumple ninguna de las reglas de la lista, puede ser aceptado o rechazado según haya sido configurado el iptables. Para lograr mantener un nivel óptimo de seguridad, se recomienda que sea configurado para que rechace el paquete.

Cuando un paquete cumple con una determinada regla de una lista, se define qué hacer con éste mediante una acción (Target). Las acciones utilizadas en iptables son: ACCEPT, que permite el paso del paquete. DROP, que lo bloquea, QUEUE y RETURN.

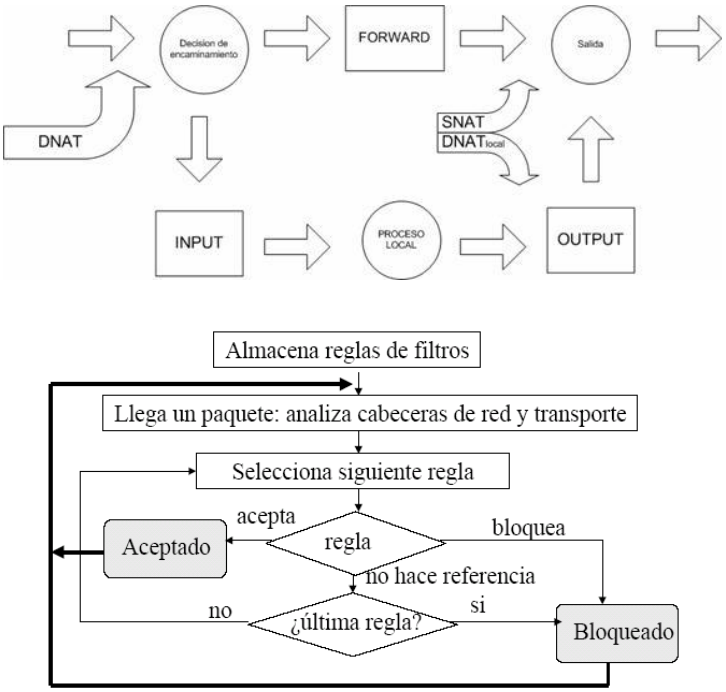


Figura 3.6

Como se ve en el gráfico, básicamente se mira si el paquete esta destinado a la propia maquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD. INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino

- **CREACIÓN DE UNA POLÍTICA DE SEGURIDAD EN IPTABLES**

Se definirá una política de seguridad básica para ilustrar el funcionamiento del firewall.

Lo primero que puede hacerse antes de comenzar a definir las reglas de filtrado, es eliminar las reglas asociadas a cada lista, de forma que no interfieran con las que se van a definir. Para ello se utiliza la opción '-F'. Además, se puede definir una política por defecto mediante la opción '-P'. Esta política será la que se aplique cuando un paquete no cumpla con ninguna de las reglas establecidas en las listas. Ejemplo:

```
[root@localhost]# /sbin/iptables -P INPUT DROP
[root@localhost]# /sbin/iptables -F INPUT
[root@localhost]# /sbin/iptables -P OUTPUT ACCEPT
[root@localhost]# /sbin/iptables -F OUTPUT
[root@localhost]# /sbin/iptables -P FORWARD DROP
[root@localhost]# /sbin/iptables -F INPUT
[root@localhost]#
```

3.7 REUBICACIÓN DE LOS SERVIDORES

A lo largo de los años, los departamentos de Tecnología de la Información, han desarrollado su infraestructura de Servidores según las necesidades que iban apareciendo.

Ahora, muchos de esos responsables de Tecnología, se están esforzando para determinar que hacer con todas las diferentes plataformas que tienen que administrar y operar. La solución ideal hubiera sido que todos los servidores fueran del mismo suministrador, pero lo más frecuente es una mezcolanza de productos desplegada.

- ESTÁNDAR PARA OPERACIÓN DE UN CENTRO DE TELECOMUNICACIONES

Este documento tiene por objetivo darle a conocer los requerimientos necesarios para la instalación de los equipos de telecomunicaciones **que proveen conexión a la red interna de la dependencia**, garantizando el buen funcionamiento del sistema y obteniendo el mayor tiempo de vida útil de sus componentes y periféricos. Los requerimientos son los siguientes:

- **REQUISITOS ARQUITECTÓNICOS**

- Designar un cuarto llamado Centro de Telecomunicaciones que deberá tener un área mínima de 16 m^2 (diagrama I):

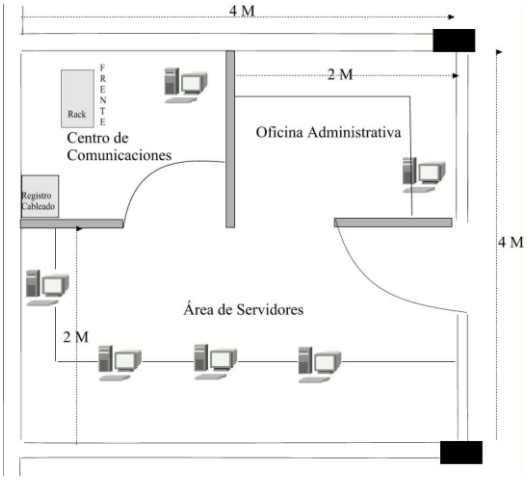


Figura 3.7

- $4m^2$ a $8m^2$ para el Área de Telecomunicaciones donde se instalarán los equipos de telecomunicaciones de la red y acometidas de enlaces: DS0, inalámbrico, ISDN y cableado de red interna de la dependencia.
- 8 m^2 para el Área de Servidores donde se ubicarán los servidores de red: Servidor de Bibliotecas, Servidor del Sistema Institucional, Servidor de Red Local y Servidor de Aplicaciones Sun Blade.
- 4 m^2 para el Área del ATI, para el monitoreo permanente de los servicios y de la red.
- Para protección del área se recomienda eliminar las ventanas de vidrio hacía el exterior o, en su caso, instalar protectores.

- **REQUISITOS AMBIENTALES**

- **Temperatura:** la temperatura debe estar entre 15º C y 30º C grados centígrados, pero se recomienda que esté a 22º C estables. También se recomienda la instalación de un **aire acondicionado tipo industrial de preferencia.**
- **Humedad:** la humedad debe estar entre 20 y 55% no condensada.
- **Iluminación:** el cuarto debe estar bien iluminado.
- **Interferencia:** el equipo debe estar alejado de fuentes de calor (reguladores, baterías de respaldo, etc.) campos electrostáticos o electromagnéticos (transformadores, tableros de control eléctrico, etc.) y de radio frecuencia (equipos de sonido, equipos de comunicación, etc.)

➢ **MODELO DE PROTECCIÓN ELÉCTRICA EN INSTALACIONES DE SISTEMAS DE CÓMPUTO Y COMUNICACIONES**

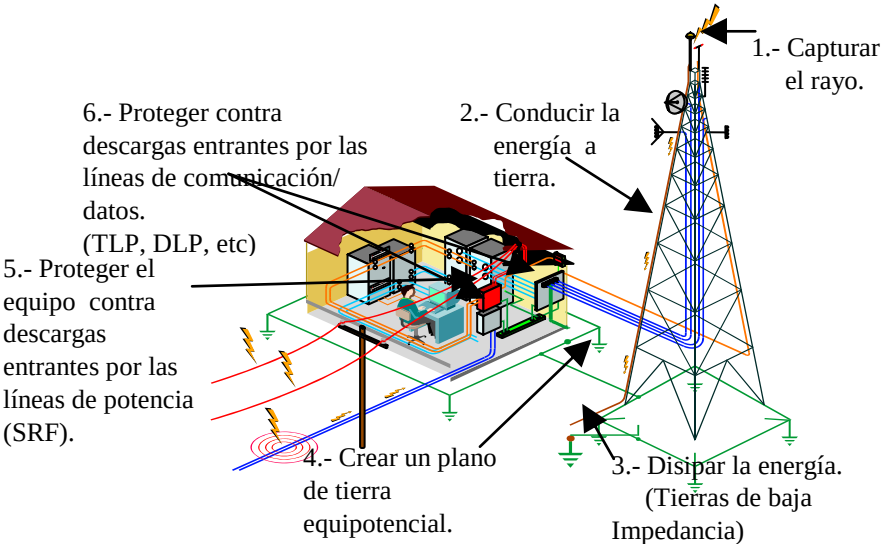


Figura 3.8

1. **CAPTURAR LA DESCARGA ATMOSFÉRICA EN UN PUNTO DESIGNADO**. Se requiere contar con una terminal aérea, para una adecuada protección ante descargas eléctricas, el cual deberá aterrizarse a un sistema de tierra física tipo de delta.
2. **CONDUCIR SIN RIESGO LA DESCARGA A TIERRA EN FORMA SEGURA.** Conductor de cobre, acero o aluminio.
3. **DISIPAR LA ENERGÍA A TIERRA.** Los componentes del sistema de tierra deberán ser: Conector soldarura exotérmica Caldwell, Electrodo, Electrodo a tierra fabricados con una barra de acero recubierta por una gruesa película de cobre (0.254 mm) de acuerdo a las Normas ANSI/UL 467-1984 y ANSI C 33-8, 1972 y Tierra La resistividad del terreno debera de ser considerada con cuidado, incluyendo el contenido de humedad y la temperatura.
4. **CREAR UN PLANO DE TIERRA EQUIPOTENCIAL.** Interconectar todos los Sistemas de:
   - ❖ Electrodos de Tierra.
   - ❖ Sistema general de Tierra.
   - ❖ Sistemas de Tierra de Pararrayos.
   - ❖ Sistemas de Tierra de Telecomunicaciones.

- ❖ Cable para Sistemas de Tierra.
- ❖ Conectar todos los objetos conductivos internos y externos de las instalaciones a Tierra.
- ❖ Proveer una diferencia de potencial lo más cercana a cero durante transitorios que eleven el potencial.

5. **PROTEGER CONTRA TRANSITORIOS ENTRANTES POR LOS CIRCUITOS DE POTENCIA.** Contar con supresores de picos cuya capacidad sea calculada de acuerdo a la capacidad de los equipos que se le conectarán. Utilizar supresores de pico con tasa de transferencia 0 para equipos de telecomunicaciones.
6. **PROTEGER CONTRA TRANSITORIOS ENTRANTES POR LOS CIRCUITOS DE COMUNICACIÓN/DATOS.** Evitando la corriente "sucia", al dividir la alimentación eléctrica de los equipos sensibles de los no sensibles, adquiriendo un transformador que limpie la corriente que se entregará al equipo sensible.

3.8 LOGEO DE CLIENTES A SU DOMINIO

La información necesaria para mantener los usuarios del sistema está en el fichero */etc/passwd*. Cada línea de este fichero contiene la descripción de cada usuario de la siguiente forma:

login:password:UID:GID:descripción:home:shell

donde:

- Login: palabra con el que se nombra al usuario.
- Password: contraseña de acceso en formato cifrado. En sistemas shadow se pone en este campo x.
- UID: número de identificación único de usuario. Es el número con el que se validan las acciones del usuario con los recursos del sistema.
- GID: grupo primario al que pertenece el usuario.
- Descripción: típicamente se incluye el nombre completo del usuario.

- Home: directorio personal del usuario, p.e */home/juanmig*. Este directorio será el inicial cuando comience una sesión, y en él se guardan los ficheros de configuración personal del usuario y sus documentos de trabajo.
- Shell: programa de línea de comandos con el que se inicia la sesión, típicamente será */bin/bash* o */bin/sh*.

3.9 ADMINISTRACIÓN DE CADA SERVIDOR

- **ACCESO REMOTO**
  - **TELNET**

Telnet es la herramienta remota más vieja y conocida, prácticamente cualquier Unix viene con ella, incluso lo soportan sistemas como NT. Telnet sólo tiene uso cuando pueda administrar el sistema desde modo comandos, lo cual lo convierte en perfecto para sistemas Unix. Telnet es increíblemente inseguro, las contraseñas y los nombres de usuarios, al igual que los datos de las sesiones vuelan en texto simple, siendo el objetivo preferido de los sniffers. Telnet viene con todas las distribuciones de Linux.

  - **SSL TELNET**

SSL Telnet es telnet con el añadido de cifrado SSL, lo cual lo hace bastante más seguro.

  - **SSH**

SSH era gratis al principio, pero ahora está bajo licencia comercial, sin embargo tiene numerosas características que lo hacen merecer la pena. Soporta diferentes tipos de autentificación (contraseña, basada en rhosts, llaves RSA), permite redireccionar puertos, y se puede configurar fácilmente a qué usuarios se les permite usarlo.

  - **LSH**

LSH es una implementación gratuita del protocolo SSH, LSH tiene licencia GNU y está empezando a perfilarse como la alternativa a SSH.

- **REXEC**

REXEC es una de las utilidades UNIX más antiguas, te permite ejecutar comandos en un sistema remoto, aunque tiene el serio fallo de no tener un modelo de seguridad real. La seguridad se consigue mediante el uso de ficheros 'rhosts', que especifican qué hosts/etc. pueden ejecutar comandos, lo cual está sujeto a spoofing y otro tipo de exploits.

- **SLUSH**

Slush está basado en OpenSSL, y actualmente soporta certificados X.509, lo cual, para grandes organizaciones, es una apuesta mucho mejor que intentar recordar varias docenas de contraseñas en diferentes servidores. Por otra parte, está completamente basado en software de código abierto, dejando pocas posibilidades a que pueda tener puertas traseras/etc.

- **NSH**

NSH es un producto comercial con todos sus detalles. Tiene soporte para cifrado, de modo que es relativamente seguro de usar. Además de eso, NSH está disponible en múltiples plataformas (Linux, BSD, Irix, etc.) con RPM's disponibles para sistemas Red Hat.

- **FSH**

Fsh significa "Ejecución rápida de comandos remotos", y el concepto es similar al de rsh/rcp. Evita el costo de estar creando continuamente sesiones cifradas, habilitando un túnel cifrado utilizando ssh o lsh, y ejecutando todos los comandos sobre él.

- **SECSH**

secsh (Shell Seguro) aporta otra capa más de seguridad de login, una vez que ha hecho log vía ssh o telnet SSL te pide otra contraseña, si introduce una errónea, secsh mata el intento de login.

- **LOCALES**

- **YAST**

YaST (Yet Another Setup Tool, "otra herramienta más de seguridad") es un comando gráfico de líneas bastante interesante, (muy similar a scoadmin) que aporta una sencilla interfaz para la mayoría de las tareas administrativas. Sin embargo, no está pensado para limitar accesos a usuarios, así que sólo es útil para depurar errores y para permitir administrar su sistema a nuevos usuarios. Otro problema es que al contrario que Linuxconf, no está orientado a redes, lo cual quiere decir que hay que hacer un log en cada sistema que quiera manipular.

- **SUDO**

Sudo le da a un usuario acceso setuid a un programa, se le puede especificar desde qué host se les permite o no hacer login y tener acceso sudo (de modo que si alguien vulnera una cuenta pero está bloqueado, se minimizan los daños). Se puede especificar bajo qué usuario se ejecutará un comando, lo cual da un grado de control relativamente preciso. Si tiene que dar acceso a los usuarios, asegúrese de especificar los hosts desde los que les está permitido hacer un login cuando estén utilizando sudo. Esta herramienta es muy similar a super pero con un control ligeramente inferior. Sudo está disponible para la mayoría de las distribuciones, como paquete interno, o paquete contribuido.
Sudo permite definir grupos de hosts, grupos de comandos, y grupos de usuarios, haciendo la administración más sencilla, a largo plazo.

- **SUPER**

Super es una de las pocas herramientas que se pueden utilizar hoy en día para dar a ciertos usuarios (y grupos) diferentes niveles de acceso a la administración del sistema. Además, se pueden especificar horas y permitir el acceso a scripts, puesto que dar acceso setuid, incluso a comandos comunes, puede tener resultados inesperados. Es una herramienta potente, pero necesita una sustancial cantidad de esfuerzo para implementarse correctamente, y creo que merece la pena.

- **RUNAS**

Runas es muy parecido a sudo y Super, con algunas variaciones. Se crea un fichero de configuración listando el comando, como quien se ejecuta, y a qué usuarios/grupos/etc. se les permite ejecutarlo como tal. Además de esto, se pueden restringir el uso de opciones, y se le puede solicitar al usuario el motivo (lo cual queda registrado con syslog).

- **REMOTAS BASADAS EN WWW**
  - **WEBMIN**

Webmin es actualmente, una herramienta de administración no comercial. Es un conjunto de scripts de perl con un servidor www autocontenido al cual se accede utilizando un visor de www. Tiene módulos para la mayoría de las funciones de administración del sistema, aunque algunas son un poco temperamentales. Una de sus características preferidas es el hecho de que mantiene su propio usuario y contraseña para acceder a webmin, y se puede personalizar a qué tiene acceso cada usuario.

  - **LINUXCONF**

Linuxconf es una herramienta de administración Linux de propósito general, que se puede utilizar desde la línea de comandos, desde X, o vía su propio servidor www. Es una herramienta favorita para administración automatizada del sistema utilizada principalmente para hacer configuraciones de red complejas, ya que es relativamente ligera desde la línea de comandos. Desde X proporciona un vistazo general de todo aquello que puede configurarse (PPP, usuarios, discos, etc.). Para utilizarlo vía visor www, primero hay que ejecutar Linuxconf en la máquina y añadir el o los hosts o redes a las que se quiere permitir conectarse, salvar los cambios y salir.

  - **COAS**

El proyecto COAS (Caldera Open Administration System) es un proyecto muy ambicioso para proporcionar un marco abierto de administración de sistemas, desde línea de comandos (con interfaz semi-gráfico), desde X (utilizando el componente qt) hasta el web. Hace una abstracción de los datos reales de configuración aportando una capa intermedia, permitiendo de esta forma su uso en variadas plataformas Linux.

- **OTRAS HERRAMIENTAS BASADAS EN RED**
  - **VNC**

El Virtual Network Computer (VNC) es parecido a X o a PCAnywhere. Se puede mostrar un escritorio gráfico, y controlarlo remotamente, con NT o Linux como servidor y/o cliente. El VNC es bastante bueno a través de una Ethernet de 10 megabit, sin embargo tiende a utilizar un montón de potencia computacional relativamente comparado con otros métodos de administración remota. La seguridad del VNC no es tan buena, pero hay varios sitios con información acerca de asegurar VNC, utilizando SSL, SSH y otros métodos.

3.10 CONTROL DE ANCHOS DE BANDA

A) ADMINISTRANDO ANCHO DE BANDA CON SQUID

Uno de los inconvenientes más frecuente a la hora de administrar recursos en una red conectada a Internet es el consumo del ancho de banda por parte de los usuarios.

Para satisfacer las necesidades de los usuarios, squid ha implementado una característica llamada “Delay Pools”.

Esta característica implementa una forma para suministrar asignaciones de tokens de ancho de banda en una Red por medio de pools. Estos pools permiten crear una distribución más favorable del ancho de banda al que se acceder por la interfaz que esta conectada a la WAN y que es accedida por las estaciones de nuestra LAN a través de nuestro servidor squid.

Para poder usar esta característica es necesario habilitarla en el squid en tiempo de compilación, ya que viene deshabilitada por defecto en la mayoría de las distribuciones.

Para efectuar esta operación básicamente se puede realizar lo siguiente:

```
./configure –enable-delay-pools
make all
make install
```

Los delays_pools constan básicamente de las siguientes etiquetas y variables.

Las variables a tener en cuenta son:

aggregate (restore/maximun)
individual (restore/maximum)
network (restore/maximun)

Los parámetro aggregate, individual y network nos permiten actuar para limitar el tráfico. Estos parámetros vienen en pares restore/maximun, donde restore es el numero de bytes/seg (no bits/seg) situados dentro del bucket de bytes y maximun el numero de bytes máximo que puede estar dentro del bucket.

Las etiquetas a usar son:

- **delay_pools:** el cual representa el numero de delay pools a ser usado
- **delay_class:** define la clase de cada delay_pool. Existen tres clases de delay pools, clase 1, clase 2 y clase 3. cada uno se diferencia en la forma como limitan el ancho de banda.

En el caso de la clase 1 contiene un simple y unificado bucket, el cual es usado para todas las solicitudes en un pool determinado.

La Clase 2 contiene un bucket unificado y 255 buckets, uno por cada host en una red de 8 bits (en una red Clase C).

La Clase 3 contiene 255 buckets para las subredes en una red de 16 bits (red Clase B), y un bucket individual por cada host en esta red.

delay_access nos permite determinar cuales pools van a aceptar solicitudes y cuales no. Para ello es necesario crear unos ACLs (Access Control List) que especifique los rangos de direcciones IPs para cada pool.

delay_parameters define los parámetros para cada delay pool (en Bytes por segundo)

La sintaxis por cada tipo de clase es la siguiente:

- delay_parameters pool aggregate (Clase 1)
- delay_parameters pool aggregate individual (Clase 2)
- delay_parameters pool aggregate individual network (Clase 3)

(el parámetro pool es el numero del pool al que se hace referencia) Conociendo que es cada etiqueta procedamos con ejemplos, su sintaxis y uso.

➢ *CONTROLES DE ACCESO*

Una de las características más interesantes de este servidor proxy es la posibilidad de establecer unas reglas de control de acceso que pueden complementar perfectamente nuestro objetivo de filtrado de paquetes.

Para ello, confeccionaremos unas Listas de Control de Acceso para designar qué máquinas o redes tienen permitido, o no, acceder al servidor. Cada una de ellas tendrá asociada unas Reglas de Control que regulará esta actividad. Es decir, definimos unas listas, por una parte y establecemos unas reglas específicas para cada una de ellas.

3.11 IP ESTÁTICA DE LOS USUARIOS

➢ IP FIJAS CON DHCP

El servidor DHCPD de GNU/Linux procura dar siempre la misma IP a un PC. Aunque haya caducado una concesión, sigue guardando la entrada en un fichero histórico; sólo asigna de nuevo esa IP a otra máquina si no quedan más IP libres o si esa otra máquina ha pedido explícitamente esa dirección (lo que sólo ocurrirá normalmente si el PC ya estaba usando esa IP, que también la guarda en el disco para volver a pedir la misma si se vuelve a arrancar). El resultado es que si tenemos más IP que máquinas distintas llegan a conectarse, en la práctica es muy similar a que fueran IP fijas en lugar de dinámicas.

Pueden darse casos, no obstante, en los que accidentalmente un PC cambie de IP aun habiendo direcciones libres, aunque sean raros. Uno de ellos es si el disco duro se llena y no se puede grabar el fichero de asignaciones; en ese caso puede llegar otro PC, pedir la IP y al no saber que está arrendada asignarse. El que haya un usuario que sin saberlo esté

ejecutando en su PC un servidor DHCPD también puede provocar en determinadas circunstancias cambios de IP.

Muchos administradores prefieren resolver estos pocos casos si se llegan a dar, a tener que mantener asignaciones de IP estáticas en el servidor. Con Linux el procedimiento pasa por parar dhclient (bastaría, por ejemplo, con desactivar esa interfaz de red), para a continuación modificar el fichero /var/lib/dhcp/dhclient.leases. Tras cancelar con Webmin los arrendamientos volvemos a arrancar la interfaz de red.

Si considera preferible el asignar la dirección estáticamente, anote la dirección MAC de la tarjeta (si se cambia de tarjeta de red habrá que cambiar la asignación). Este dato lo puedes obtener desde el propio PC con Linux utilizando ifconfig (es el parámetro HWaddr) o la herramienta Webmin. Desde otro PC podemos mirarlo haciendo un ping a esa dirección y ejecutando arp. Con este dato usamos Webmin para configurar el servidor DHCPD: pinchamos en la opción añadir nueva máquina y rellenamos los campos nombre de máquina, dirección hardware y dirección IP fijada. Asimismo, en máquina asignada a ponemos la subred en que estará la máquina y de la que tomará el resto de la configuración (servidor DNS, ruta por defecto, etc.). Es importante que la IP que asignemos a la máquina no esté en rango de direcciones dentro de la configuración de la subred.

Otro truco para lograr reasignar una IP a un PC que la ha cambiado es poner las direcciones temporalmente de forma manual con el método que acabamos de describir en los dos PC involucrados y hacer que tomen la IP del servidor DHCPD (reiniciando la red). A continuación podemos quitar la asignación manual y reiniciamos de nuevo la red para que pida la IP que acaba de recibir.

3.12 HERRAMIENTAS DE SEGURIDAD

Linux es reconocido como uno de los sistemas operativos de mayor fiabilidad a la hora de concentrarnos en la seguridad de nuestros sistemas. Los servicios que ofrecen gozan de excelentes críticas. El servidor de páginas web Apache es por ejemplo el más usado en internet por su velocidad y seguridad.

Gnu/Linux dispone de un grupo de herramientas de alerta en casos de ataque, diagnosticando el tipo y actuando en consecuencia, pudiendo de esta forma armar esquemas de seguridad reduciendo al mínimo la posibilidad de ser vulnerados.

¿Por que utilizar herramientas de seguridad en los sistemas Linux? Ningún sistema operativo se puede considerarse `seguro' tal y como se instala por defecto; normalmente, cualquier distribución de un sistema se instala pensando en proporcionar los mínimos problemas a un administrador que desee poner la maquina a trabajar inmediatamente, sin tener que preocuparse de la seguridad. Es una cuestión de puro marketing: imaginemos un sistema Linux que por defecto se instalara en su modo mas restrictivo en cuanto a seguridad; cuando el administrador desee ponerlo en funcionamiento conectándolo a una red, ofreciendo ciertos servicios, gestionando usuarios y periféricos deberá conocer muy bien al sistema, ya que ha de dar explícitamente los permisos necesarios para realizar cada tarea, con la consiguiente perdida de tiempo. Es mucho más productivo para cualquier empresa desarrolladora de sistemas proporcionarlos completamente abiertos, de forma que el administrador no tenga que preocuparse mucho de como funciona cada parte del sistema que acaba de instalar: simplemente inserta el CDROM original, el software se instala, y todo funciona a la primera, aparentemente sin problemas.

Esta política, que lamentablemente siguen casi todas las empresas desarrolladoras, convierte a un sistema Linux que no se haya configurado mínimamente en un fácil objetivo para cualquier atacante. Para verificar ataques existen los logs de transacciones (“/users/logs/squid/access.log”)

Es más, la complejidad de Linux hace que un administrador que para aumentar la seguridad de su sistema se limite a cerrar ciertos servicios de red o detener algunos demonios obtenga una sensación de falsa seguridad: esta persona va a pensar que su sistema es seguro simplemente por realizar un par de modificaciones en el, cosa que es completamente falsa.

3.13 CONTROL DE ANTIVIRUS, FILTRADO, ANTISPAM

- **CONTROL DE ANTIVIRUS**

1. Linux es un sistema bastante seguro. Sólo por desconocimiento o imprudencia, se podría colar un virus en nuestro sistema;
2. El mejor antivirus que existe hoy en día es usar linux, y a ser posible en cuanto estemos familiarizados con los programas que habitualmente necesitamos usar sólo linux.

Linux no tiene ningún solo virus (hubo dos experimentos - propiamente no eran virus - pero de "laboratorio"). Linux no necesita usar antivirus para su propio sistema (sí, para detectar virus en archivos con destino a su ejecución por parte de otros sistemas).

Actualmente (tampoco en el pasado) Linux no tiene ningún virus. Posiblemente, por la razón de que es difícil que pueda tenerlos, porque significaría no tomar unas mínimas medidas de control o seguridad, de acuerdo al uso que cada cual pueda hacer de su sistema.

Son importantes otras cuestiones, pero fundamentalmente cuatro aspectos:

1) En su concepción, LINUX ES UN SISTEMA MUY SEGURO. Sólo hay un usuario que lo puede todo, se llama "root". El resto de los usuarios del sistema tienen los privilegios disminuidos, a no ser que el usuario root les conceda otros. Su acceso debe hacerse siempre por contraseña, y que no lo vamos a utilizar normalmente, pues para nuestro trabajo habitual entraremos como un usuario con pocos privilegios desde el punto de vista de la administración del sistema. Las contraseñas que utilizaremos serán difícil de adivinar o comprobar (nunca palabras de diccionario, o como mínimo, deberían ir acompañadas de otros signos). Incluso podemos cambiarlas periódicamente. Además podemos hacer que sea realmente difícil y larga de teclear (por ejemplo, mediante su encriptación mediante MD5). En fin, los usuarios normales y corrientes no tenemos grandes secretos que guardar.

2) LA COMUNIDAD LINUX ES UNA COMUNIDAD VIGILANTE DEL ORIGEN DE LOS PROGRAMAS. Los programas que se instalan en linux deben proceder de fuentes totalmente fiables. En las instalaciones se recomienda utilizar, siempre que sea posible, la versión en código fuente (lo que escribe el programador) de los programas. DISPONIBILIDAD DEL CÓDIGO FUENTE: que los programas sean examinados por los que tienen suficientes conocimientos, los desarrolladores y la comunidad linuxera en general. ¿Cómo alguien puede insertar código malicioso si existen unos procedimientos de control y en el supuesto de que estos se apliquen?. El riesgo aquí podría ser instalar programas de los que no existe la posibilidad de disposición del código fuente. El acceso al código fuente dificulta enormemente - impide - ocultar código malicioso en los programas. Eso significa, en principio, que no se puede meter código oculto, aunque evidentemente puede insertarse código malicioso, intencionada. Pero si a pesar de las precauciones, adicionalmente se efectúan pruebas y tenemos monitorizado el sistema para que nos informe de qué ocurre, teóricamente estaremos en condiciones de detectar cualquier "anomalía" inmediatamente. Esto no significa que todos sepamos hacer eso, pero bueno: los que saben y se dedican a ello pueden controlarlo y comentarlo a los usuarios. Si hay algún peligro, lo veo más del lado de la permisión de la no disponibilidad del código fuente en paquetes con licencia Librería (licencia que permite a empresas o particulares proporcionar ya compilados los binarios de un programa y reservarse el código fuente...). Sabiendo esto se pueden tomar un mínimo de precauciones.
3) Tener una política de usar VERSIONES DE PRODUCCIÓN (versiones estables y comprobadas), y junto a ello una política de ACTUALIZACIÓN de versiones de nuestros programas para corregir y evitar los "bugs" o errores. También es posible usar versiones inestables y de pruebas. Por ejemplo, quienes usan lo último que sale al mercado están utilizando este último tipo de versiones. Por supuesto, ejecutar (instalar con privilegios root) CUALQUIER COSA que nos llegue por internet puede ser peligroso. Precaución entonces ante las técnicas de "ingeniería social", pues si mandan un script que no tengo ni idea de lo que hace...podría tener problemas.

4) SEGURIDAD DEL SISTEMA. Estar dispuestos a aprender todos los días algo más sobre nuestro sistema, y así podremos tener una visión clara de todos los aspectos que pueden afectar a nuestro sistema. Por ejemplo, ¿cómo EVITAR UNA ESCALADA DE PRIVILEGIOS por parte de un usuario en nuestro sistema?. Si conocemos las tácticas que pueden usarse para una escalada, inmediatamente tomaremos las medidas adecuadas que impedirán ninguna escala: [nuestro sistema ¿puede notificarnos los intentos de intrusión fallidos?; ¿podemos incrementar geométricamente el tiempo de acceso tras intentos de intrusión fallidos, y por lo tanto deshabilitar al crackeador de contraseñas más persistente?; ¿podemos llevar un registro de intentos de acceso no autorizados?; ¿es posible que pueda bloquearse el acceso ante un determinado número de intentos?; ¿podríamos conseguir recibir una notificación de detección de intentos de intrusiones o de entradas a través de nuestro teléfono móvil para tomar inmediatamente medidas?; ¿podemos conseguir que nuestro sistema no arranque sino es con nuestro propio CD custodiado bajo llave?, etc., etc...]

El mejor antivirus es un usuario responsable, en linux no existe la palabra virus en sí, sino desconocimiento de las cosas.

Si instala programas de fuentes seguras (no de softonic por ejemplo) linux funcionara siempre bien. NO necesita ningún antivirus, puede necesitar un cortafuegos pero no es tan imprescindible como en windows.

La verdad no creo, que linux sea vulnerable a un virus y las razones en las que me baso son las siguientes:

1. Tendrían que hacer un virus que gane acceso como root automáticamente.
2. Incluso siendo root tendría que saltarse una gran cantidad de permisos.
3. Esconder los procesos que se estén ejecutando.
4. Prácticamente ningún linux es igual, por lo tanto el virus funcionaria en algunas maquinas y en otras no.

- **CONTROL DE FILTRADO**

Su funcionamiento es generalmente muy simple: se analiza la cabecera de cada paquete y en función de una serie de reglas ya establecidas, la trama es bloqueada o se le permite continuar.

El mecanismo de filtrado puede considerarse como una malla que retiene ciertos paquetes no deseados. Lo más importante es encontrar el tamaño adecuado del mallado, así como el lugar donde ponerla.

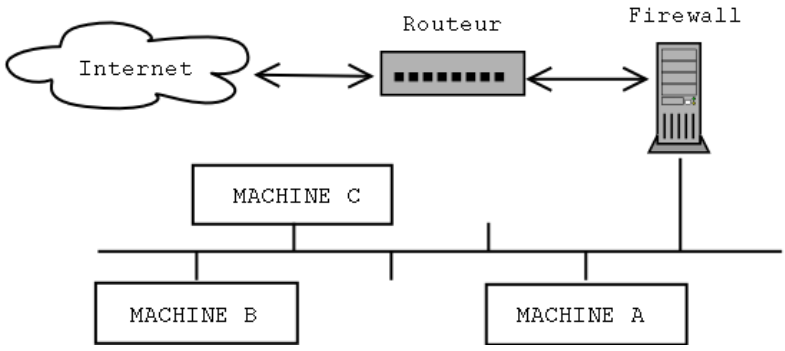


Figura 3.9

Para poder filtrar apropiadamente los paquetes, el mecanismo de filtrado debe intercalarse físicamente entre la red a proteger y el "resto del mundo". En la práctica, esto se hace con una máquina que tenga dos interfaces de red (normalmente Ethernet), una conectada a la red interna y la otra al router (encaminador) que permite el acceso al exterior. De esta forma, las comunicaciones pasarán obligatoriamente por el cortafuegos que las bloqueará o no según su contenido.

La máquina con el mecanismo de filtrado se puede configurar de 3 formas diferentes:

- gateway (pasarela) "simple": es la configuración más habitual. La máquina se utiliza como una pasarela entre dos redes o subredes. Las computadoras en la red local se deben configurar para usar el cortafuegos, en vez del router, como su ruta por defecto.
- pasarela "Proxy-ARP": la configuración anterior implica la división de la red en dos subredes, con lo que se pierde la mitad de las direcciones IP disponibles,

desperdiciándose un bit. Como ejemplo, en una subred con 16 direcciones (con una submáscara de 28 bits), sólo 14 estarán disponibles, ya que dos direcciones son para la red y el broadcast. Añadiendo 1 bit a la máscara de subred, bajamos de 14 a 6 direcciones disponibles (8 IPs menos las direcciones de red y broadcast). Cuando no se puede perder la mitad de las IPs disponibles se utiliza esta técnica. Además, esta técnica no requiere ningún cambio en la configuración de red de las máquinas existentes, ni del router, ni de las computadoras protegidas.

- puente Ethernet (Ethernet bridge): instalando una pasarela Ethernet (no una pasarela IP) se consigue un mecanismo de filtrado invisible desde otras máquinas. Esta configuración se puede llevar a cabo sin asignar direcciones IP a las interfaces Ethernet. La máquina se convierte en indetectable mediante ping, traceroute, etc.

- **REGLAS BÁSICAS DE FILTRADO**

  Ahora que sabemos dónde instalar nuestro filtro, debemos definir que tendrá que bloquear o qué aceptar.

  Existen dos formas de configurar el filtro:

  - La buena: no se permite pasar a ningún paquete, a no ser que lo autorice explícitamente alguna regla.
  - La mala: (desgraciadamente, usada a menudo) los paquetes explícitamente prohibidos se paran, todos los demás se aceptan.

Es sencillo explicarlo: en el primer caso, olvidar una regla lleva a que un servicio no funcione apropiadamente o no funcione en absoluto.

En el segundo caso, olvidar una regla crea una vulnerabilidad potencial que puede ser difícil de encontrar... si la encontramos.

- **NETFILTER**

  La aplicación de filtrado más utilizada con Linux 2.4 es Netfilter; reemplaza con creces a ípchains, utilizada con los núcleos Linux 2.2. Netfilter tiene dos partes: un componente del núcleo que debe compilarse en el núcleo y el comando iptables.

- **ANTISPAM**

La protección Anti-Spam se logra mediante un efectivo análisis de “Listas negras” y comparaciones de muestras de mensajes (actualizadas desde Internet) así como del contenido de todos los mensajes entrantes. El programa filtra los mensajes que no se desean recibir (correo no solicitado o spam) antes que éstos lleguen a los buzones de correo. El Anti-Spam puede usarse como filtro en cualquier sistema de correo (como Senmail, Qmail, Postfix y MS Exchange) en el propio servidor de correo o en una computadora remota.

- **POLÍTICA "PERMISIVIDAD BAJA + LISTAS BLANCAS"**

  La idea que está detrás de esta política de uso de filtros de correo consiste en ser muy estricto en lo que marcamos como spam, de modo que en principio quedarían marcados mensajes que en realidad son lícitos (puede darse el caso de que un mensaje que no es spam cumpla ciertos patrones comunes en los correos no deseados, es algo más frecuente de lo que parece). Para evitar que esos mensajes se nos marquen como spam podemos incluir una regla personal del tipo '*Aceptar Correo Desde*', de modo que nos llegarían con total normalidad a nuestro buzón de entrada.

  Y con esto ya tendremos el sistema antispam configurado siguiendo la política de rechazar por defecto todo lo que parezca spam, aceptando explícitamente los mensajes que provengan de aquellas personas que nosotros deseemos.

- **POLÍTICA "PERMISIVIDAD ALTA + LISTAS NEGRAS"**

  En este caso la idea es la contraria a la política anterior; ahora lo que queremos es ser más permisivos con el spam, arriesgándonos a que nos entre algo en el buzón de

entrada, procediendo a bloquear las direcciones que más correo basura nos manden. Con esto se hace realmente difícil que un correo lícito sea marcado como basura, si bien será necesario un poco más de trabajo por nuestra parte para que no nos llegue tanto spam a la carpeta '*INBOX*'.

De este modo, y tras algún tiempo configurando las reglas de rechazo tendríamos el sistema antispam configurado de tal modo que si bien podría entrarnos algo de correo basura a la carpeta de entrada, sería poco, y sin embargo resulta realmente difícil que un correo lícito sea marcado como spam.

3.14 SEGURIDAD EN LOS SERVICIOS

Describir todos los servicios existentes en la red e internet y la manera de controlar los servicios como? Negando a 1 o todos los usuarios, o mediante listas de control.

Cuando un servicio se hace accesible a la red, asegúrese de darle el “menor privilegio”, lo que quiere decir que no se permita hacer cosas que no son imprescindibles para que trabaje como se diseño. Por ejemplo, deberá hacer sus programas con setuid root o alguna otra cuenta privilegiada solo si realmente lo necesitan. También, si quiere usar un servicio solo para una aplicación muy limitada, no dude en configurarla tan restrictivamente como su aplicación especial lo permita. Por ejemplo, si quiere permitir a maquinas sin disco arrancar desde su maquina, debe facilitar el TFTP (Trivial File Transfer Service) de modo que pueda obtener los ficheros de configuración básicos del directorio /boot. Sin embargo, cuando se usa sin restringir, TFTP permite a cualquier usuario de cualquier lugar del mundo leer cualquier fichero de su sistema. Si esto no es lo que desea, por qué no restringir el servicio TFTP al directorio /boot?

Pensando en la misma línea, podrá restringir ciertos servicios a usuarios que acceden desde ciertos nodos, digamos que solo para su red local.

Otro punto importante es evitar software “peligroso”. Claro que cualquier software que utilice puede ser peligroso, porque el software puede tener fallos que algunos listos pueden explotar para acceder a su sistema. Cosas como esta ocurren, y no hay protección

segura contra ello. Este problema afecta al software libre y a productos comerciales por igual.

Sin embargo, programas que requieren privilegio especial son inherentemente más peligrosos que otros, ya que un agujero de estos puede tener consecuencias drásticas. Si instala un programa setuid con propósitos de red, sea doblemente cuidadoso y no deje de leerse toda la documentación, de modo que no cree una brecha en la seguridad por accidente.

Nunca olvide que sus precauciones pueden fallar, por muy cuidadoso que haya sido.

Por eso deberá asegurarse de que detecta pronto a los intrusos. Comprobar los ficheros de actividad es un buen comienzo, pero el intruso probablemente sea bastante listo, y borrara cualquier huella que haya dejado. Sin embargo, hay herramientas como tripwire que permite comprobar ficheros vitales del sistema para ver si sus contenidos o permisos han cambiado. tripwire realiza varios checksums fuertes sobre estos ficheros y los almacena en una base de datos. En las siguientes ejecuciones, se reevalúan y comparan los checksums con los almacenados para detectar cualquier modificación.

CAPITULO IV

4.1 ÁMBITO DESIGNADO A ESTUDIAR.

4.1.1. ANTECEDENTES DEL CYBER CAFÉ W&M NEGOCIOS NET

Desde el año 2001, el Cyber Café W&M Negocios Net, presta sus servicios a la colectividad latacungueña para satisfacer la demanda del sector productivo del país y las necesidades de la población.

Cyber Café W&M Negocios Net, es un establecimiento privado, líder en la zona central del país, creado en agosto del 2001, ofrece a la colectividad el servicio de Internet, correo, chat y asesoramiento informático.

- **VISIÓN**

  Ser una microempresa líder, integrada al desarrollo científico, educativo y productivo a nivel provincial.

- **MISIÓN**

  "GENERAR, DIFUNDIR Y APLICAR EL CONOCIMIENTO PARA PROMOVER EL DESARROLLO Y BIENESTAR DE LA SOCIEDAD LATACUNGUEÑA"

Mediante la prestación del servicio de Internet a la colectividad, se enfoca fomentar a través de la investigación el conocimiento.

4.1.2 ANTECEDENTES DEL AREA ADMINISTRATIVA DEL CYBER CAFÉ W&M NEGOCIOS NET

El Área administrativa del Cyber café W&M Negocios Net, funciona desde el mes de agosto del año 2001, se creo con el objetivo de proporcionar el servicio de Internet.

Para su operación se inicio con un servidor Clon Pentium IV, el mismo que distribuía Internet a sus 3 terminales.

Su proveedor de Internet desde su inicio fue ANDINANET con el servicio Dial-up de 56kbps.

En la actualidad cuenta con 1 servidor clon 386, el proveedor de Internet es ANDINANET, proporcionando el servicio ADSL de 128Kpbs.

El Sistema Operativo con el cual opera es Windows Xp, el mismo que esta instalado en las cuatro maquinas.

Cuenta con 2 impresoras de inyección a tinta, instaladas en el servidor, a las cuales se puede acceder desde los terminales.

La configuración de la red esta estructurada como una red de oficina, la misma que comparte recursos a los usuarios.

Los servicios se hallan concentrados en el servidor:

- Consultoría
- Internet

4.2 ESTUDIO DE LAS POLÍTICAS DE SEGURIDAD ACTUALES

Actualmente no se cuenta con políticas establecidas y documentadas, mas la única política de seguridad es el Software ANTIVIRUS NORTON el mismo que es una copia adquirida sin licencia, éste es un problema de alto riesgo ya que al ser una microempresa que está expuesta al público debería contar con las licencias respectivas de todo el software, de acuerdo a la legislación de software propietario estaría infringiendo en una acción penal. Además de las configuraciones a través de la conexión a Internet.

El servidor de Internet está expuesto a personas que por desconocimiento pueden dejar inactivo el servicio, se debe considerar que para evitar cualquier inconveniente se debe buscar otro lugar o a su vez aplicar un mecanismo que evite esta situación.

4.3 SEGURIDADES APLICABLES PARA LA RED MEDIANTE EL MODELO OSI.

Las seguridades que se considera aplicar mediante el Modelo OSI, serán de acuerdo a la posibilidad de ejecutarse en cada nivel del modelo OSI.

Mediante la utilización de un Firewall se consideran la seguridades que actúan en los niveles 3 (red) a 7 (aplicación) del Modelo OSI. Sus funciones son básicamente las siguientes:

- Llevar contabilidad de las transacciones realizadas en la red.
- Filtrar accesos no autorizados a máquinas (mediante filtrado de paquetes, o bien observando el contenido de las unidades de protocolo de Transporte, Sesión, Presentación, y aplicación).
- Alertar en caso de ataques o comportamiento extraño de los sistemas de comunicación.

A continuación se especifica las seguridades lógicas aplicadas en cada una de las capas del modelo OSI:

- **CAPA FISICA:** No es posible aplicar seguridades en este nivel debido a que las seguridades a aplicarse son lógicas y además este nivel se encarga de las conexiones físicas de la computadora hacia la red.
- **CAPA DE ENLACE:** A éste nivel no es posible aplicar seguridades lógicas ya que éste nivel opera a través del subnivel de acceso al medio el mismo que formar parte de la propia tarjeta de comunicaciones, mientras que el subnivel de enlace lógico estaría en el programa adaptador de la tarjeta (*driver* en inglés); por lo tanto volvemos a tratar con hardware.
- **CAPA DE RED:** En este nivel la seguridad que se aplica es el control de congestión del tráfico en la red, se controla evitando el uso desmesurado del ancho de banda a través de listas de acceso (acl *Acces Control List*), configuradas en el Squid.
- **CAPA DE TRANSPORTE:** Este nivel es el encargado de verificar que los datos se transmitan en forma segura, que lleguen correctamente al otro lado de la comunicación. Para lograr que la transmisión de información a este nivel sea segura se ha implementado el uso del protocolo SSH, éste protocolo sirve para acceder a máquinas remotas a través de una red, de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión.

- **CAPA DE SESIÓN (abrir sesiones de trabajo con usuarios autenticados):** La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo y procedan al intercambio de datos.

  Sus principales funciones son:

  - Establece, administra y finaliza las sesiones entre dos hosts que se están comunicando.
  - Si por algún motivo una sesión falla por cualquier causa ajena al usuario, restaura la sesión a partir de un punto seguro y sin perdida de datos o si esto no es posible termina la sesión de una manera ordenada chequeando y recuperando todas sus funciones, evitando problemas en sistemas transaccionales.
  - Se ocupa de las funciones de gestión de red que incluyen contraseñas, monitorización e información de la red.

La capa de sesión tiene la responsabilidad de asegurar la entrega correcta de la información a la siguiente capa (capa de presentación). Esta capa tiene que revisar que la información que recibe sea correcta. Para esto la capa de sesión debe realizar algunas funciones:

- **ELECCIÓN DE CLAVES**

El primero es que somos bastante poco imaginativos a la hora de idear las claves de acceso. Algunos olvidadizos incluso las anotamos cerca del equipo, o utilizamos datos que fácilmente se pueden relacionar con nosotros.

El segundo y más peligroso, es que se puede acceder como usuario root desde el propio gestor de arranque. GRUB permite acceder como root editando la entrada en el menú (pulsar e sobre la entrada seleccionada) y añadiendo single. Esta acción de editar el menú de GRUB puede protegerse mediante una contraseña desde el propio shell de GRUB

Para solucionar en parte este problema se han utilizados los beneficios que ofrece MD5. En sistemas UNIX y GNU/Linux se utiliza el algoritmo MD5 para encriptar las claves de los usuarios. En el disco se guarda el resultado del MD5 de

la clave que se introduce al dar de alta un usuario, y cuando éste quiere entrar en el sistema se compara la entrada con la que hay guardada en el disco duro, si coinciden, es la misma clave y el usuario será autenticado. He ahí el problema de encontrar y generar colisiones de *hash* a voluntad.

El MD5 también se puede usar para comprobar que los correos electrónicos no han sido alterados usando llaves públicas y privadas.

- **CAPA DE PRESENTACION**

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del diálogo. *Su tarea principal es aislar a las capas inferiores del formato de los datos de la aplicación, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red.*

En ésta capa no podemos apreciar la aplicación de seguridades ya que no existe una aplicación que se ejecute en el entorno Linux.

- **CAPA DE APLICACIÓN**

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y está relacionada con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales.

En esta capa las seguridades aplicadas, se encuentran en los siguientes servicios:

- **VSFTPD**

Se hace uso del demonio vsftpd para establecer transmisión de archivos de forma segura. Lo que permite que los datos lleguen a su destino de forma rápida y segura.

Very Secure FTP Daemon es un software utilizado para implementar servidores de archivos a través del protocolo FTP. Se distingue principalmente

porque sus valores por defecto son muy seguros y por su sencillez en la configuración, comparado con otras alternativas como Wu-ftpd. Actualmente se presume que VSFTPD es quizá el servidor FTP más seguro del mundo.

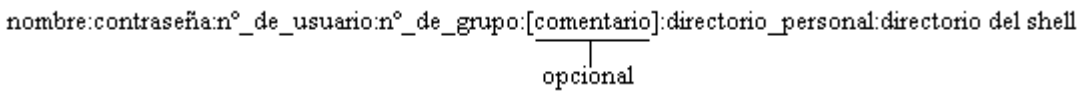
- **SENDMAIL**

A través de sendmail podemos establecer el envío de correo entre host, además de establecer seguridades que impidan que el correo sea interceptado por personas ajenas a nuestra red, para se hace uso del servicio que ofrece MD5 encriptando las claves de los usuarios.

4.4 ADMINISTRACIÓN DE LOS USUARIOS DE LA RED.

La administración de usuarios de la red esta basada en la distribución de Internet y el acceso a los recursos con los que cuenta el servidor, prácticamente no cuenta una administración responsable de los recursos que ofrece a los usuarios, en conclusión existe un mal uso de los recursos de la red.

Se propone que la administración de usuarios solamente la puede ejercer el administrador o root o usuario administrador; debido que Linux es un sistema operativo multiusuario podrá trabajar con múltiples usuarios para los cuales debe tener una correcta administración. Cada vez que damos de alta a un usuario creamos un registro en el fichero **passwd** del directorio **etc**, con la información más relevante de ese usuario; los campos que presentan son:



Para dar de alta a un usuario o modificar sus datos podemos entrar con un editor en este fichero y modificar alguno de los campos y la otra forma podemos utilizar los comandos específicos de Linux para la administración de usuarios.

Se puede administrar usuarios en modo texto utilizando comandos y se puede también administrar usuarios en modo grafico utilizando determinadas utilidades de Linux.

El entorno de cada usuario se crea copiando algunos ficheros en el momento de dar el alta. Cada vez que un usuario se presenta al sistema se ejecutan dos archivos de guiones o scripts; el primero de ellos es el script **profile** o llamado también perfil del sistema, es un fichero común a todos los usuarios que configura el entorno de todos ellos, se encuentra en el directorio etc y el otro fichero guión o script, es el fichero fichero **.bash_profile**, que configura el entorno de cada uno de los usuarios. Cada usuario tiene el suyo e incluso puede modificarlo, cada vez que el usuario se da de alta es copiado junto con el **.bashrc**, **bashlogout** .... desde el directorio /etc/skel .

Una de las tareas más importantes de cualquier administrador del sistema, es la de administrar adecuadamente usuarios y grupos, así como asignar y revocar permisos.

4.5 DETECCIÓN DE FALLAS Y COLISIONES EN LA RED.

El problema detectado es la lentitud en el acceso a la navegación en Internet, ya que se cuenta con una conexión dial-up provocando demora en el acceso a Internet.

Un problema crucial es que constantemente los virus afectan a la velocidad en los procesos que se ejecutan en la red, por ejemplo al abrir aplicaciones, imprimir, etc.

Las colisiones son imperceptibles ya que al ser una red pequeña no es posible visualizar la congestión, en donde si se puede verificar la congestión es en el acceso a Internet por la navegación que se hace lenta al contar con servicio dial-up.

Para controlar este problema se ha configurado un iptables que ayudara a resolver el problema de navegación, con el uso del mismo podremos controlar el ancho de banda, y además se evitará el ataque de virus, troyanos, gusanos, etc.

Con estas implementaciones la red en sí no se ha visto afectada por fallas y colisiones, ya que una de las ventajas al utilizar el servidor Linux como servidor de Internet brinda la facilidad de ahorrar la utilizaron del ancho de banda, pues en el momento que uno de los usuarios accede a alguna pagina esta es resuelta en el menor tiempo posible si otro usuario accede a la misma, esto beneficia mayormente la rapidez en la navegación.

4.6 PROBLEMAS ENCONTRADOS

Los problemas que afectan al funcionamiento adecuado de la red se los identifica en los siguientes aspectos:

- **HARDWARE:**

  Problemas de hardware se han encontrado pero no son tema de estudio, y por citar anotaremos el principal:

  - No existe una planificación en el cableado de la red.

- **SOFTWARE**

  - El Sistema Operativo que está en funcionamiento no satisface las necesidades para las cuales se programó su utilización.
  - Navegación lenta.
  - Ataques continuos de virus, troyanos, gusanos, etc.
  - Alteración en las configuraciones por parte de los usuarios.
  - No existe control de ancho de banda.
  - No existen seguridades que garanticen la integridad de la red.
  - Falta controlar el acceso de los usuarios a la red.
  - Riesgo en la pérdida de información o configuraciones.
  - No cuenta con políticas de seguridad (básicas)

- **ADMINISTRACIÓN**

  - Falta de políticas en la administración de la red, que sean de conocimiento de quien administra.
  - No existe una planificación de actualización del personal.

4.7 ESTRATEGIAS DE SOLUCIÓN EN LA RED.

Una vez establecidas los problemas de la red, se propone la solución a los mismos, en los siguientes aspectos:

- **HARDWARE**

  A nivel de hardware no se cita ninguna solución, como ya se indicó este aspecto no contempla el tema en estudio.

- **SOFTWARE**
  - Se cambió de Sistema Operativo, implementándose el software libre en su versión LINUX ENTERPRISE EDITION V.4.
  - Para solucionar la congestión en la navegación se cambio el acceso a Internet con la instalación del servicio ADSL de 128/64 KBPS. Andinatel es el proveedor del servicio.
  - El aspecto de virus y spam está controlado con Clamav y Spamassassin.
  - Los host han sido configurados como usuarios con restricciones, lo cual evitará la alteración en las configuraciones.
  - El control de ancho de banda se controla a través del proxy Squid.
  - Se han implementado reglas que permiten establecer seguridades a través del firewall, esto es habilitando servicios y puertos necesarios.
  - Para controlar el acceso a la red por parte de los usuarios, se usa ETHERREAL, que nos permite visualizar los host que se encuentran en la red y el flujo en la navegación.
  - Los passwords son encriptados con el algoritmo MD5.
  - Creación de un Usuario Administrador para evitar la pérdida de información o configuraciones.
- **PARA LA PARTE ADMINISTRATIVA,** se ha desarrollado un manual de políticas de seguridad en el cual se indica las alternativas para poder enfrentar posibles problemas en la red.

A través de estos componentes hemos logrado controlar los problemas que permiten operar en forma eficiente y brindar el servicio a los usuarios en forma óptima y oportuna; y a la vez permite una correcta operación del servidor el cuál estará operando constantemente y brindando seguridad.

4.8 PREVENCIÓN DE FALLAS EN LA RED

Para prevenir fallas en la red se ha considerado la utilización de Linux controlando los siguientes aspectos:

- **HARDWARE**

  Para prevenir fallas en la red a nivel de hardware, no se trata este aspecto, ya que no es considerado en el tema de estudio.

- **SOFTWARE**

  Para prevenir fallas en la red se han implementado seguridades utilizando los siguientes servicios que permiten el funcionamiento óptimo:

  - Instalacion de Linux Enterprise Edition V.4
  - Conexión ADSL.
  - Creación de un usuario administrador.
  - Los usuarios se han configurado con privilegio restringido.
  - Control de ancho de banda.
  - La configuración de un firewall.
  - Monitoreo de la red a través de ETHER REAL.
  - Uso del algoritmo criptografico MD5
  - Instalacion de antivirus y Antispam.

- **ADMINISTRACIÓN**

  En el aspecto de administración, se recomienda capacitación del personal a cargo de la red, especialmente en:

  - Administración de servidores Linux
  - Actualización de posteriores versiones de Linux.
  - Cableado estructurado
  - Redes

4.9 ESTABLECER POLÍTICAS DE SEGURIDAD PARA LA RED.

Otro aspecto muy importante de la administración de sistemas en un entorno de red es proteger al sistema y a sus usuarios, de intrusos. Los sistemas que son administrados descuidadamente ofrecen muchos huecos a los malintencionados: los ataques van desde averiguar las claves hasta acceder a nivel de Ethernet, y el daño causado puede ser desde mensajes de correo falsos hasta pérdida de datos o violación de la privacidad de los usuarios. Mencionaremos algunos problemas concretos cuando discutamos el contexto en el que pueden ocurrir, y algunas defensas comunes contra ellos.

En esta sección se comentarán algunos ejemplos y técnicas básicas para poder lidiar con la seguridad del sistema. Por supuesto, los temas relatados aquí no pueden tratar exhaustivamente todos los aspectos de seguridad con los que uno se puede encontrar; sirven meramente para ilustrar los problemas que pueden surgir. Por tanto, la lectura de un buen libro sobre seguridad es absolutamente obligada, especialmente en un sistema en red.

La seguridad del sistema comienza con una buena administración del mismo. Esto incluye comprobar la propiedad y permisos de todos los ficheros y directorios vitales, monitorizar el uso de cuentas privilegiadas, etc.

Cuando un servicio se hace accesible a la red, asegúrese de darle el “menor privilegio”. Esto significa, en una palabra que no se deberán permitir acciones que no son imprescindibles, para que se trabaje como se diseñó el servicio originalmente. También, si se quiere usar un servicio sólo para una aplicación muy limitada, el administrador del sistema no debe vacilar en configurar el servicio tan restrictivamente como la aplicación especial lo permita.

Pensando en la misma línea, se podría restringir ciertos servicios a usuarios que acceden desde ciertos nodos, digamos desde nuestra red local.

Otro punto importante a tener en cuenta es evitar software “peligroso”. Claro que cualquier software que se utilice puede resultar peligroso, dado que el software puede tener fallos que gente astuta pueda explotar para acceder a nuestro sistema. Cosas como ésta ocurren, y no hay protección segura contra ello. Este problema afecta al software libre y a

productos comerciales por igual. De cualquier modo programas que requieran privilegio especial son inherentemente más peligrosos que otros, ya que cualquier fallo aprovechable en éstos puede tener consecuencias desastrosas.

Otra fuente a considerar deberían ser aquellos programas que permiten registrarse en el sistema, o la ejecución de órdenes con autentificación limitada. Un método de autentificación se basa en la confianza del nombre del nodo llamado, el cual fue obtenido de un servidor de nombres, que pudo haber sido falseado. Hoy en día, debería ser una práctica común el reemplazar completamente los comandos **r** con la colección de herramientas **ssh**. Las herramientas **ssh** usan un método de autentificación mucho más confiable, además de proporcionar otros servicios como encriptación y compresión.

Nunca se debería de olvidar que nuestras precauciones pueden fallar, por muy cuidadosas que estas sean. Por eso se debería asegurar que la detección de los posibles intrusos es relativamente rápida. Comprobar los ficheros de actividad es un buen comienzo, pero el intruso probablemente sea bastante listo, y borrará cualquier huella que haya dejado.

4.9.1 CÓDIGO DE IPTABLES (POLÍTICAS)

```
#!/bin/sh
#
#
echo 1 > /proc/sys/net/ipv4/ip_forward
#
#
# service iptables save
#
#
IPTABLES="/sbin/iptables"
#
#
OUTSIDE=eth0
INSIDE=eth1
#
#
$IPTABLES -F
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT
$IPTABLES -F FORWARD
$IPTABLES -F -t mangle
$IPTABLES -F -t nat
$IPTABLES -X
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
#
#
$IPTABLES -t nat -A POSTROUTING -o $OUTSIDE -j MASQUERADE

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080 #
Redireccion al SQUID
```

```
iptables -A INPUT  -d 0.0.0.0 -p tcp --dport 25 -j ACCEPT # Mail Traffic
iptables -A INPUT  -d 0.0.0.0 -p tcp --dport 80 -j ACCEPT # HTTP Traffic
iptables -A INPUT  -d 0.0.0.0 -p tcp --dport 143 -j ACCEPT # HTTP Traffic
iptables -A INPUT  -d 0.0.0.0 -p tcp --dport 53 -j ACCEPT # DNS
iptables -A INPUT  -d 0.0.0.0 -p udp --dport 53 -j ACCEPT # DNS
iptables -A INPUT  -d 0.0.0.0 -p tcp --dport 110 -j ACCEPT # POP Traffic
iptables -A INPUT  -d 0.0.0.0 -p tcp --dport 1024: -j DROP # POP Traffic
iptables -A INPUT  -s 0.0.0.0 -p tcp --dport 1024: -j DROP # POP Traffic

iptables -A OUTPUT  -d 0.0.0.0 -p tcp --dport 1024: -j DROP # POP Traffic
iptables -A OUTPUT  -s 0.0.0.0 -p tcp --dport 1024: -j DROP # POP Traffic
iptables -A FORWARD  -d 0.0.0.0 -p tcp --dport 1024: -j DROP # POP Traffic
iptables -A FORWARD  -s 0.0.0.0 -p tcp --dport 1024: -j DROP # POP Traffic
```

4.9.2 NORMA ISO 17799

Para complementar las políticas aplicadas que garantizan las seguridades lógicas de la red, también se ha establecido políticas de Gestión de Seguridad de la Información basadas en la Norma ISO 17799 que garantiza la administración de políticas de Seguridad, se considera de vital importancia complementar la seguridad con esta Norma pues en cualquier Empresa es importante sustentar las infracciones en una base legal que permita actuar de forma inmediata con aquellos usuarios que no respeten las políticas emanadas.

La estructura de la normatividad de gestión en seguridad de sistemas de información, norma ISO 17799, queda especificada en diez componentes, que incluyen:

1) Política de seguridad
2) Organización de la seguridad
3) Control y clasificación de los recursos de información
4) Seguridad de personal
5) Seguridad física y del entorno
6) Manejo de las comunicaciones y las operaciones
7) Control de acceso
8) Desarrollo y mantenimiento de los sistemas

9) Gestión de continuidad de la empresa, y
10) Cumplimiento.

1. Política de seguridad

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DOCUMENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Un documento de políticas debe ser aprobado por el Gerente, publicado y comunicado, como también apropiado, para todos los empleados. La gerencia debe comprometerse y considerar la aceptación de la gestión de seguridad de información. Como mínimo, se debe incluir la siguiente guía:

- Una definición de seguridad de la información.
- Un informe del propósito de la Gerencia, apoyado en los objetivos y principios de seguridad de la información.
- Una breve explicación de las políticas de seguridad, principios, estándares y cumplimiento de requerimientos de particular importancia para la empresa, por ejemplo:

  a) Cumplimiento con la legislación y requerimientos contractuales.
  b) Requisitos de educación en seguridad.
  c) Prevención y detección de virus y otros software malignos.
  d) Gestión de continuidad de la empresa.
  e) Consecuencias de la violación de las políticas de seguridad.

- Una definición general y específica de las responsabilidades para la gestión de seguridad de la información.
- Documentos de referencia los cuales sirven de apoyo para las políticas y procedimientos.

REVISIÓN Y EVALUACIÓN

Las políticas deben tener un propietario quien es el responsable de su mantenimiento y revisión de acuerdo al proceso de revisión.

2. SEGURIDAD ORGANIZACIONAL

INFRAESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN

FOROS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es una responsabilidad compartida de la empresa por todos los miembros de la empresa. El foro puede ser parte de del cuerpo administrativo.

OUTSOURCING

REQUISITOS DE SEGURIDAD EN LOS CONTRATOS DE OUTSORUCING

Los requerimientos de seguridad de una organización outsourcing la administración y control de todos o algunos de los sistemas de información, redes y/o entorno de escritorio debe ser enviado en un contrato que este de acuerdo entre las partes.

3. CLASIFICACIÓN Y CONTROL DE LOS RECURSOS.

RESPONSABILIDAD DE LOS RECURSOS

INVENTARIO DE RECURSOS

Los inventarios de recursos ayudan a garantizar esa efectividad de protección de recursos toma lugar, y puede también ser requerida para otros propósitos comerciales, como salud y seguridad, razones seguras o financieras.

4. PERSONAL DE SEGURIDAD

DEFINICIÓN Y RECURSOS DE SEGURIDAD EN EL TRABAJO

INCLUSIÓN DE SEGURIDAD EN LAS RESPONSABILIDADES DEL TRABAJO

Los roles y actividades de seguridad, como extensión de políticas de seguridad de la información de la organización, deben ser documentadas en el momento oportuno. Se debe incluir cualquier responsabilidad general para implementación o mantenimiento de las políticas de seguridad así como especificar cualquier responsabilidad para la protección de recursos particulares, o para la exclusión de procesos y actividades de seguridad.

PROTECCIÓN Y POLÍTICAS DEL PERSONAL

Inspección permanente del personal, debe ser llevada la aplicación fuera del horario de trabajo.

ACUERDOS DE CONFIDENCIALIDAD

Acuerdos de confidencialidad o encubrimiento se usa para notificar que la información es confidencial o secreta. Los empleados normalmente deben firmar un convenio como parte inicial los términos y condiciones de su empleo.

Los convenios de confidencialidad deben ser revisados cuando hay cambios en los términos del empleo o contrato, particularmente cuando los empleados deben salir de la organización o cuando debe terminar el contrato.

CAPACITACIÓN DEL USUARIO

EDUCACIÓN Y CAPACITACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN

Todos los empleados de la organización y donde es pertinente, usuarios externos, deben revisar apropiadamente la capacitación y actualización regular en políticas y procedimientos organizacionales. Esto incluye requerimientos de seguridad, responsabilidad legal y controles comerciales, así como la capacitación en el uso correcto de recursos de procesamiento de la información, procedimientos, uso de paquetes de software, antes de acceder a la información o dar servicios.

5. SEGURIDAD FÍSICA Y DEL ENTORNO

ÁREAS DE SEGURIDAD

PERÍMETRO DE SEGURIDAD FÍSICA

La protección física puede ser alcanzada por la creación de varias barreras físicas en el entorno de las condiciones comerciales y recursos para el procesamiento de la información. Cada barrera establece un perímetro de seguridad. Las organizaciones deben usar perímetros de seguridad para proteger áreas que contienen recursos para el procesamiento de la información. Un perímetro de

seguridad es la construcción de una barrera, una pared, una tarjeta de control de entrada o el servicio de recepción.

CONTROLES FÍSICOS DE ENTRADA

Las áreas de seguridad deben ser protegidas por controles apropiados solo para permitir el acceso a personal autorizado.

SEGURIDAD DE OFICINAS, SALAS E INSTALACIONES.

Una área segura puede ser una oficina cerrada o varias salas dentro del perímetro de seguridad, los cuales pueden ser cerrados y pueden contener vitrinas con cerraduras o cajas fuertes. La selección y designación de áreas de seguridad deben tomar en cuenta la posibilidad de perdida por fuego, inundación, explosión y otras formas de desastre natural u ocasionado.

OPERACIÓN EN ÁREAS SEGURAS

Adicionalmente los controles y directrices pueden ser requerido para mejorar la seguridad. Estos controles incluyen para el personal o trabajadores contratados.

SEGURIDAD DE LOS EQUIPOS

MONTAJE Y PROTECCIÓN DEL EQUIPO

El equipo debe ser ubicado o protegido para reducir riegos desde amenazas y riesgos ambientales, y oportunidades para accesos no autorizados. Los siguientes controles deben ser considerados:

a) El equipo debe ser ubicado con mínimos accesos necesarios en áreas de trabajo.
b) El manejo de recursos sensibles de almacenamiento de datos y procesamiento de información deben ser ubicados para reducir el riesgo de descuido durante su uso.
c) Los artículos que requieren protección especial deben ser separados.

d) Los controles deben ser adoptados para minimizar el riesgo potencial de amenazas:

1) Robo,
2) Incendio,
3) Explosivos,
4) Humo,
5) Agua,
6) Polvo,
7) Vibración,
8) Efectos químicos,
9) Interferencia en el abastecimiento eléctrico,
10) Radiaciones electromagnéticas.

e) Una organización debe considerar estas políticas hacia comer, beber y fumar cerca de recurso para el procesamiento de información.
f) Las condiciones ambientales deben ser monitoreadas para condiciones que podrían afectar el funcionamiento de recursos para el procesamiento de información.
g) El uso de métodos espaciales de protección, como partes del teclado deben ser consideradas para ambientes de equipos industriales.
h) El impacto de los desastres que han sucedido en áreas cercanas, fuego en un piso del edificio, goteras en el tejado, o tierra en el piso, o una explosión en la calle debe ser considerada.

6. ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

CONTROLES EN LOS CAMBIOS OPERACIONALES

Los cambios en los recursos para el procesamiento de la información y sistemas deben ser controlados. Controles inadecuados de cambios en los recursos para el procesamiento de la información y sistemas es una causa común del sistema o fallas de seguridad. Los cambios en el desarrollo operacional pueden impactar en las aplicaciones.

PROCEDIMIENTOS DE ADMINISTRACIÓN DE INCIDENTES

Responsabilidades de administración de incidentes y procedimientos deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a incidentes de seguridad. Los siguientes controles deben ser considerados:

a) Los procedimientos deben ser establecidos para cubrir todos los potenciales tipos de incidentes de seguridad, incluyendo:
    1) Fallas en los sistemas de información y perdida de servicios;
    2) Daños de los servicios;
    3) Errores resultantes de datos comerciales incompletos o inexactos;
    4) Brechas de confidencialidad.
b) Además de los planes de contingencia normales, deben también cubrir los procedimientos:
    1) Análisis e identificación de las causas de los incidentes;
    2) Planificación e implementación de soluciones para prevenir la recurrencia, si es necesario;
    3) Recopilación de seguimientos de auditoria y evidencias similares;
    4) Comunicación con aquellos afectados o involucrados con la recuperación de incidentes;
    5) Información de la acción a las autoridades respectivas.
c) Los seguimientos de auditoria y evidencias similares deben ser recogidas y aseguradas como apropiadas para:
    1) Análisis de problemas internos;
    2) Uso como evidencia en relación a una brecha potencial de contratos, brechas de condiciones reguladoras o en los eventos de procedimientos civil

o criminal, por el mal uso de computadoras o legislación de protección de datos;

3) Negociación para la negociación de software y proveedores de servicio.

d) Acciones para recuperación de brechas de seguridad y corrección en las fallas del sistema debe ser controladas cuidadosa y formalmente. Los procedimientos deben asegurar que:

1) Solo el personal claramente identificado y autorizado están permitidos al acceso para los sistemas y datos;
2) Toda acción de emergencia tomada se documentará en detalle;
3) La acción de emergencia es reportada al administrador y revisada de manera ordenada;
4) La integridad de los sistemas comerciales y controles es confirmada con el menor retraso.

PROTECCIÓN CONTRA DAÑOS DE SOFTWARE

CONTROLES CONTRA DAÑO DE SOFTWARE

Los controles de detección y prevención para proteger contra software malicioso y apropiados procedimientos deben ser implementados. La protección contra software malicioso debe estar basada en conocimientos de seguridad, accesos apropiados al sistema, administración de control de cambios. Se deben considerar los siguientes controles:

a) Cumplimiento de requerimientos de una política formal con software autorizado, y probabilidad de uso de software no autorizado.
b) Una política formal para protección contra riesgos asociados con la obtención de archivos y cualquier software o vía externa de la red, o en cualquier otro medio, indicando que medios proteger.
c) Instalación y actualización regular de antivirus detección y reparación de software para escanear computadoras y cada medio como medida de precaución o una rutina básica.
d) Llevar revisiones regulares del software y el contenido de datos del sistema de apoyo para procesos críticos.

e) Chequear cualquier archivo en medios electrónicos de origen dudoso o no autorizado, o archivos recibidos de intrusos de la red.
f) Administrar procedimientos y responsabilidades de distribución el sistema de protección de virus, capacitación en su uso.
g) Planes apropiados de continuidad del negocio para recuperarse de ataques de virus, incluyendo todos los datos necesarios y respaldo de software y órdenes de recuperación.
h) Los procedimientos para verificar toda la información relacionada con software malicioso, y asegurar que los comunicados de advertencia sean precisos e informen.

Estos controles con especialmente importantes para redes que soportan servidores de archivos con varias estaciones de trabajo.

ADMINISTRACIÓN INTERNA
REGISTRANDO ERRORES

Los errores deben ser reportados y tomar acciones correctivas. Los errores reportados por usuarios con respecto a problemas con el procesamiento de información o sistemas de comunicación deben se registrados. Debe haber reglas claras para manejar reporte de fallas que comprenden:

a) revisión de registros de error para garantizar que los errores han sido resueltos satisfactoriamente;
b) revisión de medidas correctivas para garantizar que los controles no han sido comprometidos y que las acciones tomadas son completamente autorizadas.

ADMINISTRACIÓN DE LA RED
CONTROLES DE LA RED

Un rango de controles es requerido para conseguir y mantener la seguridad en las redes computacionales. El administrador de red debe implementar controles para garantizar la seguridad de los datos en la red y la protección de servicios

conectados desde accesos no autorizados. En particular los siguientes controles deben ser considerados:

a) La responsabilidad operacional de redes debe ser separada de operaciones computacionales.
b) Las responsabilidades y procedimientos para la administración de equipos remotos, incluyendo el equipo en áreas de usuarios,
c) Si es necesario controles especiales deben ser establecidos para salvaguardar la confidencialidad e integridad de datos que pasan sobre redes públicas, y para proteger sistemas asociados.
d) Las actividades del administrador deben ser estrechamente coordinadas para optimizar los servicios de la empresa y para asegurar que los controles son consistentemente aplicados sobre la infraestructura de procesamiento de la información.

INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

CONVENIOS CON EL INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

Algunos convenios pueden ser formales, incluyendo software propietario, debe ser establecido para el intercambio de información y software entre organizaciones. Los convenios de seguridad deben considerar las siguientes condiciones:

a) Administración de responsabilidades para controlar y notificar la transmisión.
b) Procedimiento para enviar notificaciones, transmisión, despacho y recepción.
c) mínimos estándares técnicos para empaquetado y transmisión.
d) Responsabilidades y obligaciones en eventos de pérdida de datos.
e) Normas técnicas para registrar y leer información del software.
f) Cualquier control especial que pueda ser requerido para proteger elementos sensibles, como claves de criptografía.

SEGURIDAD EN EL CORREO ELECTRÓNICO

RIEGOS DE SEGURIDAD

El correo electrónico esta siendo usado para comunicaciones comerciales, reemplazando formas tradicionales de comunicación como telex y cartas. Los riesgos de seguridad incluyen:

a) Vulnerabilidad de mensajes para accesos no autorizados, modificaciones o daños de los servicios.
b) Vulnerabilidad de errores, direcciones incorrectas, y en general fiabilidad y disponibilidad de los servicios.
c) Consideraciones legales como la necesidad potencial de pruebas de origen, destino y aceptación.
d) Implicaciones de publicar las listas acceso externas del personal.
e) Controlando el acceso del usuario remoto a las cuentas de correo electrónico.

POLÍTICAS DE CORREO ELECTRÓNICO

Las organizaciones preparan políticas claras con respecto al uso del correo electrónico, incluyen:

a) Ataques en el correo electrónico, virus, intercepción.
b) protección de cadenas de correo de electrónico.
c) Directrices de cuando no usar el correo electrónico.
d) Uso de técnicas criptográficas para protección de confidencialidad e integridad de mensajes electrónicos.
e) Controles adicionales para reconocer mensajes que no han sido autenticados.

7. CONTROL DE ACCESOS

REQUERIMIENTOS DE LA EMPRESA PARA EL CONTROL DE ACCESO
POLÍTICAS DEL CONTROL DE ACCESO
POLÍTICAS Y REQUERIMIENTOS COMERCIALES

Los requerimientos comerciales para el control de acceso deben definirse y documentarse. Las políticas deben tomar en cuenta lo siguiente:

a) Requerimientos de seguridad de aplicaciones comerciales individuales.
b) Identificación de toda información relacionada con aplicaciones comerciales.
c) Consistencia entre los controles de acceso y clasificación de políticas de información de sistemas diferentes y redes.
d) Legislación relevante y cualquier obligación contractual con respecto a la protección de acceso a datos o servicios.
e) estándares para perfiles de acceso de usuarios para categorías comunes de trabajo.

REGLAS DE CONTROL DE ACCESO

Se debe considerar lo siguiente:

a) Diferenciación entre reglas que siempre deben esforzarse y reglas que son opcionales o condicionales.
b) Establecer reglas basadas en el cumplimiento.
c) Cambios en el etiquetado de la información que son iniciados automáticamente.
d) Reglas que requieren un administrador u otra aprobación antes de su promulgación o aquellas que no se ejecutan.

ADMINISTRACIÓN DE ACCESOS A LOS USUARIOS
USUARIOS REGISTRADOS

Debe haber un registro formal del usuario y un procedimiento de registro para garantizar acceso a sistemas de información multiusuario y servicios. Los accesos a servicios de información multiusuario deben ser controlados a través de procesos de registro de usuario, los cuales incluyen:

a) Usando un único ID de usuario, para que los usuarios puedan enlazarse y ser responsables por sus acciones.
b) Chequeando que el usuario tiene autorización del dueño del sistema para su uso.
c) Chequeando que los niveles de acceso otorgados son apropiados para propósitos comerciales.
d) Dar a los usuarios un informe escrito de sus derechos de acceso.

e) Mantener un registro formal de todas las personas registradas para usar los servicios.
f) Inmediatamente quitar los derechos de accesos a usuarios que se han cambiado de trabajo o han salido de la organización.
g) Periódicamente revisar y quitar IDs y cuentas de usuario repetidas.
h) Asegurar que la IDs de usuario repetidas no son asignadas a otros usuarios.

ADMINISTRACIÓN DE PRIVILEGIOS

La asignación y uso de privilegios deben ser restringidas y controladas. Se deben considerar los siguientes pasos:

a) Los privilegios asociados con cada resultado del sistema, operación del sistema administración de la base de datos y cada aplicación y deben identificarse las categorías de personal a que ellos necesitan ser asignados.
b) Se debe mantener un proceso de autorización y registro de los privilegios asignados.

RESPONSABILIDADES DEL USUARIO
USO DE PASSWORD

Los usuarios deben continuar con la buena práctica de seguridad en la selección y uso de contraseñas. Los usuarios deben ser advertidos de:

a) Mantener contraseñas confidenciales.
b) Evitar guardar registrado en un papel la contraseña, a menos que esta pueda guardarse con seguridad.
c) Cambiar las contraseñas cuando haya cualquier indicación que implique el sistema o contraseñas.
d) Seleccionar las contraseñas con una longitud mínima de 6 caracteres como:
    1) Fácil de recordar
    2) No basado en cualquier de lo contrario se podría suponer fácilmente.
    3) Libre de caracteres consecutivos o secuencia de números o grupos de letras.

e) Cambiar las contraseñas con intervalos regulares o basarse en el número de accesos.

CONTROL DE ACCESO A LA RED
POLÍTICAS DE USO DE LOS SERVICIOS DE LA RED

Conexiones inseguras de los servicios de la red pueden afectar la organización completamente. Una política debe ser formulada involucrando el uso de la red y servicios de la red. Estas deben cubrir:

a) Las redes y servicios de la red los cuales están permitidos para ser accesados.
b) Procedimientos de autorización para determinar a quién se permite acceder a qué redes y conectarse a los servicios de la red.
c) Administrar los controles y procedimientos para proteger el acceso a las conexiones de red y servicios de la red.

CONTROL EN LAS CONEXIONES DE LA RED

Los requerimientos de las políticas de control de acceso para redes compartidas, sobre todo aquellos que se extienden por los límites organizacionales, pueden requerir la incorporación de controles para restringir la capacidad de conexión de los usuarios. Las restricciones aplicadas deben basarse en las políticas de acceso y requerimientos de las aplicaciones comerciales, y deben ser por lo tanto guardadas y actualizadas.

CONTROL DE TRAFICO DE LA RED

Las redes compartidas, sobre todo aquéllos que se extienden por los límites organizacionales, pueden requerir la incorporación de controles de asignación de ruta para asegurar que las conexiones computacionales y flujo de información no abra brechas en las políticas de control de acceso de las aplicaciones comerciales.

Los controles de dirección de ruta deben ser basados procedencias positivas y mecanismos de chequeo de direcciones destino. Puede ser implementado un software o hardware.

SEGURIDAD DE LOS SERVICIOS DE LA RED

Una amplia gama de servicios de red públicos o privados están disponibles, algunas de las cuales ofrecen servicios de valor agregado. Los servicios de red pueden tener únicas o complejas características.

APLICACIÓN DE CONTROL DE ACCESOS
RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

Los usuarios de sistemas de aplicaciones, incluyendo personal de soporte, deben ser proveídos con accesos a información y funciones del sistema de aplicación en concordancia con la definición de políticas de control de acceso.

AISLAMIENTO DE SISTEMAS SENSIBLES

Los sistemas sensibles pueden requerir un ambiente informático especializado. Algunos sistemas de aplicación son suficientemente sensibles a la pérdida potencial que ellos requieren el manejo especial. Las siguientes aplicaciones se deben considerar:

a) La sensibilidad de un sistema de aplicación debe ser explícitamente identificada y documentada por los propietarios de la aplicación.
b) Cuando una aplicación sensible esta corriendo en un ambiente compartido, los sistemas de aplicación con los cuales compartirá recursos deben ser identificados y estar de acuerdo con los propietarios de las aplicaciones sensibles.

MONITOREO DE ACCESO Y USO DEL SISTEMA
EVENTOS REGISTRADOS

Los registros de auditoria registran excepciones y otros eventos relevantes de seguridad, debe producirse y mantenerse para un periodo convenido para ayudar en investigaciones futuras y monitoreo de control de acceso. Los registros de auditoria deben incluir:

a) IDs de usuarios
b) Fechas y hora para registros de entrada y registros de salida
c) Identificación del Terminal o identificación de ser posible.
d) Archivos de éxito y rechazo de intentos de acceso al sistema.
e) Archivos de éxito y rechazo de datos y otros recursos de intentos de acceso.

USO MONITOREADO DEL SISTEMA
PROCEDIMIENTOS Y ÁREAS DE RIESGO

Los procedimientos para uso monitoreado de recursos de procesamiento de la información deben establecerse. Tales procedimientos son necesarios para asegurar que los usuarios están realizando sólo actividades que han sido autorizadas explícitamente. Las áreas que deben considerarse incluye:

a) Accesos autorizados, incluyendo detalles como:
b) Todas las funciones con privilegios.
c) Intentos de accesos no autorizados.
d) Sistema de alerta o fallas.

FACTORES DE RIESGOS

El resultado de actividades monitoreadas deben revisarse regularmente. Los factores de riesgo que deben ser considerados incluyen:

a) Los procesos de aplicación críticos.
b) Los valores, de sensibilidad o críticos, de la información a tratarse.
c) La experiencia pasada de infiltración y mal uso del sistema.
d) La extensión de interconexión del sistema.

SINCRONIZACIÓN DEL TIEMPO

La correcta situación del reloj de la computadora es importante para asegurar la exactitud en los registros de auditoria, los cuales pueden requerirse para investigaciones o como evidencia en casos legales o disciplinarios. Cuando un computador o dispositivo de comunicación tiene la capacidad de operar en tiempo

real, debe fijarse un Standard convenido, coordinar la hora universal u hora Standard local.

8. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

CONTROLES CRIPTOGRÁFICOS

POLÍTICAS SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Tomando una decisión como si una solución criptográfica es apropiada debe verse como parte de un proceso amplio de evaluación de riesgos y selección de controles. Una organización debe desarrollar una política en el uso de controles criptográficos para protección de su información. En tales políticas es necesario el máximo beneficio y mínimo riesgo.

ENCRIPTACIÓN

La encriptación es una técnica de criptografía que puede usarse para proteger la confidencialidad de la información. Esto debe considerarse para proteger información crítica o sensible.

El proveedor especialista debe buscar el nivel apropiado de protección, para seleccionar el producto apropiado que proveerá la protección requerida y la implementación de un sistema seguro.

FIRMAS DIGITALES

Las firmas digitales proveen un recurso de protección de autenticación e integridad de documentos electrónicos.

Las firmas digitales pueden aplicarse de cualquier forma a un documento que esta siendo procesado electrónicamente.

SERVICIOS DE NO REPUDIO

Los servicios de no repudio deben usarse donde podría ser necesario resolver disputas acerca de la ocurrencia o no ocurrencia de un evento o acción, una disputa involucra el uso de una firma digital o un contrato electrónico o pago. Ello

puede ayudar a establecer evidencia para demostrar si un evento o acción particular ha dado lugar, negación de enviar una instrucción digitalmente firmada que se usa en el correo electrónico.

ADMINISTRACIÓN DE CLAVES
PROTECCIÓN DE CLAVES CRIPTOGRÁFICAS

La administración de claves criptográficas es esencial para el uso efectivo de técnicas criptográficas. Todas las claves deben proteger contra modificación y destrucción y claves privadas y secretas, necesitan protección contra revelación no autorizada.

ESTÁNDARES, PROCEDIMIENTOS Y MÉTODOS

Un sistema de administración de claves debe basarse en fijar normas convenidas, procedimientos y métodos seguros.

Para reducir la posibilidad de cumplimiento, las claves deben tener definido fecha de activación y desactivación, de modo que pueden usarse por periodo determinado. El periodo de tiempo debe depender de las circunstancias sobre las cuales el control criptográfico esta siendo usado y los riesgos percibidos.

9. ADMINISTRACIÓN CONTINUA DE LA EMPRESA

ASPECTOS PARA LA ADMINISTRACIÓN CONTINUA DE LA EMPRESA
PROCESOS PARA LA ADMINISTRACIÓN CONTINUA DE LA EMPRESA

La continuidad empresarial debe empezar por identificar eventos que pueden causar interrupción de los procesos comerciales, fallas de equipos, inundaciones e incendio. Esto debe seguirse por una valoración de riesgo para determinar el impacto de esas interrupciones.

Dependientemente de los resultados de la valoración de riesgos, un plan estratégico debe desarrollarse para determinar la proximidad global de la continuidad comercial.

10. CUMPLIMIENTO

CUMPLIMIENTO CON REQUERIMIENTOS LEGALES

IDENTIFICACIÓN DE LEGISLACIÓN APLICABLE

Todo lo referente a reglamentos, regulaciones y requerimientos contractuales deben explícitamente definirse y documentarse para cada sistema de información. Las especificaciones de controles y responsabilidades individuales para encontrar los requerimientos deben igualmente definirse y documentarse.

DERECHOS DE PROPIEDAD INTELECTUAL

COPYRIGHT

Procedimientos apropiados deben implementarse para asegurar el cumplimiento con restricciones legales en el uso de material respeto de que puede haber derechos de propiedad intelectual. La infracción de copyright puede llevar a una acción legal los cuales pueden involucrar procedimientos criminales.

SOFTWARE COPYRIGHT

Productos de software propietario son usualmente proporcionados bajo un acuerdo de la licencia como, limites de uso de los productos para maquinas especificas y puede limitarse a la creación de copias de seguridad.

RECOPILACIÓN DE EVIDENCIA

REGLAS PARA EVIDENCIA

Es necesario tener la evidencia adecuada para apoyar una acción contra una persona de la organización. siempre que esta acción sea una cuestión disciplinaria interior, la evidencia se describirá por los procedimientos internos.

ADMISIBILIDAD DE EVIDENCIA

Para lograr admisibilidad de la evidencia, las organizaciones deben asegurar que su sistema de información cumpla con cualquier Standard publicado o código de práctica para la producción de evidencia admisible.

CONSIDERACIONES EN LA AUDITORIA DE SISTEMAS

CONTROL PARA LA AUDITORIA DE SISTEMAS

Los requerimientos y actividades de auditoria involucran chequeos en los sistemas operacionales deben cuidadosamente planear y estar de acuerdo para minimizar los riesgos o discrepancias en los procesos comerciales.

CAPITULO V

IMPLEMENTACIÓN DE SEGURIDADES EN LA RED

5.1 CONTROL DE SERVICIOS

El mantenimiento de la seguridad en su sistema Linux es extremadamente importante. Una forma de administrar la seguridad en el sistema es mediante una gestión minuciosa del acceso a los servicios del sistema. Probablemente el sistema deberá proporcionar acceso a determinados servicios (por ejemplo, `httpd` si se ejecuta un servidor Web). Sin embargo, si no se necesita proveer este servicio, se debería desactivar esta función para que de este modo se minimice la exposición a potenciales fallos.

Hay diferentes métodos de administrar el acceso a los servicios del sistema. Se debe decidir qué método usar en función del servicio, la configuración del sistema y el nivel de conocimientos que tenga de Linux.

La forma más fácil de denegar el acceso a un servicio es desactivándolo. Tanto los servicios administrados con `xinetd` y los servicios en la jerarquía `/etc/rc.d` se pueden configurar para iniciarse o detenerse con tres aplicaciones diferentes:

- **HERRAMIENTA DE CONFIGURACIÓN DE SERVICIOS:** Es una aplicación gráfica que muestra una descripción de cada servicio, muestra si los servicios se han iniciado en el momento del arranque (para los niveles de ejecución 3, 4, y 5), y permite que los servicios sean arrancados, detenidos o reiniciados.
- **NTSYSV:** Es una aplicación basada en texto que permite configurar cuáles servicios son arrancados al momento de arranque para cada nivel de ejecución. Los cambios no toman efecto de inmediato para los servicios no `xinetd`. Los servicios que no son `xinetd` no pueden ser arrancados, detenidos o reiniciados usando este programa.
- **`CHKCONFIG:`** Es una utilidad de línea de comandos permite activar o desactivar servicios para los diferentes niveles de ejecución. Los cambios no toman efecto de inmediato para los servicios no `xinetd`. Los servicios no `xinetd` no pueden ser arrancados, detenidos o reiniciados usando esta utilidad.

Otra forma de administrar el acceso a los servicios del sistema es mediante el uso de `iptables` para configurar un firewall IP. Para que un usuario nuevo de Linux, tenga en cuenta que `iptables` puede que no sea la mejor solución.

Por otro lado, la ventaja de utilizar `iptables` es flexibilidad. Por ejemplo, si se necesita una solución personalizada que proporcione a determinados hosts el acceso a servicios concretos, `iptables` puede ser la herramienta que necesita.

Alternativamente, si se busca una utilidad que establezca reglas de acceso generales para la máquina, hacer la prueba con **GNOME Lokkit**. **GNOME Lokkit** es una aplicación tipo GUI que hará preguntas sobre cómo se desea usar el equipo. Basado en las respuestas, configurará un cortafuegos sencillo. También se puede usar la **Herramienta de configuración de nivel de seguridad**.

5.1.1. NIVELES DE EJECUCIÓN

Antes de configurar el acceso a servicios, se deb entender qué son los niveles de ejecución en Linux. Un nivel de ejecución es un estado o un *modo* que los servicios incluidos en el directorio `/etc/rc.d/rc<x>.d` definen, donde `<x>` es el número del nivel de ejecución.

Linux utiliza los siguientes niveles de ejecución:

- 0 — Parada
- 1 — Modo de un usuario
- 2 — No se utiliza (definido por el usuario)
- 3 — Modo completo de multiusuarios
- 4 — No se utiliza (definido por el usuario)
- 5 — Modo completo de multiusuarios (con una pantalla de conexión basada en X)
- 6 — Rearranque

Si se usa una pantalla de texto para el ingreso al sistema, se estará operando a nivel de ejecución 3.

Si se usa una pantalla gráfica para ingresar al sistema, se estará operando a nivel de ejecución 5.

El nivel de ejecución por defecto se puede cambiar si se modifica el fichero `/etc/inittab`, que contiene una línea junto a la parte superior del fichero con el siguiente aspecto:

```
id:5:initdefault:
```

Se cambia el número de esta línea para reflejar el nivel de ejecución que desee. El cambio no tendrá efecto hasta rearrancar el sistema.

Para cambiar el nivel de ejecución inmediatamente, se usa el comando `telinit` seguido del número del nivel de ejecución. Debe ser usuario root para poder usar este comando.

5.1.2 HERRAMIENTA DE CONFIGURACIÓN DE SERVICIOS

La **Herramienta de configuración de servicios** es una aplicación gráfica desarrollada por Red Hat para configurar qué servicios SysV en `/etc/rc.d/init.d` se inician en el momento del arranque (para los niveles de ejecución 3, 4, y 5) y cuáles servicios `xinetd` están activados. También permite arrancar, detener y rearrancar servicios SysV así como rearrancar `xinetd`.

Para arrancar la **Herramienta de configuración de servicios** desde el escritorio, se debe ir al botón **Menú principal** (en el Panel) => **Configuración del servidor** => **Servicios** o escribir el comando `redhat-config-services` en el intérprete de comandos (por ejemplo, en un **XTerm** o un **terminal de GNOME**).

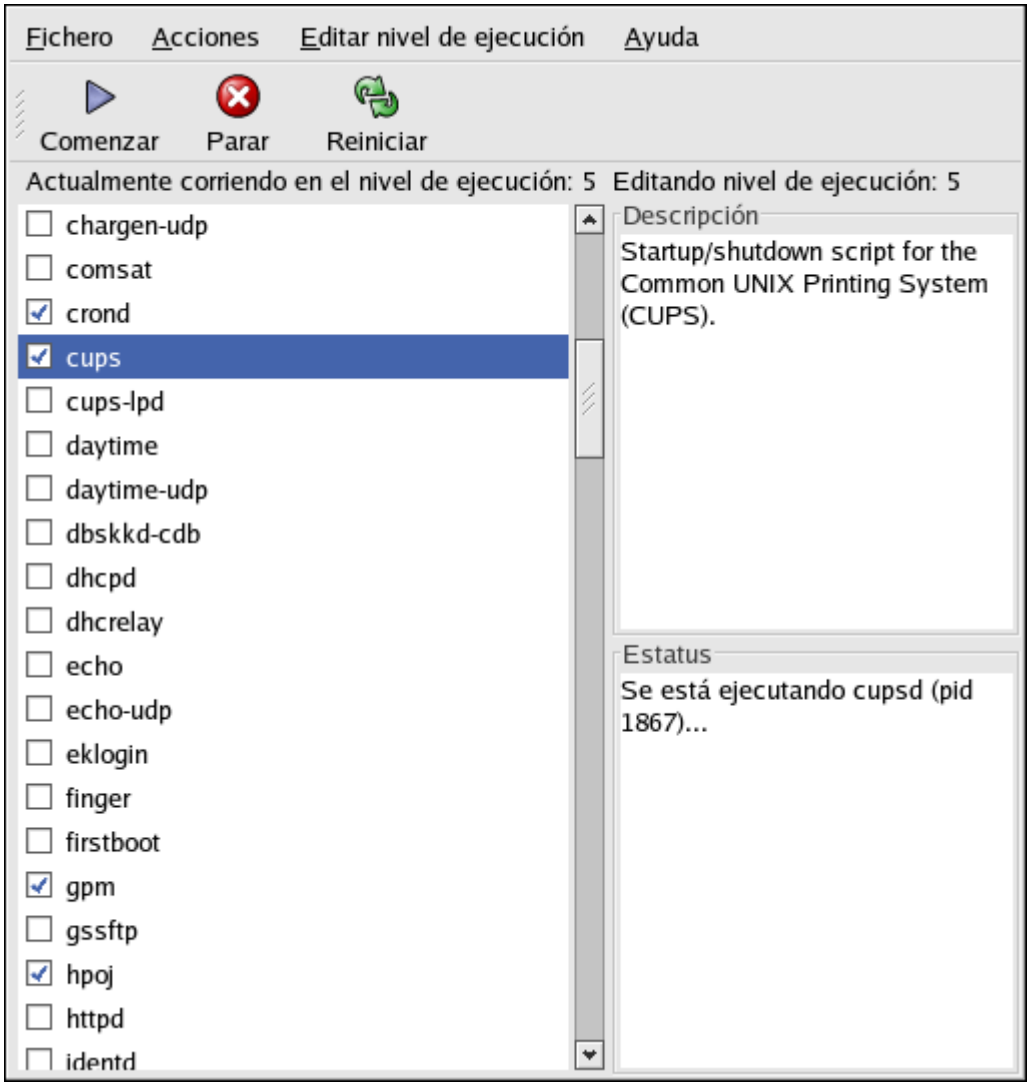


Figura 5.1 Herramienta de configuración de servicios

La **Herramienta de configuración de servicios** muestra el nivel de ejecución así como también el nivel de ejecución en el cual está modificando actualmente. Para modificar otro nivel de ejecución, seleccione **Editar nivel de ejecución** desde el menú desplegable y seleccione los niveles 3, 4, o 5.

La **Herramienta de configuración de servicios** muestra los servicios de `/etc/rc.d/init.d` y los servicios controlados por `xinetd`. Hacer click en un servicio para mostrar una breve descripción del servicio y también para ver el estado del mismo. Si el servicio no es `xinetd`, la ventana de estado muestra si el servicio se está ejecutando o no. Si el servicio es controlado por `xinetd`, la ventana de estado mostrará la frase **servicio xinetd**.

Para arrancar, detener o rearrancar un servicio inmediatamente, seleccione el servicio y haga click en el botón adecuado (o elija la acción correspondiente en el menú desplegable **Acciones**). Si el servicio es `xinetd`, los botones de acción estarán desactivados porque no pueden ser arrancados o detenidos individualmente.

Si se activa o desactiva un servicio `xinetd` marcando o desmarcando la casilla de verificación al lado del nombre del servicio, debe seleccionar **Archivo** => **Guardar cambios** desde el menú desplegable para reiniciar `xinetd` e inmediatamente activar/desactivar el servicio `xinetd` que se cambió. También se configura `xinetd` para recordar la configuración. Se puede activar/desactivar más de un servicio `xinetd` a la vez y guardar los cambios cuando se haya terminado.

Por ejemplo, imaginemos que verificamos `rsync` para activarlo a nivel de ejecución 3 y luego guarda los cambios. El servicio `rsync` se activará de inmediato. La próxima vez que arranque `xinetd`, `rsync` estará todavía activado.

Para activar un servicio no `xinetd` para que se inicie en el momento de arranque del sistema para el nivel de ejecución seleccionado actualmente, marcar la casilla de verificación al lado del nombre del servicio en la lista. Después de configurar el nivel de ejecución, aplicar los cambios seleccionando **Archivo** => **Guardar cambios** desde el menú desplegable. La configuración del nivel de ejecución es modificada, pero el nivel de ejecución no es reiniciado; por tanto los cambios no toman efecto de inmediato.

Por ejemplo, se asume que está configurado un nivel de ejecución 3. Si cambia el valor para el servicio `anacron` de marcado a desmarcado y luego selecciona **Guardar cambios**, el nivel de ejecución 3 cambia y entonces `anacron` no es iniciado al momento de arranque. Sin embargo, el nivel de ejecución 3 no es reinicializado, por tanto `anacron` todavía estará ejecutándose. Llegados a este punto, seleccionar una de las siguientes opciones:

1. **DETENER EL SERVICIO `ANACRON` —** Detener el servicio seleccionándolo de la lista y haciendo click en el botón **Parar el servicio**. Aparecerá un mensaje para indicar que se ha detenido correctamente el servicio.

2. **REINICIALIZAR EL NIVEL DE EJECUCIÓN** — Reinicializar el nivel de ejecución escribiendo en el intérprete de comandos del shell el comando `telinit 3` (donde 3 es el número de nivel de ejecución). Esta opción es recomendada si cambia el valor **Comenzar al arrancar** de más de un servicio y quiere activar los cambios inmediatamente.
3. **NO ES NECESARIO DETENER EL SERVICIO `ANACRON`**. Puede esperar a que se rearranque el sistema para detener el servicio. La próxima vez que se arranque el sistema, se inicializará el nivel de ejecución sin que se ejecute el servicio `anacron`.

5.1.3 SEGURIDADES EN LOS SERVICIOS LINUX

SERVICIO	SEGURIDAD	MODELO OSI
telnet	Ssh	Aplicación
ftp	Vsftp	Aplicación
Samba	Samba security =user	Aplicación
Mail	Spamassassin Clamav	Aplicación
http	https	Aplicación
administración de Usuario	MD5	Sesión
Acceso de Servicios	Firewall	Transporte
Proxy Red	Squid	Red

Tabla 5.1 Seguridad en los Servicios Linux

5.1.4 SERVICIO DE SHELL

5.1.4.1 SERVICIO SSH

- **DESCRIPCIÓN**

SSH permite a los usuarios registrarse en sistemas de host remotamente. A diferencia de FTP o Telnet, SSH encripta la sesión de registro imposibilitando que alguien pueda obtener contraseñas no encriptadas.

- **CONFIGURACIÓN**

- ***EL DEMONIO SSHD***

El demonio **sshd** es el programa que espera conexiones de red de los clientes ssh, controla la autenticación y ejecuta el comando requerido. El puerto por defecto en el que escucha es el 22 y su fichero de configuración es `/etc/ssh/sshd_config`.

Otras opciones a destacar son:

- X11Forwarding yes|no : habilitar o deshabilitar la redirección X
- PasswordAuthentication yes|no : especifica si deseamos utilizar la autenticación básica

En esta configuración se indica también la ruta en la que encontrar las claves que identifican nuestro servidor. Estas son la base de la autenticación mediante clave pública y los valores por defecto son:

- HostKey `/etc/ssh/ssh_host_key`
- HostKey `/etc/ssh/ssh_host_rsa_key`
- HostKey `/etc/ssh/ssh_host_dsa_key`

Estas claves generales al sistema, junto con su correspondiente clave pública.

- ***LOS CLIENTES SSH***

Los programas que permiten al usuario utilizar el protocolo *SSH* son **scp**, **sftp** y **ssh**.

Se pueden configurar opciones generales al sistema en el fichero `/etc/ssh/ssh_config` como por ejemplo:

- ForwardX11 yes|no: habilitar o deshabilitar la redirección X
- PasswordAuthentication yes|no: especifica si deseamos utilizar la autenticación básica en nuestros clientes.

En él se indican las rutas para obtener las claves públicas y privadas de cada usuario:

- IdentityFile `~/.ssh/identity`
- IdentityFile `~/.ssh/id_rsa`
- IdentityFile `~/.ssh/id_dsa`

Estas entradas indican que las claves privada y publica de cada usuario se encontrarán en el directorio `.ssh` del HOME del usuario. En este directorio se encuentra también el fichero `authorized_keys2` que controla la autenticación mediante claves.

➢ **PRUEBA**

El comando **ssh** ofrece comunicación encriptada y segura entre dos sistemas sobre una red no segura. Este comando reemplaza al **telnet**, **rlogin**, **rsh**.

Para iniciar una sesión en otra máquina usando **ssh**:

```
[usuario1@localhost usuario1]$ ssh usuario1@servidor.dominio.es
The authenticity of host 'servidor.dominio.es (192.168.0.2)' can't be
established.
RSA key fingerprint is
97:4f:66:f5:96:ba:6d:b2:ef:65:35:45:18:0d:cc:29.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'servidor.dominio.es' (RSA) to the list of
known hosts.
usuario1@servidor.dominio.es's password:
[usuario1@servidor.dominio.es usuario1]$
```

La primera vez que se realiza la conexión debe aceptar la firma del otro host. De esta manera se establece una relación de confianza que se traduce en archivar la clave pública de este servidor en el fichero $HOME/.ssh/known_hosts.

La sintaxis básica del comando **ssh** es:

```
Ssh user@hostname [command]
```

El comando es opcional. Si se especifica en lugar de obtener un shell se ejecuta el comando en la máquina remota.

Por ejemplo podríamos hacer un ls en la máquina remota y observar su salida:

```
ssh usuario1@servidor.dominio.es ls
```

O realizar alguna operación mas elaborada como realizar una copia en local de un directorio remoto, como en el ejemplo:

```
ssh usuario1@servidor.dominio.es "tar cf - /home/usuario1" |\
                                  tar xvf -
```

- ***SCP***

El comando **scp** permite copiar ficheros entre dos máquinas. Utiliza **ssh** para la transmisión de la información, por lo que ofrece la misma seguridad que el **ssh**. De la misma manera utiliza los métodos de autenticación de **ssh**. Este comando reemplaza al **rcp**, **ftp**.

Este es un ejemplo de uso del **scp** para copiar desde la máquina local a una remota:

```
[usuario1@localhost]scp /tmp/file
usuario1@servidor.dominio.es:/tmp
```

También podemos copiar ficheros entre dos máquinas remotas:

```
[usuario1@localhost]scp usuario1@anotherhost:/tmp/file \
                        usuario1@servidor.dominio.es:/tmp
```

La sintaxis del comando es:

```
scp [-pqrvBC46] [-F ssh_config] [-S program] [-P port] [-c cipher]
         [-i identity_file] [-o ssh_option] [[user@]host1:]file1
[...]
         [[user@]host2:]file2
```

Puedes consultar las opciones en la página man de **scp**, estas son las más habituales:

- `-p`: conserva las propiedades del archivo. Permisos del archivo, fecha de última de modificación.
- `-r`: copia recursiva de directorios

La sintaxis para especificar el origen o destino de los archivos tiene la forma **[[user@]host:]file** donde:

- **`user`**: es el usuario de la máquina. Si no se especifica es el actual.
- **`host`**: es la máquina origen o destino del archivo. Si no se informa es la máquina local.
- **`file`**: fichero o directorio a copiar. Por defecto es el directorio HOME del usuario. En caso de ser un directorio deberás especificar la opción `-r`.

- ***SFTP***

El comando **sftp** transfiere archivos entre máquinas de forma interactiva.

Los comandos interactivos son similares al clásico **ftp**:

```
[usuario1@localhost usuario1]$ sftp servidor.dominio.es
Connecting to servidor.dominio.es...
usuario1@servidor's password:
sftp> help
Available commands:
cd path                       Change remote directory to 'path'
lcd path                      Change local directory to 'path'
```

```
chgrp grp path                  Change group of file 'path' to 'grp'
chmod mode path                 Change permissions of file 'path' to
'mode'
chown own path                  Change owner of file 'path' to 'own'
help                            Display this help text
get remote-path [local-path]    Download file
lls [ls-options [path]]         Display local directory listing
ln oldpath newpath              Symlink remote file
lmkdir path                     Create local directory
lpwd                            Print local working directory
ls [path]                       Display remote directory listing
lumask umask                    Set local umask to 'umask'
mkdir path                      Create remote directory
put local-path [remote-path]    Upload file
pwd                             Display remote working directory
exit                            Quit sftp
quit                            Quit sftp
rename oldpath newpath          Rename remote file
rmdir path                      Remove remote directory
rm path                         Delete remote file
symlink oldpath newpath         Symlink remote file
version                         Show SFTP version
!command                        Execute 'command' in local shell
!                               Escape to local shell
?                               Synonym for help
sftp>
```

Un ejemplo de uso:

```
[usuario1@localhost]sftp usuario1@servidor.dominio.es
sftp> get fichero
```

- **MÉTODOS DE AUTENTICACIÓN**

SSH puede utilizar varios métodos de autenticación y hay archivos que controlan los permisos para estos métodos.

- ***AUTENTICACIÓN MEDIANTE USUARIO/CONTRASEÑA***

Es la autenticación básica. Se puede habilitar o deshabilitar en `/etc/ssh/sshd_config` y `/etc/ssh/ssh_config`.

- ***AUTENTICACIÓN BASADA EN HOST/USUARIO***

Como en los comandos "r" se puede configurar el acceso a **ssh** mediante ficheros que especifican desde que usuario y máquina se permite.

Estos ficheros son:

- `/etc/ssh/shosts.equiv`: con el mismo funcionamiento que `/etc/hosts.equiv`
- `$HOME/.shosts`: a nivel de usuario, como el fichero `$HOME/.rhost`

- ***AUTENTICACIÓN MEDIANTE CLAVES***

Para obtener el máximo partido a *SSH* podemos utilizar su capacidad de autenticación mediante clave pública y privada.

Para ello el cliente debe generar sus claves privada y pública, compartiendo esta última con el servidor para poder identificarse. Una vez hecho esto las conexiones se podrán establecer sin necesidad de utilizar el esquema clásico de usuario y contraseña.

Un mensaje encriptado con la pública sólo puede desencriptarse con la correspondiente clave privada. `OpenSSH` utiliza estas propiedades de los algoritmos de clave pública y privada para realizar la autenticación sin intercambio de contraseñas.

Estos son los pasos a seguir para poder utilizar esta autenticación.

1. Generar la clave en el cliente.

```
[root@espe ~]# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
/home/prueba/.ssh
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/prueba/.ssh.
Your public key has been saved in /home/prueba/.ssh.pub.
The key fingerprint is:
72:ab:aa:83:52:00:38:c8:1a:47:05:af:0e:8b:62:dc
root@espe.com
[root@espe ~]#
```

2. La passphrase si se rellena tiene un comportamiento similar a la contraseña, será solicitada al utilizar esta clave. Deberá ser una frase, en la que se pueden incluir espacios en blanco y signos de puntuación.

3. En nuestro caso hemos decidido dejarla vacía para así poder utilizar este método de autenticación en procesos no interactivos. Puedes utilizar una frase de paso si no confías en la seguridad de tu máquina.

   La passphrase se puede cambiar con el comando ssh-keygen -p.

4. El tipo de la clave se especifica mediante el parámetro `-t`, y puede ser:
   - rsa1 para ssh v1
   - rsa, dsa para ssh v2

   En el ejemplo se ha utilizado el tipo dsa, y se ha guardado en los archivos por defecto. Estos son `$HOME/.ssh/id_dsa` para la clave privada y `$HOME/.ssh/id_dsa.pub` para la clave pública.

   La clave privada es la que nos identifica, por lo que debe ser accesible únicamente por el usuario propietario.

5.1.4.2 SERVICIO TRANSFERENCIA DE ARCHIVOS (VSFTP)

- **DESCRIPCIÓN**

`vsftpd:` Es un demonio FTP rápido y seguro, preferido para Red Hat Enterprise Linux.

El demonio FTP vsftpd (o Very Secure FTP Daemon) está diseñado desde la base para ser rápido, estable y lo más importante, seguro. Su habilidad para manejar grandes números de conexiones de forma eficiente y segura es lo que hace que vsftpd sea el único FTP independiente distribuido con Red Hat Enterprise Linux.

El modelo de seguridad utilizado por `vsftpd` tiene tres aspectos principales:

- **CLARA SEPARACIÓN DE PROCESOS PRIVILEGIADOS Y SIN PRIVILEGIOS** — Procesos separados manejan tareas diferentes y cada uno de estos procesos se ejecuta con los privilegios mínimos requeridos para la tarea.
- **LAS TAREAS QUE REQUIEREN ALTOS PRIVILEGIOS SON MANEJADAS POR PROCESOS CON LOS MÍNIMOS PRIVILEGIOS NECESARIOS** — Influenciando las compatibilidades encontradas en la biblioteca

`libcap`, las tareas que usualmente requieren privilegios de Usuario Administrador se pueden ejecutar de forma más segura desde un proceso menos privilegiado.

- **LA MAYORÍA DE LOS PROCESOS SE EJECUTAN ENJAULADOS EN UN AMBIENTE `CHROOT` —** Siempre que sea posible, se cambia la raíz de los procesos al directorio compartido; este directorio se considera luego como la jaula chroot. Por ejemplo, si el directorio `/var/ftp/` es el directorio compartido principal, `vsftpd` reasigna `/var/ftp/` al nuevo directorio raíz, conocido como /. Esto previene actividades maliciosas de cualquier hacker potencial en algún directorio que no estén por debajo del nuevo directorio root.

El uso de estas prácticas de seguridad tiene el efecto siguiente en cómo `vsftpd` trata con las peticiones:

- **EL PROCESO PADRE SE EJECUTA CON EL MÍNIMO DE PRIVILEGIOS REQUERIDO —** El proceso padre calcula dinámicamente el nivel de privilegios requerido para minimizar el nivel de riesgos. Los procesos hijo manejan la interacción directa con los clientes FTP y se ejecutan casi sin ningún privilegio.
- **TODAS LAS OPERACIONES QUE REQUIEREN ALTOS PRIVILEGIOS SON MANEJADAS POR UN PEQUEÑO PROCESO PADRE** —vsftpd lanza procesos hijos sin privilegios para manejar las conexiones entrantes. Esto permite al proceso padre privilegiado, ser tan pequeño como sea posible y manejar relativamente pocas tareas.
- **EL PROCESO PADRE NO CONFIA EN NINGUNA DE LAS PETICIONES DESDE PROCESOS HIJOS SIN PRIVILEGIOS** — Las comunicaciones con procesos hijos se reciben sobre un socket y la validez de cualquier información desde un proceso hijo es verificada antes de proceder.
- **LA MAYOR PARTE DE LA INTERACCIÓN CON CLIENTES FTP LA MANEJAN PROCESOS HIJO SIN PRIVILEGIOS EN UNA JAULA `CHROOT`. —** Debido a que estos procesos hijo no tienen privilegios y solamente tienen acceso al directorio que está siendo compartido, cualquier proceso fallido solamente permitirá al atacante acceder a los archivos compartidos.

- **CONFIGURACIÓN**

- ***FICHEROS DE CONFIGURACIÓN***

`/etc/vsftpd.user_list`	Lista que definirá usuarios a enjaular o no a enjaular, dependiendo de la configuración.
`/etc/vsftpd/vsftpd.conf`	Fichero de configuración.

- ***PROCEDIMIENTOS***

Con el editor de texto editar `/etc/vsftpd/vsftpd.conf`. A continuación se analiza los parámetros a modificar o añadir según sea necesario.

- **PARÁMETRO ANONYMOUS_ENABLE**

Este parámetro se utiliza para definir si se permitirán los accesos anónimos al servidor. Establezca el valor como valores YES o NO de acuerdo a lo que se requiera.

```
anonymous_enable=YES
```

- **PARÁMETRO LOCAL_ENABLE.**

Este parámetro es particularmente atractivo si se combina con la función de jaula. Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema. Establezca el valor YES o NO de acuerdo a lo que se requiera.

```
Local_enable=YES
```

- **PARÁMETRO WRITE_ENABLE.**

Este parámetro establece si se permite el mandato "write" (escritura) en el servidor. Establezca el valor YES o NO de acuerdo a lo que se requiera.

```
Write_enable=YES
```

- **PARÁMETRO FTPD_BANNER.**

Este parámetro sirve para establecer el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Puede establecerse cualquier frase breve que considere conveniente.

```
ftpd_banner=Bienvenido al servidor FTP TESIS ESPE.
```

- **ESTABLECIENDO JAULAS PARA LOS USUARIOS: PARÁMETROS chroot_local_user y chroot_list_file.**

De modo predefinido los usuarios del sistema que se autentiquen tendrán acceso a otros directorios del sistema fuera de su directorio personal. Si se desea recluir a los usuarios a solo poder utilizar su propio directorio personal, puede hacerse fácilmente con el parámetro *chroot_local_user* que habilitará la función de *chroot()* y los parámetros chroot_list_enable y chroot_list_file para establecer el fichero con la lista de usuarios que quedarán excluidos de la función *chroot()*.

```
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list
```

Con lo anterior, cada vez que un usuario local se autentique en el servidor FTP, solo tendrá acceso a su propio directorio personal y lo que este contenga. **No olvide crear. /etc/vsftpd/vsftpd.chroot_list, ya que de otro modo no arrancará vsftpd**.

chroot_local_user

Permite o no a los usuarios locales el acceso a la maquina

chroot_local_user=true
chroot_local_user=false

Para decirle al servidor de FTP que usuarios tienen permiso para acceder tenemos que coger la ruta de el archivo antes comentado donde se encontraba la lista de usuarios (vsftpd.user_list)

Para ello en el archivo de configuración pondríamos algo como esto:

Chroot_list_file=/etc/vsftpd.user_list

Básicamente con estos comandos se configurar el servidor FTP en Linux sin ningún problema.

- ## CONTROL DEL ANCHO DE BANDA.

- **PARÁMETRO anon_max_rate**

  Este parámetro es utilizado para limitar la tasa de transferencia en bytes por segundo para los usuarios anónimos, algo sumamente útil en servidores FTP de acceso público. En el siguiente ejemplo se limita la tasa de transferencia a 5 Kb por segundo para los usuarios anónimos:

```
Anon_max_rate=5120
```

- **PARÁMETRO local_max_rate.**

  Este parámetro hace lo mismo que anon_max_rate, pero aplica para usuarios locales del servidor. En el siguiente ejemplo se limita la tasa de transferencia a 5 Kb por segundo para los usuarios locales:

```
local_max_rate=5120
```

- **PARÁMETRO max_clients.**

  Este parámetro establece el número máximo de clientes que podrán acceder simultáneamente hacia el servidor FTP. En el siguiente ejemplo se limitará el acceso a 5 clientes simultáneos.

```
max_clients=5
```

- **PARÁMETRO max_per_ip.**

  Este parámetro establece el número máximo de conexiones que se pueden realizar desde una misma dirección IP. Tome en cuenta que algunas redes acceden a través de un servidor proxy o puerta de enlace y debido a esto podrían quedar bloqueados innecesariamente algunos accesos. En el siguiente ejemplo se limita el número de conexiones por IP simultáneas a 5.

```
max_per_ip=5
```

- ***APLICANDO LOS CAMBIOS.***

A diferencia de otros daemon FTP, VSFTPD no requiere configurarse como daemon sobre demanda y por tanto no depende de xinetd. De modo tal, podrá inicializarse, detenerse o reinicializarse a través del mandato `service` y añadirse al arranque del sistema en un nivel o niveles de corrida en particular con el mandato `chkconfig`.

Para ejecutar por primera vez el servicio, ejecutar:

```
/sbin/service vfstpd Start
```

Para hacer que los cambios hechos a la configuración surtan efecto, ejecutar:

```
/sbin/service vsftpd restart
```

Para detener el daemon, ejecutar:

```
/sbin/service vsftpd stop
```

Para añadir VSFTPD al arranque del sistema, que son los niveles regularmente utilizados para trabajar, ejecutar:

```
/sbin/chkconfig vsftpd on
```

- **PRUEBA**

Luego de realizadas las configuraciones descritas anteriormente procedemos a realizar la prueba correspondiente, y el resultado fue el siguiente:

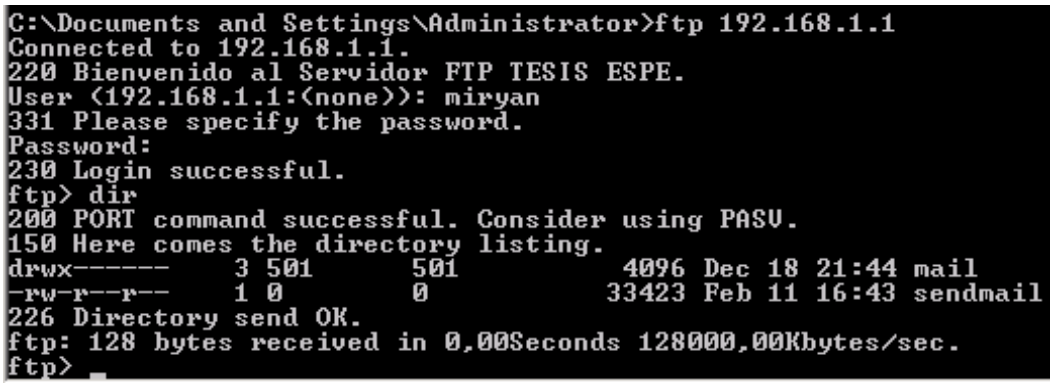


Gráfico 5.2 Prueba de vsftpd

5.1.4.3 SERVICIO DE MAIL (CORREO ELECTRÓNICO)

- **DESCRIPCIÓN**

PROTOCOLOS DE CORREO ELECTRÓNICO

Hoy día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al servidor de correo del recipiente y allí se le suministra al cliente de correo del recipiente.

Para permitir todo este proceso, existe una variedad de protocolos de red estándar que permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o email.

5.1.4.3.1 PROTOCOLOS DE TRANSPORTE DE CORREO

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el *Protocolo simple de transferencia de correo* (*Simple Mail Transfer Protocol* o *SMTP*).

- **SMTP**

El objetivo principal del protocolo simple de transferencia de correo, SMTP, es transmitir correo entre servidores de correo. Sin embargo, es crítico para los clientes de correo también. Para poder enviar correo, el cliente envía el mensaje a un servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega. Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.

En Red Hat Enterprise Linux, un usuario puede configurar un servidor SMTP en la máquina local para manejar la entrega de correo. Sin embargo, también es posible configurar servidores remotos SMTP para el correo saliente.

Un punto importante sobre el protocolo SMTP es que no requiere autenticación. Esto permite que cualquiera en la Internet pueda enviar correo a cualquiera otra persona o a grandes grupos de personas. Esta característica de SMTP es lo que hace posible el correo basura o *spam*. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que sólo los hosts conocidos accedan al servidor SMTP. Los servidores que no ponen tales restricciones son llamados servidores *open relay*.

Red Hat Enterprise Linux utiliza Sendmail **(`/usr/sbin/sendmail`)** como su programa SMTP por defecto. Sin embargo, también está disponible una aplicación más simple de servidor de correo llamada Postfix **(`/usr/sbin/postfix`).**

- ***PROTOCOLOS DE ACCESO A CORREO***

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el *Post Office Protocol* (*POP*) y el *Internet Message Access Protocol* (*IMAP*).

A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para ambos protocolos son pasadas a través de la red sin encriptar.

- **POP**

El servidor por defecto POP bajo Red Hat Enterprise Linux es **`/usr/sbin/ipop3d`** y es proporcionado por el paquete `imap`. Cuando se utiliza POP, los mensajes de correo son descargados a través de las aplicaciones de correo cliente. *Por defecto, la mayoría de los clientes de correo POP son configurados para borrar automáticamente el mensaje en el servidor de correo después que éste ha sido transferido exitosamente*.

POP es completamente compatible con estándares importantes de mensajería de Internet, tales como *Multipurpose Internet Mail Extensions* (*MIME*), el cual permite los anexos de correo.

POP funciona mejor para usuarios que tienen un sistema en el cual leer correo. También funciona bien para usuarios que no tienen una conexión permanente a la Internet o a la red que contiene el servidor de correo. Desafortunadamente para aquellos con conexiones lentas, POP requiere que luego de la autenticación los programas cliente descarguen el contenido completo de cada mensaje. Esto puede tomar un buen tiempo si algún mensaje tiene anexos grandes.

- **IMAP**

El servidor por defecto IMAP bajo Red Hat Enterprise Linux es `/usr/sbin/imapd` y es proporcionado por el paquete `imap`. Cuando utilice un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leerlos o borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.

IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.

Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP.

IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

➢ CONFIGURACIÓN

- SENDMAIL

El propósito principal de Sendmail, como cualquier otro MTA, es el de transferir correo de forma segura entre hosts, usualmente usando el protocolo SMTP. Sin embargo, Sendmail es altamente configurable, permitiendo el control sobre casi cada aspecto del manejo de correos, incluyendo el protocolo utilizado.

Todos los ficheros de configuración de sendmail se encuentran en el directorio **/etc** o **/etc/mail**, o en ambos.

El fichero principal es **sendmail.cf**. Es probablemente el fichero de configuración más complejo y difícil de manejar. Por fortuna se han ido incorporando una serie de ficheros aparte con los que se configura lo más importante del servidor de correo, sin necesidad de tocar el sendmail.cf. Esos ficheros son:

- **local-host-names**: donde se indica a que dominios pertenece el servidor de correo
- **access**: donde se dice que ips y que dominios tienen permiso para utilizar el servidor de correo.
- **mailertable**: donde se pueden aplicar enrutamientos para dominios.
- **sendmail.mc**: fichero de macros donde se pueden configurar distintas opciones de sendmail, como el smtp autentificado.

Con el sendmail.cf se puede crear un sistema de reglas para manipular los correos, pero la sintaxis es francamente ofuscada.

- **¿COMO MONTAR UN SERVIDOR DE CORREO?**

  Imaginemos que tenemos un linux con el sendmail instalado, en concreto el paquete de sendmail y el sendmail-cf (para verificar se puede hacer: `rpm -qa | grep sendmail`).

  Imaginemos que tenemos una maquina linux conectada a internet con una ip publica o un servidor conectado a un router que redirige el puerto 25 al servidor.

Tenemos el dominio espe.com y queremos tener que el servidor envié/reciba correos en plan "juan@espe.com" o "amigo@espe.com".

- **¿QUÉ PASOS HAY QUE SEGUIR?**

1. **PRIMERO:** hay que decirle al sendmail a que dominio sirve. Para eso editamos el fichero /etc/mail/local-host-names y añadimos "**espe.com**"
2. **SEGUNDO**: hay que habilitar el acceso a alguna red para que sea capaz de enviar correo a través de nuestro servidor. Por defecto sendmail solo dejará enviar correos desde si mismo, para evitar el SPAM. Si queremos usar el servidor de correo para poder mandar, debemos especificar la ip desde la que accederemos, generalmente la red local en la que se encuentra el servidor o una lista de ips de confianza. Para eso editamos el fichero /etc/mail/access y ponemos:

localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY
192.168.1	RELAY
espe.com	RELAY
spam.com	REJECT

Si no hacemos esto, cuando intentemos enviar correo el servidor nos contestara con el mítico "relaying denied" (transmisión denegada).

Hay que distinguir entre enviar y recibir: el servidor de correo es un intercambiador de correo, un MTA (Mail Transfer Agent). Como un buzón universal debe poder recibir correo de cualquier sitio. Pero hay que controlar que el envío no se pueda hacer desde cualquier lado, para que nadie utilice nuestro servidor para hacer SPAM o envíos masivos. Por otro lado, si no queremos que se reciba correos de determinado sitio se puede filtrar a través de la IP de origen.

3. **TERCERO:** hay que asegurarse de que sendmail escucha en el puerto 25 y que no tiene al puerto asociado a localhost. Para verificarlo hacemos netstat -ln y veremos los puertos en escucha que hay en el sistema. Si sale algo como:

```
tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN
```

Entonces es correcto.
Si estuviera escuchando en localhost:

```
tcp 0 127.0.0.1:25 0.0.0.0:* LISTEN
```

El puerto 25 solo será accesible desde el propio servidor y estará cerrado al resto del mundo.

Para cambiar esto hay que tocar el fichero /etc/mail/sendmail.mc y comentar una directiva en la que se menciona 127.0.0.1. Para comentar la directiva ponemos delante "dnl"

El fichero sendmail.mc es un fichero de macros, una vez modificado debemos ejecutar un comando que se especifica al principio del propio fichero, normalmente:

```
m4 /etc/mail/sendmail.mc > /etc/sendmail.cf
```

También al modificar los otros ficheros que se encuentran en /etc/mail hay que moverse ahí y ejecutar "`make`".

Cada vez que se metan cambios en estos ficheros, hay que aplicar make o m4 y **además reiniciar el sendmail**.

- **¿CÓMO COMPROBAR QUE EL SERVIDOR DE CORREO ESTA FUNCIONANDO?**

Lo primero, ver que el proceso sendmail esta en marcha con un `ps -axf | grep sendmail` o `ps -fea | grep sendmail`

Otra comprobación mas seria mirar si el puerto 25 esta abierto con: `netstat -ln | grep 25`

Otra comprobación mas seria mirar si el fichero /var/run/sendmail.pid existe.

Otra comprobación más rápida y eficaz es:

telnet localhost 25 o desde el exterior telnet servidor.decorreo.espe.com 25 y comprobar la respuesta, que será algo así como:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220    servidor.decorreo.espe.com    ESMTP    Sendmail
8.12.8/8.12.8; Fri, 4 Apr 2003 16:30:12 +0200
```

Podemos escribir QUIT para salir.

- **¿CÓMO PUEDO VER LA ACTIVIDAD DEL SERVIDOR DE CORREO?**

Una vez más, hay que ir a los logs, los logs nos hablan abiertamente de lo que pasa en nuestro sistema. Podemos ejecutar:

```
tail -f /var/log/maillog
```

veremos cada evento relacionado con el correo, cada email recibido, enviado, cada consulta al buzón a través de pop3 o imap.

Dependiendo del sistema, quizá los logs estén en otra parte. **/var/log/syslog** o **/var/log/messages**

En los logs veremos la actividad y también los errores de determinados buzones.

Es más: si el sendmail no se inicia, hay que mirar en los logs para ver lo que pasa, y tendremos la respuesta. Se mira en /var/log/maillog o /var/log/messages.

- **POP 3 (PROTOCOLO PARA ACCEDER HACIA EL CORREO)**

Habilitar protocolos de lectura de correo:

Si utiliza Red Hat Enterprise Linux 4.0, el paquete imap es reemplazado por dovecot, el cual funciona como otros servicios. Se debe editar el fichero **/etc/dovecot.conf** y habilitar los servicios de imap y/o pop3 del siguiente modo (de modo predefinido solo está habilitado imap):

```
protocols = imap pop3
```

El servicio se agrega al arranque del sistema y se inicializa del siguiente modo:

```
/sbin/chkconfig dovecot on
/sbin/service dovecot start
```

- **PRUEBA**

El resultado de ejecutar los procedimientos anteriores puestos en práctica es el siguiente:

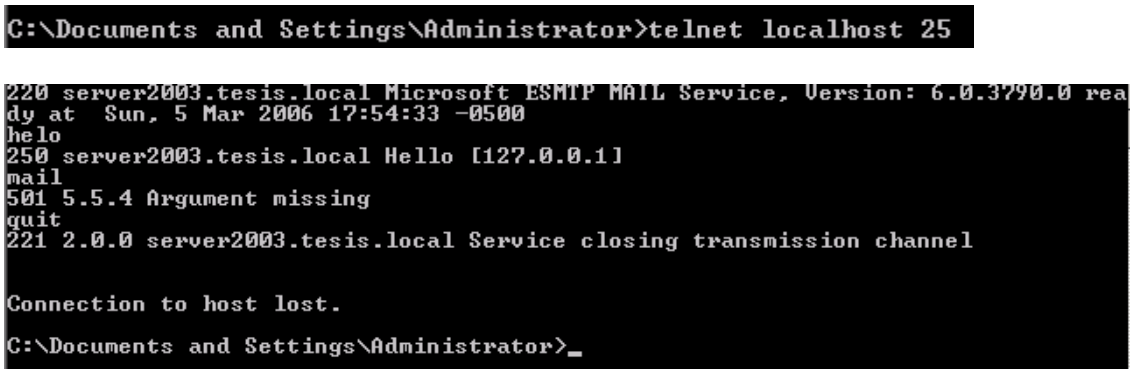


Gráfico 5.3 Prueba de Sendmail

5.2 CONTROL DE CORREO

El correo se lo controla a través del Servidor de Correo Sendmail, este es de gran utilidad ya que además de prestar el servicio de correo, impide el ingreso de Spam y la utilización de generador de spam.

Las medidas para asegurar el servicio de correo pretenden:

- Proteger el servidor de ataques externos
- Proteger el servicio garantizando una correcta utilización de este.

El Sendmail es el agente de correo más conocido. Además consta de dos procesos con diferente propietario, Uno de propiedad del root y el otro de propiedad del usuario mail. Un ataque al proceso root del sendmail puede ocasionar graves problemas en el servidor como es la ejecución de programas con privilegios de Usuario Administrador.

A continuación se dan una serie de recomendaciones para proteger este servicio.

- **CREACIÓN DE HOSTS AUTORIZADOS**

Por medio de la configuración del sendmail se autorizara un grupo de dominios para que puedan realizar transferencias de correo por medio de un servidor principal.

Por ejemplo un distribuidor de servicios de Internet tiene un contrato con 2 empresas, las cuales les tiene que servir como servidor de correo. Estas empresas son:

espe.edu.ec y mitesis.com.ec

Para permitir que estos servidores puedan enviar correo se edita el archivo **/etc/mail/access** agregando estos dominios a la regla de permitido (RELAY)

El formato que se debe utilizar en este archivo esta dado por las siguientes reglas:
#<dir_email> < palabra clave >
#<dominio > < palabra clave >
#<dir_red> < palabra clave >

Estas palabras claves son:
OK (acepta los correos)
REJECT (Rechaza los correos)
RELAY (Implícitamente una aprobación con otras reglas)
DISCARD (el correo es descartado)

También se puede colocar texto para responder los correos enviados.

Un ejemplo de este archivo es:

cyberspammer.com	ERROR:"550 No aceptamos este tipo de correo"
sendmail.org	OK
192.168	RELAY
localhost.localdomain	RELAY
mitesis.edu.ec	RELAY
espe.edu.ec	RELAY

Como se puede apreciar en este mismo archivo se rechaza los correos entrantes de los dominios que se desee. Una vez definida estos datos se crea la base de datos con el comando "make" dentro del directorio "**/etc/mail**".

Existe una lista de las personas que envían correo basura esta lista es llamada "Realtime Blackhole List (RBL)" y es actualizada por los administradores de muchas partes del mundo. El inconveniente que tiene esta lista es que si algún servidor de una red determinada manda correo basura y el resto de la red no, toda la red puede estar señalada en la lista y por eso se estará rechazando algunos verdaderos correos.

Para activar este servicio se agrega la siguiente línea al archivo /etc/sendmail.mc

FEATURE(rbl)

Y se crea el archivo de configuración del sendmail el "sendmail.cf" por medio de:

linux:~ # m4 /etc/sendmail.mc > /etc/sendmail.cf

Para asegurar la integridad del correo que se envia y recibe; se ha considerado las utilidades que brindan los siguientes componentes:

- **SENDMAIL:** se utiliza como servidor de correo
- **SPAMASSASSIN:** Este permite evitar el ingreso de Spam.
- **CLAMAV:** Es un Antivirus que trabaja con el correo.

- **SENDMAIL:**

En nuestro caso de estudio sendmail se lo ha configurado para el envío y recepción de correo dentro de la LAN.

Así como también se han considerado los siguientes aspectos:

a) Establecer hosts autorizados

b) Creación de listas negras (direcciones indeseables y que pueden ser portadoras de virus)
c) Asociación a un Dominio (espe.com)

- **SPAMMASSASSIN**

SpamAssassin es una aplicación que analiza las diferentes partes de un mensaje de correo, empezando por la cabecera y pasando por cada parte del cuerpo del mensaje. Siguiendo una larguísima lista de reglas comprueba si las mismas se asemejan al contenido del mensaje. Según el porcentje de semejanza de las reglas con el mensaje, añade una línea en la cabecera del mismo indicando la puntuación que le otorga. Dicha puntuación es la puntuación de Spam, es decir, la valoración de "cuánto" de Spam contiene el mensaje.

SpamAsassin no elimina ningún mensaje, ni le recorta ningún trozo, ni toma ninguna determinación con respecto a su destino. Una vez puntuado lo entrega al POP3 (o al siguiente "agente intermediario"), con la cabecera modificada indicando la puntuación de Spam.

El spamassassin es un filtro basado en scripts en Perl que procesan los mensajes y detectan, en base a una reglas bastantes complejas, si el mensajes es un spam. El resultado de filtrar los mensajes es un puntaje, que si supera determinado valor (5.0 por defecto) es considerado un spam.

La mejor manera de hacerlo funcionar es arrancar el demonio `spamd` y comunicarse con él a través del spamc. De esta forma nos ahorramos varios ciclos de CPU arrancando el Perl.

- *CONFIGURACIÓN CON EL PROCMAIL*

Con toda la información descrita previamente se pueden aplicar filtros en el procmail del usuario, en el genérico para todo el sistema o en el propio cliente (MUA) de correo electrónico.

En éste caso se llama al spamc desde el **/etc/procmailrc** para hacerlo de forma global:

```
DROPPRIVS=yes
:0fw
| /usr/bin/spamc -f
```

Luego en el **$HOME/.procmailrc** se filtra los spams a una carpeta especial para que no moleste al recoger correo:

```
:0:
* ^X-Spam-Status: Yes
mail/spams
```

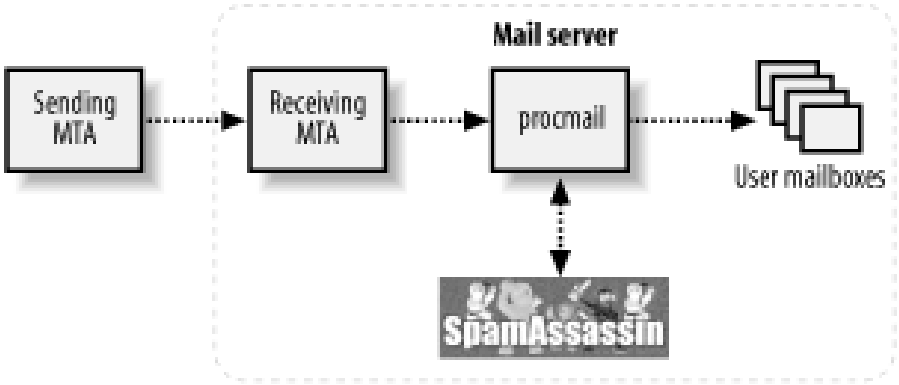


Gráfico 5.4 Proceso de Spamassassin

- **CLAMAV**

Clam AntiVirus, como el nombre indica, es una aplicación que examina ficheros para ver si contienen virus. Se ha escogido ClamAV como analizador de virus por dos razones:

```
1) Es GPL
2) La actualización se hace desde comandos del shell, por lo que se
   puede programar una Tarea Automática con Cron.
```

De igual forma que SpamAssassin, ClamAV también actúa como "agente intermediario" entre la recepción y la entrega de los mensajes de correo, de forma que tampoco tomará decisión alguna sobre el destino de los mismos. Simplemente los marcará si llevan adjunto algún fichero infectado con un virus, y los relegará al POP3 o al siguiente "agente intermediario".

Primero se instala el programa antivirus y se actualiza la base de datos de virus conocidos. Además, se comprueba que funciona correctamente antes de seguir con otros pasos. Para esto, y dando por entendido que esta conectado como administrador, se digita lo siguiente:

- **CONFIGURACIÓN PREVIA:**

Si es la primera vez que instalamos Clam entonces debemos crear un usuario y un grupo para él:

- groupadd clamav
- useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav

- **INSTALACIÓN:**

- Descomprimir las fuentes: *tar zxpvf clamav-x.yz.tar.gz*
- Si queremos que el archivo de configuración este en /etc, debemos indicarle: *./configure --sysconfdir=/etc*
- *make*
- *su -c 'make install'*

Listo, con eso tenemos instalado el clam.

- **PRUEBA:**

Para probarlo ejecutamos una busqueda de virus a traves del directorio de las fuentes:

clamscan -r -l scan.txt /usr/src/clamav-0.60/

Y el archivo resultante scan.txt debe contener algo así como:

Scan started: Thu Oct 2 18:42:28 2003
/usr/src/clamav-0.60//test/test1: ClamAV-Test-Signature FOUND
/usr/src/clamav-0.60//test/test1.bz2: ClamAV-Test-Signature FOUND
/usr/src/clamav-0.60//test/test2.zip: ClamAV-Test-Signature FOUND
/usr/src/clamav-0.60//test/test3.rar: ClamAV-Test-Signature FOUND
/usr/src/clamav-0.60//test/test2.badext: ClamAV-Test-Signature FOUND
-- summary --
Known viruses: 7846

Scanned directories: 38
Scanned files: 377
Infected files: 5
Data scanned: 6.19 Mb
I/O buffer size: 131072 bytes
Time: 9.945 sec (0 m 9 s)

Una vez que termine el proceso, entre otras cosas, este "port" instalará **clamscan** que es una forma de poder usar el antivirus desde la línea de comandos y contra los ficheros o directorios que queramos, un "demonio" llamado **clamd** que permitirá que otros programas le envíen ficheros y el comprobará si esos ficheros están o no infectados por alguno de los virus que **ClamAV** reconoce, y también **freshclam** que permite actualizar de forma automática la base de datos de virus conocidos.

Se inicia actualizando de forma manual la base de datos de virus, pues la que incluye **ClamAV** por defecto, no es más que de pruebas. Para esto, nada más fácil que teclear:

```
# freshclam
```

con lo que se visualiza algo similar a:

```
ClamAV update process started at Sat Apr 17 16:07:54 2004
Reading CVD header (main.cvd): OK
Downloading main.cvd [*]
main.cvd updated (version: 22, sigs: 20229, f-level: 1, builder:
tkojm)
Reading CVD header (daily.cvd): OK
Downloading daily.cvd [*]
daily.cvd updated (version: 265, sigs: 846, f-level: 1, builder:
tkojm)
Database updated (21075 signatures) from database.clamav.net
(195.70.36.141).
```

es decir, que se realiza una conexión a la base de datos de **ClamAV** y que se nos actualiza automáticamente nuestra base de datos de virus conocidos.

Ahora se debe comprobar como funciona el nuevo antivirus. Para esto ya no hace falta ser administrador, se conecta como usuario "normal", ubicarse en el directorio personal y teclea:

```
$ clamscan
```

de esta forma se verá que se testean todos los ficheros de el directorio */home*. Se puede añadirle a **`clamscan`** parámetros como ***-r* ó *-l*** que pueden ser interesantes (usar **`man clamscan`** para conocer las demás opciones).

Por cierto, si aún no se ha hecho **`make clean`** en ***/usr/ports/security/clamav*** se puede situar ahí y teclear **`clamscan -r`**. Verá que al menos se encuentra 5 ficheros infectados; pero no se asuste, estos ficheros vienen a modo de ejemplo para comprobar el correcto funcionamiento de **`ClamAV`** y no son realmente virus.

Por otra parte, para que estos cambios luego no den problemas al arrancar los "demonios", se realiza también lo siguiente:

```
# chown -R mailnull:mailnull /var/run/clamav/
# chown -R mailnull:mailnull /var/log/clamav/
# chown -R mailnull:mailnull /usr/local/share/clamav
```

También es conveniente hacer que tanto el arranque del "demonio" **`clamd`** como el proceso de actualización de la base de datos de `ClamAV` sea automático. Para esto, se añade las siguientes líneas al fichero */etc/rc.conf:*

```
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"
clamav_freshclam_flags="--checks=1 --
datadir=/usr/local/share/clamav \
                        --daemon-
notify=/usr/local/etc/clamav.conf"
```

Para probar que tal funcionan los cambios que hemos hecho se digita:

```
# /usr/local/etc/rc.d/clamav-freshclam.sh start
```

ahora se revisa el fichero */var/log/clamav/freshclam.log* y se debe ver algo como:

```
freshclam daemon started (pid=21264)
ClamAV update process started at Sat Apr 17 17:23:14 2004
main.cvd is up to date (version: 22, sigs: 20229, f-level: 1,
builder: tkojm)
daily.cvd is up to date (version: 266, sigs: 847, f-level: 1,
builder: tomek)
```

confirmándonos que todo está correcto.

De todas formas, para terminar la configuración de `ClamAV` aún nos queda otro pequeño cambio en el fichero */usr/local/etc/clamav.conf*. Busca la línea ***LocalSocket /var/run/clamav/clamd*** y cambiar por esta otra ***LocalSocket /var/spool/MIMEDefang/clamd.sock***

Una vez hecho esto, si se intenta arrancar `clamd` con:

```
# /usr/local/etc/rc.d/clamav-clamd.sh start
```

5.3 CONTROL DE ANCHO DE BANDA

El control ancho de banda se lo hace a través de squid en el parámetro disponible para acceso a Internet.

cache_dir (Cuanto almacenar Internet en el disco duro)

Este parámetro se utiliza para establecer que tamaño se desea que tenga el cache en el disco duro para Squid. Para entender esto un poco mejor, responda a esta pregunta: ¿Cuanto desea almacenar de Internet en el disco duro? Por defecto Squid utilizará un cache de 100 MB, de modo tal que encontrará la siguiente línea:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Se puede incrementar el tamaño del cache hasta donde lo desee el administrador. Mientras más grande el cache, más objetos de almacenarán en éste y por lo tanto se utilizará menos el *ancho de banda*. La siguiente línea establece un cache de 700 MB:

```
cache_dir ufs /var/spool/squid 700 16 256
```

Los números 16 y 256 significan que el directorio del cache contendrá 16 subdirectorios con 256 niveles cada uno. No modifique esto números, no hay necesidad de hacerlo.

Es muy importante considerar que si se especifica un determinado tamaño de cache y este excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente. Sea cauteloso con el tamaño de cache especificado.

V.4 ESCENARIOS DE PRUEBAS

Como resultado de la investigación, se experimentó con implementaciones en Sistemas Operativos. Se eligieron dos versiones de sistemas operativos sistemas populares y utilizados en el entorno Red Hat Linux 9.0 y Red Hat Enterprise Linux 4.0.

Las conexiones seguras host-to-host fueron probadas sobre Red Hat Linux 9.0 y Red Hat Enterprise Linux 4.0. Este proyecto tiene como principal objetivo hacer del Mail seguro y privado, apoyar la difusión y uso de Firewall, produciendo tecnología bajo esquemas de libre distribución para GNU/Linux y no sujeto a restricciones de exportación. Se considera una excelente alternativa para ser utilizado como plataforma base de desarrollo, de tal forma que este trabajo de tesis complemente una iniciativa ya con camino recorrido.

V.4.1. ESCENARIO HOST – TO – SERVER

Esta prueba se la realiza a través del envío de correo del host al servidor, así:

El host 192.168.1.2 envia un mensaje de correo a través del servidor de correo (Sendamil) el mismo que es recibido por el servidor 192.168.1.1; esta acción será ejecutada dentro de la zona militarizada.

El mensaje de correo será depositado en el repositorio de correo para luego acceder el servidor.

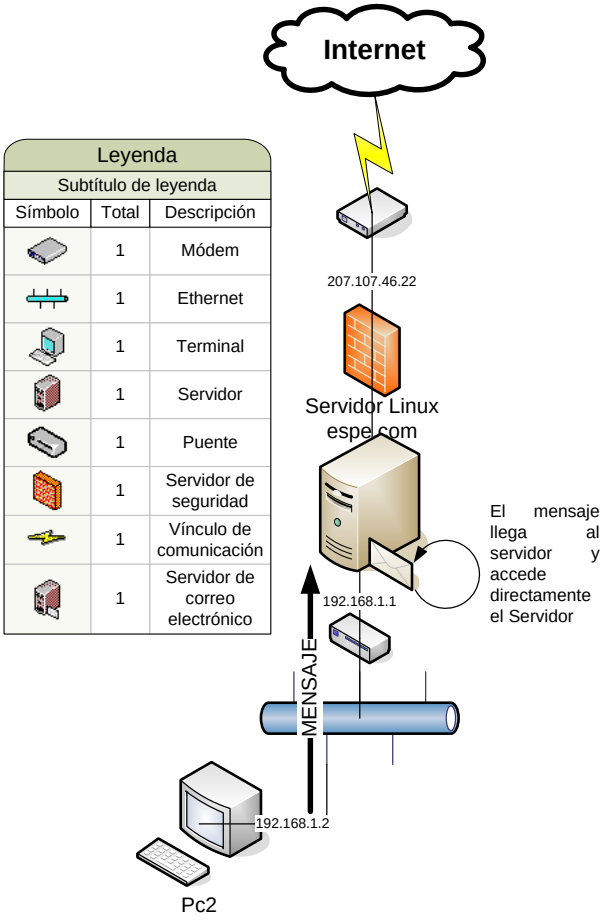


Gráfico 5.5 Escenario Host – to - Server

V.4.2. ESCENARIO SERVER TO HOST

En éste escenario el servidor envia un mensaje de correo al host 192.168.1.2; para acceder al mensaje el host recurre el repositorio del servidor en donde se encuentran todos los mensajes, luego de acceder al mensaje éste se borrará del servidor.

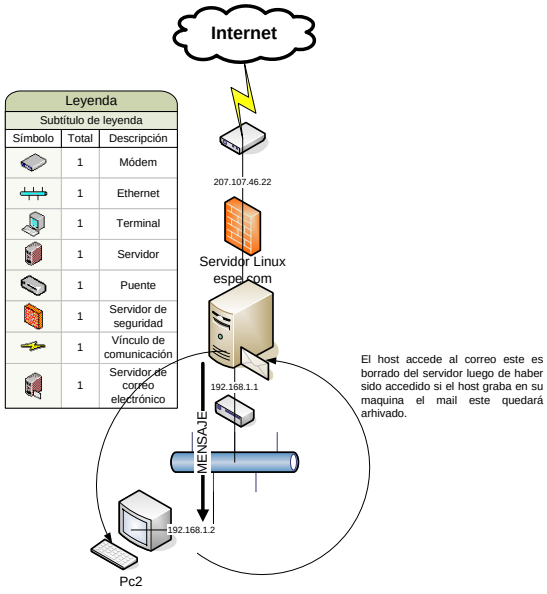


Gráfico 5.6 Escenario Server – to – Host

V.4.3. ESCENARIO SERVER TO SERVER

Esta prueba se la realiza enviando un correo desde el servidor espe.com al servidor mimesisespe.com, como el envio es entre servidores al llegar el mensaje este inmediatamente puede ser leido, luego de su llegada.

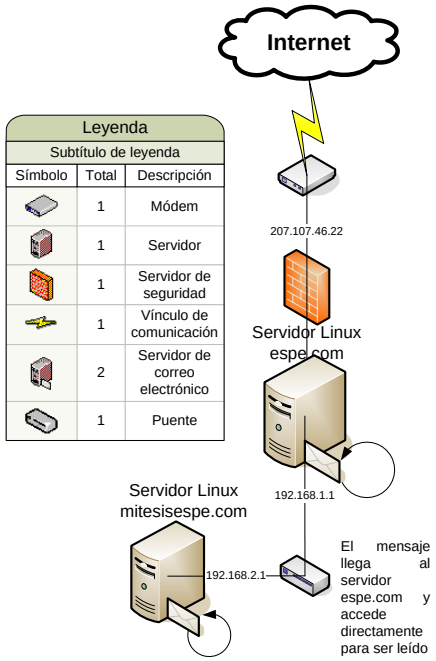


Gráfico 5.7 Esceneario Server – to – Server

V.4.4. ESCENARIO CONTROLADO (SOLUCIÓN)

Este escenario consiste en la solucion al problema encontrado; pues como vemos en el grafico se dispone de una red militarizada, a partir de ella todos los accesos a la red desde afuera se encuentran protegidos por el firewall; además el proxy Squid permite establecer un enmascaramiento de la red, para poder acceder al Internet, es decir, que al exterior la unica direccion IP que es visible es la 200.107.46.22 del servidor, y las demás máquinas se encuentran aisladas, en el entorno LAN todas son reconocidas y reciben los servicios implementados en el servidor.

Además los mails ingresados a la red y los que se envian entre los usuarios de la misma estan controlados por Spamassassin y Clamav.

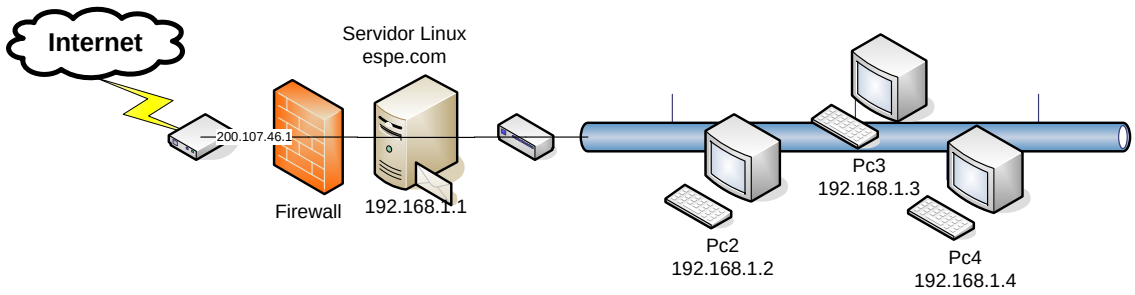


Gráfico 5.8 Escenario controlado

V.5 APLICABILIDAD DE LAS POLÍTICAS DEFINIDAS

De acuerdo a lo investigado las políticas aplicables en la red de la Microempresa W&M son las que a continuación se indican debido a la infraestructura y las necesidades de la misma.

5.5.1 PROTOTIPO OPERATIVO

El escenario en el cual se desarrollan las politicas establecidas está basado en los siguientes componentes:

- Sistema Operativo RET HAT ENTERPRISE LINUX 4.0
- Firewall
- Proxy Squid

- Acceso a Internet ADSL
- Control de ancho de banda

No Orden	Acción (B/A)	Fuente (IP)	Fuente (puerto)	Destino (IP)	Destino (puerto)	Opciones/ flags
1	acepta	192.168.1.2	*	192.168.1.1	80	*
2	acepta	192.168.1.2	*	192.168.1.1	25	*
3	bloquea	192.100.1.1	*	192.168.1.3	*	*

Tabla 5.2 Filtrado del Firewall

5.5.2 SERVICIOS

Los servicios que presta la red son:

- Servidor de Internet
- Administración de recursos de la red
- Control de virus y spam

CAPITULO VI

6.1 CONCLUSIONES

- La utilización de firewall es de gran ayuda ya que permite prevenir ataques informáticos y por ende pérdida de información.
- La implementación de políticas de seguridad ayuda a las organizaciones a dar un valor agregado a los servicios que presta, así como también crear un ambiente de confianza entre sus clientes.
- En este trabajo se ha abordado la aplicación de mecanismos de seguridad a través de protocolos y servicios, pudiendo apreciarse su funcionamiento en cada uno de los niveles del Modelo OSI.
- Se ha considerado un escenario real de pruebas con las ventajas inherentes de experimentar en un ambiente real, e interactuar directamente con otras nuevas tecnologías, los resultados obtenidos han contribuido a la consideración de Firewall, como una alternativa para brindar servicios de seguridad en el Internet en nuestro medio.
- Con el fin de entender la aplicación y funcionamiento de protocolos de seguridad, se estudió el modelo de comunicación OSI, la clasificación de mecanismos y modelos de aplicación de Seguridad en Redes y los protocolos de seguridad estándares.
- Se realizaron actividades para observar el comportamiento sobre los dos aspectos importantes al aplicar mecanismos de seguridad: seguridad y costo. Actividades de intrusión, análisis de tráfico y control de ancho de banda.
- La aplicación de Seguridad es indispensable en las redes públicas.
- La utilización de Linux es de gran ayuda ya que permite conocer de cerca y apreciarlas ventajas en relacion al costo de software.
- El aspecto más importante al buscar proteger una red, es la Política de Seguridad, que establece la misión de los recursos informáticos y define los niveles de protección deseados.
- Este trabajo de tesis representa una fuerte crecimiento profesional y personal al abordar uno de los temas que representan la Seguridad en redes.
-

6.2 RECOMENDACIONES

- Crear una Política de Seguridad donde se contemplen todos los usuarios, recursos de una red, instalar un Firewall como apoyo al control de acceso, monitoreo de la red y de bitácoras (loggs de transacciones) de sistemas.
- Los usuarios por su parte, deben proteger sus archivos sensibles de confidencialidad, aplicar candados o seguridades, claves para inicializar su computadora, claves robustas de usuario.
- Fomentar en los estudiantes el uso y propagación del Software Libre, ya que ello ayudará a disminuir costos y dejar de ser dependientes del software propietario.
- Con este trabajo de tesis, se inicia la labor de consultoría de los estudiantes y mi interés por seguir investigando sobre el Software Libre.

BIBLIOGRAFÍA:

FUENTES DE INFORMACIÓN:

REFRENDACIÓN

LATACUNGA JULIO 2006

_____

MIRYAN DORILA IZA CARATE
AUTORA

_____

ING. JOSÉ LUIS CARRILLO
DECANO DE LA FACULTAD DE
SISTEMAS E INFORMÁTICA

_____

DR. RODRIGO VACA
SECRETARIO ACADÉMICO
ESPE SEDE LATACUNGA