UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

FACULTAD DE CIENCIAS

DEPARTAMENTO DE COMPUTACIÓN

TRABAJO MONOGRÁFICO

TITULO:

DISEÑO DEL MODELO SEGURIDAD DEL SISTEMA DE INFORMACIÓN DE LA UNAN-LEÓN

ELABORADO POR:

- **Bra. LIDIA PATRICIA LÓPEZ CARMONA.**
- **Bra. MARTHA MARÍA CARMONA.**

TUTOR:

ING. MARCOS ANTONIO CÁRCAMO NARVÁEZ.

León, Septiembre 2003

INDICE

AGRADECIMIENTO

A **DIOS** por darnos la vida y las oportunidades que han hecho que nuestros sueños y vocaciones se hagan realidad y toda la fuerza, inteligencia y confianza para poder coronar nuestra carrera y por estar con nosotras en todos aquellos momentos de alegría y sufrimiento.

A nuestros **PADRES** ya que sin la ayuda de ellos no hubiese sido posible lograr coronar nuestra carrera universitaria, por estar siempre a nuestro lado apoyándonos para salir adelante y lograr la realización de una de todas nuestras metas.

A nuestro Tutor **Ing. MARCOS ANTONIO CARCAMO NARVAEZ**, por habernos tenido paciencia y por darnos toda la información necesaria para poder realizar este trabajo monográfico.

A nuestro profesor **Lic. NESTOR CASTRO,** por ayudarnos cuando más lo necesitábamos para configurar el Firewall.

A nuestros **AMIGOS** que de una u otra manera nos apoyaron a lo largo de nuestra carrera.

DEDICATORIA

A **DIOS** nuestro padre celestial, por ser el que nos ha inspirado durante los tiempos de sufrimiento y dolor; sobre todo por darnos la vida y las oportunidades que han hecho que nuestros sueños y vocaciones se hagan realidad y toda la fuerza, inteligencia y confianza para poder coronar nuestra carrera.

A nuestras madres **OLGA ESPERANZA CARMONA PINEDA Y MARÍA ELENA CARMONA PINEDA** por ser una fuente de esperanza y apoyo, que nos dieron animo para ir detrás de nuestra pasión, quienes confiaron en nosotras para que encontráramos nuestro propio camino cuando pasábamos apuros con los problemas propios.

A nuestros **HERMANOS, HERMANAS Y DEMÁS FAMILIARES** que nos han brindado su apoyo en todo momento.

A nuestro querido tutor y amigo **Ing. MARCOS ANTONIO CARCAMO NARVAEZ** por ser un amigo constante y una fuente de animo. Por su generosidad a la hora de dedicar semanas a la revisión de la tesis.

CAPITULO I. GENERALIDADES

I. INTRODUCCION.

II. ANTECEDENTES Y JUSTIFICACION.

III. OBJETIVOS DEL PROYECTO.

IV. METODOLOGIA.

I. INTRODUCCIÓN.

Cuando Internet subió rápidamente de las cenizas de ARPANET ganó popularidad entre las universidades e investigadores como una manera de comunicación rápida y conveniente de información y recursos. La seguridad no era un problema.

La eclosión en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la seguridad informática cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestro ordenador se conecta a Internet, se abren ante nosotros toda una nueva serie de posibilidades, sin embargo éstas traen consigo toda una serie de nuevos y en ocasiones complejos tipos de ataque. Más aun, mientras en un ordenador aislado el posible origen de los ataques es bastante restringido, al conectarnos a Internet, cualquier usuario de cualquier parte del mundo puede considerar nuestro sistema un objetivo apetecible.

El número de incidentes se ha doblado todos los años durante los últimos cinco años. Éste es un resultado de que administradores de sistemas estén desprevenidos de los peligros al conectar una computadora (o red) a Internet, combinado con la falta de entrenamiento de cómo abastecer de seguridad a las computadoras correctamente. Es vital conocer a su enemigo para ser capaz de tomar las medidas correctas.

La tecnología día a día va creciendo de una manera considerable y rápida, todos debemos de estar a la altura de la misma para poder estar actualizados. La UNAN – León ha sido una de las Universidades preocupadas por su desarrollo tecnológico y sus mejoras por el bien de la misma y de sus estudiantes.

Desde el año 1989 se empezó a desarrollar el área de informática, pero fue hasta en 1994 que se estableció lo que ahora es la división de Informática. Esta división ha desarrollado muchas aplicaciones a beneficio de toda la Universidad, siendo la más reciente la instalación de la Red de voz y datos de la UNAN – León.

La red es el medio (vía) que permite la comunicación entre los diferentes ordenadores (diferentes áreas y usuarios) conectadas a ella, la información que circula a través de la red debe llegar a su destino ***correctamente*** y sin peligro de ser “Alterada”, “Robada”, “Atacada”, etc. de igual forma deben permanecer dentro de bases de datos.

Aquí es donde entra en juego lo que es “Seguridad”, que es un proceso muy amplio que va desde los detalles mas mínimos como la eliminación de documentos que contengan información critica (ejemplo un password), hasta el de proteger nuestra red completa (Intranet) del exterior (Internet).

Una red confiable debe brindar seguridad básica como: Seguridad de la Información (Datos que circulan por ella) y Seguridad de ella misma (dispositivos, etc). Resolver los problemas de seguridad en una red es el elemento más importante después que se tiene instalada. Determinar por ejemplo quienes son nuestros verdaderos enemigos (intrusos) es una tarea difícil sobre todo porque no solo tenemos intrusos del exterior (Por medio de Internet) sino que muchas veces los mismos usuarios de nuestra red pueden ser nuestros atacantes.

En este trabajo trataremos de resolver este problema de la manera más comprensible y fácil; viendo la Seguridad desde dos áreas de aplicación:

- Seguridad en la Intranets.
- Seguridad de Internet.

Enfatizando nuestro trabajo en lo referente a la Seguridad en la Intranet.

Considerando las limitantes existentes en la institución a nivel Económico, se presenta la iniciativa de realizar este trabajo utilizando las herramientas de software fácilmente accesibles. En este sentido, nuestro grupo de trabajo elaboro con sentido practico la formulación y evaluación del diseño de la seguridad, esperando sea aceptada y así aprovechar nuestro interés en establecer un mejor nivel de seguridad de la red de la Unan-León.

II. ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

a. Antecedentes del Proyecto.

1989: Se desarrolló el sistema de información para la elaboración de cheques y nóminas de la UNAN – León, dando origen a la Unidad de Cómputos.

1991: Se elevó la Unidad de Cómputo a oficina al ampliarse sus funciones.
Se inició el desarrollo de un sistema de inventario.
Se instaló en la Facultad de Ciencias un laboratorio con máquinas 80286 prestadas por el CSE.

1993: Se desarrolló el Sistema Automatizado de Registro Académico.

1994: Se creó la División de Informática y el Departamento de Computación.
Se inició la carrera de Licenciatura en Computación.
Se implementó una Red Local en el Recinto Central de la UNAN con cable coaxial y topología bus.
Se tenía acceso a Internet a través de conexión PPP con Nicarao, UNI y al Nodo de la OPS (Organización Panamericana de la Salud)

1996: Se instaló un nodo propio de Internet.

1997: Se inició la interconexión de los diferentes Campus Universitarios al nodo de Internet.

2000: Se cambió la conexión anterior a una inalámbrica entre Edificio Central y el Campus Médico surgiendo así la Red de Voz y Datos vía radio enlace a frecuencia regulada.

2001: Se realizó la conexión de Radio Enlace del Campus Agropecuario al Edificio Central (E1).

2002: Adquisición de 300 PC.
Apertura de la carrera de Ingeniería de Sistemas.
La facultad de derecho, Anexo de derecho y el HEODRA se interconectan al nodo central con tecnología HDSL.

2003: Actualmente la UNAN-León cuenta con 560 personas empleadas como personal académico y 550 personas como personal administrativo.
En lo orgánico está formada por 7 facultades, 3 escuelas y 4 Vice-rectorías, general, de Investigación y Desarrollo, cooperación externa y la académica.

Además cuenta con más de 800 computadoras, de las cuales más del 50% se encuentran conectadas a la red local, además de contar con 300 usuarios que se conectan a la red vía Internet.
Se interconectan al nodo central el Antiguo edificio del CIP (Control Integrado de Plaga) y bienestar estudiantil con cable coaxial.
A excepción de la facultad de ciencias de la educación, el resto de las facultades están conectadas directamente a la red.

Desde que se creó la red de informática de la UNAN-León hace ya muchos años, la falta de un buen diseño de seguridad para la red, ha sido uno de los problemas que se han investigado muy poco a pesar de ser muy requerido.

b. Justificación del Proyecto.

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Universidad. Sin ellos la universidad quedaría completamente desorientada. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos.

Las razones expuestas a continuación fundamentan la necesidad de ejecución del presente proyecto:

- El sistema actual no logra controlar el ataque que recibe por parte de intrusos internos o externos.

- La Red de Informática de la Universidad, no logra dar una máxima confiabilidad en lo que se refiere a la seguridad y disponibilidad de servicios.

- Debido al creciente desarrollo de la tecnología de comunicación e informática se hace necesario mejorar los niveles de seguridad de la red que satisfaga los requerimientos de los usuarios y para que esta sea capaz de ser competitiva en el ámbito internacional.

- La red actual es atacada constantemente por virus y el sistema no es efectivo ante estos ataques.

- El nivel económico de la universidad requiere que se elabore un modelo de seguridad acorde a sus necesidades, así como también a sus recursos económicos.

Si se logra realizar la ejecución del proyecto, podríamos mejorar las condiciones de seguridad de la red de informática de la universidad.

III. OBJETIVOS DEL PROYECTO

a. Objetivo General.

Diseñar un modelo de seguridad del SI en la UNAN-León, para garantizar una mayor Confiabilidad, Disponibilidad e Integridad de la información en la institución.

b. Objetivos Específicos.

- Crear un SI basados en las posibilidades económicas de la universidad.
- Mejorar la calidad de seguridad informática de forma oportuna y satisfactoria.
- Definir una metodología estándar para realizar un modelo de seguridad que se adapte a las necesidades propias de la institución.
- Evaluar las posibles amenazas y vulnerabilidades que pueden ocurrir dentro de la red informática.
- Definir estrategias de Prevención, Detección y Corrección.
- Reducir el porcentaje de inseguridad y accesos no autorizados en la red de la universidad.
- Demostrar la importancia del uso de los Firewalls en la red.
- Proveer una fuente bibliográfica para futuras investigaciones.

IV. METODOLOGIA

El método que utilizaremos durante el desarrollo de nuestro proyecto es el "Método Científico General", que contribuye a establecer la estrategia de investigación, por ejemplo cuando se aborda un problema desde este punto de vista sistemático, nos ayuda a comprender sus componentes internos, su totalidad y relación con el medio externo. Es una metódica ordenada y coherente.

Mecanismos para recopilar Información serán:

1. Entrevistas con usuarios y expertos en la materia.
2. Consultas Bibliográficas.
3. Pruebas experimentales.

Para nuestro trabajo usaremos la siguiente metodología que se basa en la realización de los procedimientos del diseño que son 5 y se mencionarán a continuación, además de las posibles preguntas que se deben tomar en cuenta al realizar el diseño:

1. Establecer una política de seguridad.

¿Qué debemos proteger y cómo?

2. Análisis de las vulnerabilidades y amenazas posibles a la seguridad.

¿Qué es lo que ocurre con frecuencia?
¿Cuáles son nuestras debilidades?

3. Estudio de las contramedidas antes las vulnerabilidades y amenazas.

¿Qué debemos hacer y cómo debemos implementar dichas medidas?

4. Implementación de las medidas y tests

¿Son efectivas las medidas de seguridad tomadas?
¿Qué herramientas podemos usar?

5. Entrenamiento de usuarios, operación y administración, auditoria del sistema.

¿Hay problemas durante la operación?
¿Existe un plan de contingencia?

CAPITULO II. MARCO TEORICO

I. SISTEMAS

II. SEGURIDAD DE LOS SISTEMAS DE INFORMACION

III. DESARROLLO TEORICO DEL MODELO DE SEGURIDAD

I. SISTEMAS

Debido a que nuestro propósito final es el diseño de un modelo de seguridad para un SI, abordaremos la temática desarrollando los elementos que constituyen dicho modelo.

1. Teoría de los Sistemas

La teoría general de sistemas (T.G.S.) surgió con los trabajos del biólogo alemán Ludwig von Bertalanffy, publicados entre 1950 y 1968.

La T.G.S. Se fundamentan en tres premisas básicas:

a) Los sistemas existen dentro de sistemas.
b) Los sistemas son abiertos.
c) Las funciones de un sistema dependen de su estructura.

Sistema

La palabra “sistema” tiene muchas connotaciones: un conjunto de elementos interdependientes e interactúantes; un grupo de unidades combinadas que forman un todo organizado y cuyo resultado (output) es mayor que el resultado que las unidades podrían tener si funcionaran independientemente.

Los sistemas deben ser altamente homeostáticos y deben evolucionar permanentemente para evitar la entropía.

La homeostasis es la propiedad de un sistema que define su nivel de respuesta y de adaptación al contexto.

La entropía de un sistema es el desgaste que el sistema presenta por el transcurso del tiempo o por el funcionamiento del mismo. Los sistemas altamente entrópicos tienden a desaparecer por el desgaste generado por su proceso sistémico. Los mismos deben tener rigurosos sistemas de control y mecanismos de revisión, reelaboración y cambio permanente, para evitar su desaparición a través del tiempo.

Tipos de Sistemas

Existe una gran variedad de sistemas y una amplia gama de tipologías para clasificarlos, de acuerdo con ciertas características básicas.
En cuanto a su constitución, los sistemas pueden ser físicos o abstractos:

a) Sistemas físicos o concretos: Cuando están compuestos por equipos, por maquinaria y por objetos y cosas reales. Pueden ser descritos en términos cuantitativos de desempeño.
b) Sistemas Abstractos: Cuando están compuestos por conceptos, planes, hipótesis e ideas. Aquí, los símbolos representan atributos y objetos, que muchas veces solo existen en el pensamiento de las personas.

En realidad el sistema físico (Hardware) opera en consonancia con el sistema abstracto (Software).

2. Sistemas de Información

El concepto de "Información" es la noción central de la cibernética. La información es uno de los elementos primordiales en un sistema de información, su clasificación es indispensable dentro de dichos sistemas, ya que se deben definir niveles de acceso a la información almacenada, esto nos permite asegurar que la información estará disponible para cada uno de los usuarios según sea su perfil (Nivel). Dichos niveles se determinaran de acuerdo a las características tanto del sistemas como de los usuarios.

¿Qué entendemos por sistemas de comunicación e información?

Son sistemas integrados que poseen entradas, canales de comunicación por los cuales circulan los datos, unidades de control y procesamiento, salidas, resultados.

Elementos claves de la Tecnología de la Información: procesamiento de datos, automatización de oficinas, telecomunicaciones, inteligencia artificial y la tecnología Internet-Intranet-Extranet, desarrollos multimedia.

La combinación de la técnica de información con personas agrupadas para alcanzar objetivos determinados o para el control, forman el llamado *Sistema de Información automatizado,* al cual, de acuerdo con las necesidades, se conectan los abonados (personas o dispositivos) que suministran o utilizan dicha información.

Los Sistemas de Información que funcionan sin la participación de personas se llaman *Automáticos*. En tales sistemas la persona solo desempeña funciones de control o utilizan dicha información.

Un Sistema de Información *automatizado* se transforma en sistema automatizado de mando (SAM) si la información suministrada se obtiene de un objeto (proceso) cualquiera, mientras que la información de salida se utiliza para variar (con cierto fin) el estado de ese mismo objeto (proceso).

Los Sistemas de Información automatizados y los SAM han encontrado amplia aplicación en todas las ramas de la economía.

Hoy en día tiene lugar un intenso proceso de integración de semejantes sistemas con el fin de formar sistemas de empresas productivas y en adelante integrar sistemas de una rama o de un departamento de producción.

Clasificación de los sistemas Automatizados de Información

- De Procesos Tecnológicos
- De Procesos Informativos
  - Sistemas de Información Gerenciales(Contables, Recursos Humanos, Transporte, Inventario, Registro Académico, Etc.)
  - Sistemas de Información Documentales
  - Sistemas de Información Estadísticos
  - Sistemas de Información Gráficos
  - Sistemas Web
  - Sistemas Mixtos
  - Sistemas para la Toma de Decisiones

Tecnologías de la Información y Comunicaciones (TIC)

En los albores del desarrollo de las computadoras y procesos conexos hablamos de centros de cómputos donde se procesaba la información vital de las empresas u organización (Contabilidad, recursos humanos, inventario, etc), posteriormente surgieron los centros o departamentos informáticos (**infor**mación y tele**mática**), con el desarrollo de la tecnología éstas tienden a integrarse y surge un nuevo concepto: TIC.

Las TIC Se basan en la integración de las tecnologías digitales tanto de la información como de las comunicaciones, podemos definirlas como una fusión de los sistemas de información con los sistemas de comunicación.
Las tecnologías de la información que integra son: voz, datos y video.
Las tecnologías de la comunicaciones que integra son las diferentes técnicas de comunicación:

Satélites (GEO, MEO, LEO, ZEPELLIN)
Terrestres (COBRE, FO, RDI)
Inalámbricas (PAGING, CELULAR, TRUNKING)

3. Eficiencia de los SI

Modelo RASIS

La Eficiencia de los sistemas de información esta basada en cinco conceptos. Combinando estos conceptos son llamados RASIS.

Reliability	(Fiabilidad)
Availability	(Disponibilidad)
Serviceability	(Disponibilidad de Servicios)
Integrity	(Integridad)
Security	(Seguridad)

RASIS es un modelo que debe seguir todo sistema de información que desee brindar: Fiabilidad, Disponibilidad, Disponibilidad de Servicio, Integridad y Seguridad. La clave para mejorar la fiabilidad está en como el modelo RASIS es aplicado de forma apropiada. El nivel de fiabilidad requerido de un sistema variará según la actuación del sistema y los usuarios y de las condiciones requerida.

Fiabilidad: El objetivo de fiabilidad es minimizar la ocurrencia de fracasos del sistema durante los funcionamientos.
La medida es el MTBF: Tiempo medio entre caída del sistema. Entre mayor el MTBF es, la fiabilidad será mejor.

Disponibilidad: Permite la operación continua del sistema lo mas prolongado posible sin paros, incluso si un fallo ocurre.

Disponibilidad de Servicio: Habilita el descubrimiento temprano y las reparaciones tempranas de faltas a través del mantenimiento simple.
La medida es el MTTR: Tiempo medio de recuperación del sistema. Entre más corto es la MTTR, la disponibilidad de servicio superior es.

Integridad: El objetivo de integridad es mantener la consistencia de los datos. Por ejemplo, después de procesar las transacciones múltiples simultáneamente, los datos puestos al día podrían ser incoherentes.
No hay ninguna medida de la evaluación general.

Seguridad: Asegurará el incremento de la protección de las características de privacidad y resguardo de los datos.
No hay ninguna medida de la evaluación general.

4. Importancia de la Información

Las empresas dependen hoy en día de los equipos informáticos y de los datos que hay allí almacenados. Dependen también cada vez más de las comunicaciones a través de redes de datos.
Si falla el sistema informático y no puede recuperarse, la empresa puede desaparecer.

La información de una empresa o institución se entenderá como:

- Todo el conjunto de datos.
- Todos los mensajes intercambiados.
- Todo el historial de clientes y proveedores.
- Todo el historial de productos.
- Toda la contabilidad de la empresa…. etc.

Si esta información se pierde o deteriora, le será muy difícil a la empresa recuperarse y seguir siendo competitiva. El éxito de una empresa dependerá de la calidad de la información que genera y gestiona.

II. SEGURIDAD DE LOS SISTEMAS DE INFORMACION (SI)

El tema de seguridad es el de mayor importancia dada la difusión informática, la proliferación de redes y la sensibilidad de la información almacenada y transmitida en un número creciente de empresas públicas y privadas. Prácticamente en todas las organizaciones en las cuales la informática juega un papel vital, el tema de la seguridad ocupa hoy en día una prioridad muy alta.

Existe un acuerdo y conciencia general sobre la importancia de la Seguridad de los Sistemas de Información (SSI). La SSI está relacionada con la disponibilidad, confidencialidad e integridad de la información tratada por los ordenadores y las redes de comunicación. Se usan comúnmente otros términos que en esencia tienen el mismo significado, tales como seguridad de la información, seguridad de los ordenadores, seguridad de datos o protección de la información, pero en aras de la consistencia, usaremos el término Seguridad de los Sistemas de Información o Seguridad Informática en las páginas siguientes.

Hay 2 categorías de la seguridad, seguridad en un **sentido amplio** y seguridad en un **sentido estrecho.**

La Seguridad en un Sentido Amplio: Para proteger los sistemas de información de todos los tipos de “amenazas” incluso los fuegos, terremotos, los fallos en la alimentación de corriente, etc.

La Seguridad en un Sentido Estrecho: Afianzando y Manteniendo la Confidencialidad, la Integridad, la disponibilidad (la seguridad de información).
Prevenir el acceso desautorizado, el goteo de información, etc.
No incluye las catástrofes naturales. El objetivo de “la seguridad” se limita principalmente a la seguridad en el sentido estrecho. Aquí “la seguridad” también se llama generalmente “la seguridad de Información”.

Seguridad informática

Debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información o de sus sistemas de tratamiento. Apuntaremos sólo dos ejemplos de esta vulnerabilidad creciente. Primero, con la gran expansión del uso de ordenadores personales se ha magnificado el problema de la SSI, debido sobre todo a la carencia de controles de seguridad básicos en este tipo de sistemas. En segundo lugar, la evolución hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre organizaciones distintas, plantea retos importantes a la gestión de la seguridad. Los riesgos fundamentales asociados con la incorrecta protección de la información son:

- Revelación a personas no autorizadas
- Inexactitud de los datos
- Inaccesibilidad de la información cuando se necesita

Estos aspectos se relacionan con las tres características que debe cubrir un SI seguro: *confidencialidad, integridad y disponibilidad*. Así pues, preservar estas tres características de la información constituye el objetivo de la seguridad.

Los problemas técnicos, las amenazas ambientales, las condiciones de instalación desfavorables, los usuarios, la situación política y social, son otros tantos factores susceptibles de poner en peligro el buen funcionamiento de los SI. Las amenazas a los SI van desde desastres naturales tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos, virus, con un origen tanto interno como externo.

1. Definición de Seguridad Informática

La definiremos, como la estructura de control establecida para gestionar la disponibilidad, integridad, confidencialidad y consistencia de los datos, sistemas de información y recursos informáticos. Dependiendo del tipo de sistema informático con el que tratemos (militar, comercial, bancario, etc), el orden de importancia de estos tres factores es diferente, e incluso entran en juego otros elementos como la autenticidad o el no repudio.

Definición operacional: Un ordenador es seguro si podemos contar con que su hardware y su software se comporten como se espera de ellos.

2. Servicios de Seguridad

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

Confidencialidad

Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

La confidencialidad, a veces denominada secreto o privacidad, se refiere a la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

En áreas de seguridad gubernamentales y universidades el secreto asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad, normalmente impuestas por disposiciones legales o administrativas.

En entornos de negocios, la confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc.

Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa. En estos entornos los otros dos aspectos de la seguridad son menos críticos.

Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son, por ejemplo:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

Integridad

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

Suelen integrarse varios conceptos análogos en este segundo aspecto de la seguridad:

- Precisión
- Integridad
- Autenticidad

Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado.

De hecho el problema de la integridad no sólo se refiere a modificaciones *intencionadas*, sino también a *cambios accidentales* o no intencionados.

En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la *autenticidad*. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos.

En el entorno financiero o bancario, este aspecto de la seguridad es el más importante. En los bancos, cuando se realizan transferencias de fondos u otros tipos de transacciones, normalmente es más importante mantener la integridad y precisión de los datos que evitar que sean interceptados o conocidos (mantener la confidencialidad).

Autenticidad.

En el campo de la criptografía hay diversos métodos para mantener/asegurar la autenticidad de los mensajes y la precisión de los datos recibidos. Se usan para ello códigos/firmas añadidos a los mensajes en origen y recalculadas/comprobadas en el destino. Este método puede asegurar no sólo la integridad de los datos (lo enviado es igual a lo recibido), sino la autenticidad de la misma (quién lo envía es quien dice que es).

Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro.

Disponibilidad

Se entiende por disponibilidad:

- El grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.
- La situación que se produce cuando se puede acceder a un SI en un periodo de tiempo considerado aceptable.

Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo.

Lo opuesto a disponibilidad, y uno de los posibles métodos de ataque a un sistema informático, se denomina "denegación de servicio" (*denial of service*). Una denegación de servicio significa que los usuarios no pueden obtener del sistema los recursos deseados:

- El ordenador puede estar estropeado o haber una caída del SO.
- No hay suficiente memoria para ejecutar programas.
- Los discos, cintas o impresora no están disponibles o están llenos.
- No se puede acceder a la información.

De hecho, muchos ataques, como el caso del gusano de 1988, no buscaban borrar, robar, o modificar la información, sino bloquear el sistema creando nuevos procesos que saturaban recursos.

3. Otros Aspectos Relacionados

Existen otros aspectos o características de la seguridad que pueden en su mayor parte incluirse o asimilarse a uno de los tres aspectos fundamentales, pero que es importante concretar en sí mismos.

Imposibilidad de rechazo (no-repudio)

Esta propiedad permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante terceros que no la envió o la recibió.

Esta propiedad y la anterior son especialmente importantes en el entorno bancario y en el uso del comercio digital.

Consistencia

Asegurar que el sistema se comporta como se supone que debe hacerlo con los usuarios autorizados. Si el software o el hardware de repente comienzan a comportarse de un modo radicalmente diferente al esperado, puede ser un desastre. Por ejemplo si la orden "ls" (comando Linux para listar archivos) comenzara a borrar los ficheros listados.

Esta propiedad es amenazada por ejemplo por el uso de los Caballos de Troya. Programas que no hacen lo que se supone que deben hacer, o que además se dedican a otras tareas.

Aislamiento

Regula el acceso al sistema, impidiendo que personas no autorizadas entren en él. Este aspecto está relacionado directamente con la confidencialidad, aunque se centra más en el acceso al sistema que a la información que contiene.

Auditoria

Capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema, y quién y cuándo las han llevado a cabo. La única forma de lograr este objetivo es mantener un registro de las actividades del sistema, y que este registro esté altamente protegido contra modificación.

4. Principios Fundamentales de la Seguridad Informática

Ningún equipo conectado a la red está seguro de abuso y debe ser considerado como un riesgo potencial. Aun cuando no es un riesgo de seguridad hoy, el podría ser mañana. Una regla dorada es esa seguridad siempre es más fácil instalar y mucho más barato mantener si se hace cuando un equipo se instala o un programa es escrito que remendarlo después. Se debe poner la seguridad en la agenda cotidiana.

Principio de menor privilegio

Por ejemplo, en un sistema UNIX el usuario necesita acceder al fichero */etc/passwd*, donde normalmente se guarda su password, para poder entrar al sistema. Sin embargo, durante el resto de su trabajo en el sistema no necesita acceder a los passwords. Siguiendo el principio de menor privilegio debería evitarse este acceso o bien situar los passwords cifrados en otro fichero. De hecho la mayoría de los sistemas UNIX no aplican esta medida de seguridad y permiten que cualquier usuario pueda consultar todos los passwords cifrados en cualquier momento.

La seguridad no se obtiene a través de la oscuridad

Al dejar nuestro computador o red aislada no podemos decir que estamos poniendo seguridad en nuestra red.

Principio del eslabón más débil

Por ejemplo, supongamos que establecemos una política de asignación de passwords muy segura, en la que estos se asignan automáticamente, son aleatorios y se cambian cada semana. Si en nuestro sistema utilizamos la red Ethernet para conectar nuestras máquinas, y no protegemos la conexión, no nos servirá de nada la política de passwords establecidas. Por defecto, por Ethernet los passwords circulan descifrados. Si cualquiera puede acceder a nuestra red y "escuchar" todos los paquetes que circulan por la misma, es trivial que pueda conocer nuestros passwords. En este sistema el punto débil es la red. Por mucho que hayamos reforzado la seguridad en otros puntos, el sistema sigue siendo altamente vulnerable.

Defensa en profundidad

Por ejemplo en nuestro sistema podemos establecer un mecanismo de passwords altamente seguro como primera barrera de seguridad. Adicionalmente podemos utilizar algún método criptográfico fuerte para cifrar la información almacenada. De este modo cualquier atacante que consiga averiguar nuestro password y atravesar

la primera barrera, se encontrará con la información cifrada y podremos seguir manteniendo su confidencialidad.

Seguridad en caso de fallo

Por ejemplo, si nuestros mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario que dejen pasar a cualquiera aunque no esté autorizado.

Simplicidad

La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

III. DESARROLLO TEORICO DEL MODELO DE SEGURIDAD

Para la creación de un modelo de seguridad existe una metodología a seguir, la cual esta integrada de 5 temas:

1. Establecer una política de seguridad.
2. Análisis de las vulnerabilidades y amenazas posibles a la seguridad.
3. Estudio de las contramedidas antes las vulnerabilidades y amenazas.
4. Implementación de las medidas y tests
5. Entrenamiento de usuarios, operación y administración, auditoria del sistema.

A continuación se desarrollará el marco teórico de cada uno de estos, en el orden estipulado.

1. Políticas de Seguridad

Cada día es mayor la **importancia de la información**, especialmente relacionada con sistemas basados en el uso de tecnología de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la revelación de la información y otras incidencias, tienen un impacto mucho mayor que hace unos años: de ahí la necesidad de **protecciones adecuadas** que se evaluarán y recomendarán dentro de las políticas de seguridad.

Si no existen suficientes y adecuadas medidas de protección se puede perder información vital, o al menos no estar disponible en el momento requerido de aquí surge la necesidad de tener un esquema que nos permita asegurar la Integridad, Disponibilidad, Confiabilidad de nuestra red.

La protección no debe basarse solo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando por la mentalización a los directivos para que, en cascada, afecte a todo los niveles de la pirámide organizativa.

El punto base sobre el cual debemos comenzar a tratar el tema de la seguridad de los sistemas de información (trata los riesgos informáticos o creados por la informática) son las políticas de seguridad.

Las políticas son orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.
La seguridad son mecanismos que aseguran un buen funcionamiento (exento en todo peligro, daño o riesgo).

Las políticas de seguridad son documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de computo, las responsabilidades y derechos tanto de usuarios como de administradores, describe **lo que se va a proteger** y de lo **que se esta tratando de proteger**, estos documentos son el primer paso en la construcción de Firewalls efectivos (el Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataques).

Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Estos documentos nos permitirán describir cada uno de los elementos del sistema que debemos proteger, como Prevenirlos, Detectarlos y Corregirlos.

De tal forma que podamos asegurar la integridad de los datos así como del sistema mismo. En muchos casos las políticas definen metas u objetivos generales que luego se alcanzan por medio de medidas de seguridad.

El software y el hardware utilizados en una red son una parte importante de la seguridad, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas", que cada empresa u organización debe generar.

Si bien las políticas varían considerablemente según el tipo de organización de que se trate, en general incluyen declaraciones generales sobre metas, objetivos, comportamiento y responsabilidades de los empleados en relación a las violaciones de seguridad. A menudo las políticas van acompañadas de normas, instrucciones y procedimientos.

En general, las políticas definen las áreas sobre las cuales debe enfocarse la atención en lo que concierne a la seguridad. Las políticas podrían dictar que todo el software desarrollado o adquirido se pruebe a fondo antes de utilizarse. Se necesitará tomar en cuenta varios detalles sobre cómo aplicar esta política.

1.1 ¿Por qué Son Importantes las Políticas?

a) Porque aseguran la aplicación correcta de las medidas de seguridad

Con la ilusión de resolver los problemas de seguridad, en muchas organizaciones simplemente se compran uno o más productos de seguridad. Luego que se instalan los productos, sin embargo, se genera una gran desilusión al darse cuenta que los resultados esperados no se han materializado. Por ejemplo supóngase que una organización ha adquirido un producto de control de acceso para una red de computadoras. La sola instalación del sistema hará poco para mejorar la seguridad. Se debe primero *decidir cuáles usuarios deben tener acceso a qué recursos de información.* También deben establecerse los procedimientos para que el personal técnico implante el control de acceso, además debe definir la manera de revisar las bitácoras (logs) y otros registros generados por el sistema. Éstas y otras medidas constituyen parte de la infraestructura organizativa necesaria para que los productos y servicios de seguridad sean efectivos.

Una empresa necesita de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad. Las políticas y una estimación preliminar de los riesgos son el punto de partida para establecer una infraestructura organizativa apropiada.

Continuando con el mismo ejemplo anterior de control de acceso, se debería primero llevar a cabo un análisis de riesgo de los sistemas de información. Luego de este análisis pueden establecerse las políticas a fin de tener una guía para la aplicación de las medidas.

b) Porque guían el proceso de selección e implantación de los productos de seguridad

La mayoría de las organizaciones no tienen los recursos para diseñar e implantar medidas de control desde cero. Por tal razón a menudo escogen soluciones

proporcionadas por los fabricantes de productos de seguridad y luego intentan adaptar esos productos a las políticas, procedimientos, normas y demás esfuerzos de integración dentro de la organización. Como resultado, los productos de seguridad escogidos y su aplicación pueden no resultar adecuados a las verdaderas necesidades de la organización. Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía la gerencia en lo que a seguridad se refiere. De manera que tales políticas pueden ser una manera de garantizar de que se está apropiadamente seleccionando, desarrollando e implantando los sistemas de seguridad.

c) Porque demuestran el apoyo de la Presidencia y de la Junta Directiva (Rectoría y Consejo Universitario)

La mayoría de las personas no está consciente de la gravedad de los riesgos relativos a la seguridad y no se toman el tiempo para analizar estos riesgos a fondo. Las políticas son una manera clara y definitiva para que la alta gerencia pueda mostrar que: “La seguridad de los activos de información es importante” y “El personal debe prestar la atención debida a la seguridad”.

Las políticas pueden entonces propiciar las condiciones para proteger los activos de información. Un ejemplo muy frecuente involucra a los gerentes a nivel medio que se resisten a asignar dinero para la seguridad en sus presupuestos. Pero si las políticas han sido emitidas por la Junta Directiva o la alta gerencia, entonces los gerentes a nivel medio no podrán continuar ignorando las medidas de seguridad.

d) Para evitar responsabilidades legales

La razón puede ser atribuida a: negligencia, violación de confianza, fallas en el uso de medidas de seguridad, mal práctica, etc.

e) Para lograr una mejor seguridad

A menudo un departamento estará a favor de las medidas de seguridad, mientras que otro dentro de la misma organización se opondrá o será indiferente. Si ambos departamentos comparten recursos informáticos (por ejemplo una LAN o un servidor), el departamento que se opone pondrá en riesgo la seguridad del otro departamento y de la organización completa.

Aunque no es ni factible ni deseable que todas las personas en una organización se familiaricen con las complejidades de la seguridad informática, es importante que todas ellas se comprometan con mantener algún nivel mínimo de protección. Las políticas pueden usarse para definir el nivel de esta protección mínima, a veces llamada línea de base.

1.2. Pasos Para el Desarrollo de Políticas y Procedimientos en Seguridad de Información

Antes de embarcarse en un esfuerzo de elaborar las políticas de seguridad, es aconsejable aclarar quién es responsable de promulgarlas y aplicarlas. Otro requisito previo necesario para tener éxito involucra la perspectiva de la alta gerencia. Sólo después de que sus miembros tomen conciencia de que los activos de información son un factor vital para el éxito de la organización, es que la seguridad informática es apreciada como un asunto serio que merece atención.

Idealmente, el desarrollo de políticas de seguridad debe comenzarse después de una evaluación a fondo de las vulnerabilidades, amenazas y riesgos. Esta evaluación debería indicar, quizás sólo a grandes rasgos, el valor de la información en cuestión, los riesgos a los cuales esa información se sujeta, y las vulnerabilidades asociadas a la manera actual de manejar la información. También pueden ser incluidos en la declaración de las políticas, los tipos generales de riesgos enfrentados por la organización, así como cualquier otra información útil obtenida a partir del análisis de riesgos.

Un buen objetivo a tener presente cuando se redactan las políticas, es que ellas deberían durar durante varios años, por ejemplo cinco años. En realidad, se harán modificaciones más a menudo, pero para evitar que se vuelvan obsoletas rápidamente, debe elaborarse para que sean independientes de productos comerciales específicos, estructuras organizativas específicas, así como las leyes específicas y regulaciones.

Las políticas deben revisarse en forma periódica, preferiblemente cada año, para asegurarse de que todavía son pertinentes y efectivas. Es importante eliminar aquellas políticas que ya no son útiles o que ya no son aplicables.

1.3 ¿Cómo deben elaborarse las políticas?

a) Recopilar material de apoyo

Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgo que indique claramente las necesidades de seguridad actuales de la organización. Antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención.
Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de organización (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

b) Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir políticas que se piensa aplicar de inmediato así como aquellas que se piensa aplicar en el futuro.

c) Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se estará ahora listos para redactar las políticas.

Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia. Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la Presidencia y Junta Directiva para su aprobación. Es fundamental de que luego de la entrada en vigor, las políticas se apliquen estrictamente. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto. Las políticas de seguridad deben diseñarse de acuerdo a las necesidades específicas e una organización. Algunas organizaciones tienen muchas políticas, mientras otros tienen sólo unas cuantas.

Elementos que debe contener una política de seguridad:

1. Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
2. Objetivos de la política y descripción clara de los elementos involucrados en su definición.
3. Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la institución.
4. Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
5. Definición de violaciones y de las consecuencias del no cumplimiento de la política.
6. Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

2. Vulnerabilidades y Amenazas

2.1. Tipos de Vulnerabilidades

Vulnerabilidad

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

Realmente la seguridad es la facultad de estar cubierto de algún riesgo o amenaza. Desde este punto de vista la seguridad total es muy difícil de lograr, puesto que implicaría describir todos los riesgos y amenazas a que puede verse sometido el sistema. Lo que se manifiesta en los sistemas no es la seguridad, sino más bien la inseguridad o vulnerabilidad. No se puede hablar de un sistema informático totalmente seguro, sino más bien de uno en el que no se conocen tipos de ataques que puedan vulnerarlo, debido a que se han establecido medidas contra ellos.

Algunos tipos de vulnerabilidad de un sistema son los siguientes:

Vulnerabilidad física.

Se encuentra en el nivel del edificio o entorno físico del sistema. Se relaciona con la posibilidad de entrar o acceder físicamente al sistema para robar, modificar o destruir el mismo.

Vulnerabilidad natural.

Se refiere al grado en que el sistema puede verse afectado por desastres naturales o ambientales que pueden dañar el sistema, tales como el fuego, inundaciones, rayos, terremotos, o quizás más comúnmente, fallos eléctricos o picos de potencia. También el polvo, la humedad o la temperatura excesiva son aspectos a tener en cuenta.

Vulnerabilidad del hardware y del software.

Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, ciertos sistemas requieren la posesión de algún tipo de herramienta o tarjeta para poder acceder a los mismos.

Ciertos fallos o debilidades del software del sistema hacen más fácil acceder al mismo y lo hacen menos fiable.

Vulnerabilidad de los medios o dispositivos.

Se refiere a la posibilidad de robar o dañar los discos, cintas, listados de impresora, etc.

Vulnerabilidad por emanación.

Todos los dispositivos eléctricos y electrónicos emiten radiaciones electromagnéticas. Existen dispositivos y medios de interceptar estas emanaciones y descifrar o reconstruir la información almacenada o transmitida.

Vulnerabilidad de las comunicaciones.

La conexión de los ordenadores a redes supone sin duda un enorme incremento de la vulnerabilidad del sistema. Aumenta enormemente la escala del riesgo a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intentar tenerlo. También se añade el riesgo de intercepción de las comunicaciones:

- Se puede penetrar al sistema a través de la red.
- Interceptar información que es transmitida desde o hacia el sistema.

Vulnerabilidad humana.

La gente que administra y utiliza el sistema representa la mayor vulnerabilidad del sistema. Toda la seguridad del sistema descansa sobre el administrador del mismo que tiene acceso al máximo nivel y sin restricciones al mismo.

Los usuarios del sistema también suponen un gran riesgo al mismo. Ellos son los que pueden acceder al mismo, tanto físicamente como mediante conexión. Existen estudios que demuestran que más del 50% de los problemas de seguridad detectados son debidos a los usuarios de los mismos.

Las 10 vulnerabilidades de los sistemas Windows

1. Servicios de IIS (Internet Information Server)

IIS tiene un gran número de vulnerabilidades que básicamente son de tres tipos: error al tratar peticiones inesperadas, desbordamientos de memoria intermedia y las aplicaciones de ejemplo incluidas en IIS.

2. Microsoft Data Access Components (MDAC) - Remote Data Services (RDS):

Las versiones antiguas de los servicios de datos remotos permiten a un usuario remoto ejecutar órdenes en el sistema infectado con privilegios de administrador.

3. Microsoft SQL Server

SQL Server tiene un buen número de importantes agujeros de seguridad que pueden ser utilizados para revelar información sensible, alterar el contenido de las bases de datos y comprometer los servidores de bases de datos.

4. NetBIOS - Recursos compartidos de redes Windows sin protección

Una configuración errónea de los recursos de la red de Windows puede permitir el acceso a los archivos críticos de un sistema o bien ofrecer un mecanismo para que un atacante pueda controlar el ordenador de la víctima.

5. Conexiones anónimas y nulas

A través de conexiones de usuario anónimo o sin usuario, un atacante puede obtener información sobre la configuración de la máquina, los usuarios definidos y los recursos compartidos. Es el primer paso de un ataque contra una máquina Windows.

6. Autenticación LAN Manager

Debido a la necesidad de ofrecer compatibilidad descendente, Windows continúa utilizando un mecanismo de cifrado de las contraseñas muy ineficiente. Una vez capturada la contraseña, utilizando la fuerza bruta (probar todas las combinaciones posibles) es factible descifrarla en periodos de tiempo muy cortos.

7. Autenticación de Windows: Cuentas sin contraseña o con contraseña débil.

Una de las vulnerabilidades más frecuente es la existencia de cuentas de usuario sin contraseñas (que pueden ser identificadas fácilmente si se permite conexiones nulas al sistema) o con contraseñas débiles.

8. Internet Explorer

Internet Explorer es el navegador por defecto incluido en todas las versiones de Windows. Todas las versiones publicadas hasta la fecha, sin los últimos parches publicados, tienen importantes vulnerabilidades de seguridad.

9. Acceso remoto al registro

Una configuración errónea del sistema puede permitir el acceso remoto al registro del sistema, una base de datos jerárquica donde están definidos todos los parámetros del sistema: configuración de programas, dispositivos y usuarios.

10. Windows Scripting Host

Este es un componente presente en Windows 98, ME, 2000 y XP (así como en 95 y NT si se ha instalado Internet Explorer 5 o posterior) que permite la ejecución de scripts en Visual Basic.

Algunos de los últimos gusanos (como el "I Love You") utilizan este componente para su ejecución.

Las 10 vulnerabilidades de los sistemas Unix

1. Llamadas de procedimiento remoto (RPC)

RPC permite que los programas de un ordenador ejecuten procedimientos en otro ordenador, enviando datos y recibiendo los resultados. No obstante, el servicio fue diseñado hace muchos años y la seguridad no era entonces un factor clave. Así, muchos procedimientos RPC se ejecutan con privilegios de root y no realizan ningún tipo de comprobación.

2. Servidor web Apache

A pesar que Apache no tiene el mismo número de problemas de seguridad que el IIS, no es un producto invulnerable. Por tanto debemos verificar que estamos utilizando la última versión, no únicamente del servidor Web sino también de los diferentes módulos.

3. Secure Shell (SSH)

El protocolo SSH1 se ha demostrado como potencialmente vulnerable a la posibilidad de interceptar y descifrar una comunicación, por lo que se desaconseja su utilización.

Si se utiliza OpenSSH, debemos considerar que algunas bibliotecas de funciones utilizadas (como OpenSSL) tienen sus propias vulnerabilidades que pueden afectar a la seguridad de las comunicaciones.

4. Protocolo SNMP

Según la versión del protocolo SNMP utilizada, los mecanismos de autenticación son extraordinariamente simples. Esto, unido a la posibilidad de modificar la configuración de los dispositivos de la red, lo convierte en un importante agujero en la seguridad corporativa.

5. Protocolo FTP

El protocolo FTP transmite las contraseñas de los usuarios por la red sin ningún tipo de protección. Por otra parte, algunos de los programas servidores de FTP más utilizados en los sistemas Unix tienen un buen número de importantes vulnerabilidades.

6. Servicios R (relaciones de confianza)

Se trata de una serie de servicios que permiten el acceso a sistemas remotos, sin necesidad de volver a autenticarse en los mismos. No obstante, cuando se diseñaron estos mecanismos, la seguridad no era un factor clave por lo que el sistema de autenticación es muy débil y fácilmente suplantable. Se desaconseja su utilización en cualquier entorno.

7. Servicio LPD

Muchas implementaciones del servicio LPD tienen serios problemas de seguridad que permiten a un atacante remoto ejecutar código con privilegio de root.

8. Sendmail

Sendmail ha sido, históricamente, uno de los servicios más atacados. No obstante, en los últimos dos años no se ha descubierto ningún problema especialmente grave. Por tanto, es importante verificar que se está utilizando una versión moderna.

9. BIND / DNS

Se han descubierto recientemente diversas vulnerabilidades en el servicio de resolución de nombres de dominio que pueden ser utilizadas para ejecutar código en las máquinas vulnerables o bien utilizarlas como plataformas para atacar a otros sistemas. Por tanto, también es importante verificar que se está utilizando una versión moderna.

10. Autenticación de Unix: cuentas sin contraseña o con contraseña débil

Al igual que sucede en los sistemas Windows, muchos sistemas Unix tienen cuentas de usuario sin contraseñas o con contraseñas débiles. También la instalación por defecto de algunos programas crea cuentas de usuarios con contraseñas conocidas.

2.2. Tipos de Amenazas

Amenaza.

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc), o un suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema.

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). **Un ataque no es más que la realización de una amenaza.**

Intercepción

Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

Modificación

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

Interrupción

Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Generación

Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

Ataques a nuestra información, ¿cuales son las amenazas ?

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

1. **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

2. **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
3. **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de córdobas en la cuenta A" podría ser modificado para decir "Ingresa un millón de córdobas en la cuenta B".

4. **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de *denegación de servicio*, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Éstos son algunas de las amenazas que usted enfrenta:

- El virus
- Los gusanos
- Los Caballos troyanos
- La ingeniería social
- Los olfateadores de contraseña
- Mail, Web, IRC
- Ataques de tipo hombre en medio
- El secuestro de sesión
- Engaño y envenenamiento del DNS
- Mal configuración de los archivos compartidos
- Portscans y networkscan
- Ataque DOS (Denial Of Service)
- La intrusión:
    - Automática (Nimda, Código rojo)
    - Manual
        - Aprovechamiento de los agujeros de seguridad
        - Por contraseñas débiles u olfateó de estas
- Engaño de la tabla ARP
- Wardialing
- La invasión desde fuera a través de la red
- El ilegal uso del sistema por personas internas sin el permiso para usarlo
- Acceso a los datos protegidos por una persona que tiene permiso para usar el sistema
- El robo de datos que se transmiten o alteración de los datos

Virus

Son programas hechos por alguien y su función es muy diversa, pero básicamente todos tienen la capacidad de reproducirse y una estrategia de propagación. Lo más peligroso del virus es su "payload" que puede ser desde una pelotita rebotando en la pantalla hasta el formateo del disco.

Puede ser ingresado al sistema por un dispositivo externo (diskettes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc) y los sectores de boot-partición de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y a demás son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras.
Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

Troyanos

Son programas que tras una aparente función encierran en su interior otra función. Por ejemplo, un troyano típico, puede presentarnos una pantalla igual a aquella en la que tenemos que escribir nuestro login y nuestro password, cuando los introduzcamos, los almacenara. Lamentablemente los troyanos en Windows están muy de moda desde que aparecieron troyanos como Backoriffice o Netbus, que tras instalarse en el equipo, permiten el acceso remoto a tu ordenador desde Internet y su control remoto. Diariamente aparecen más troyanos de este tipo.

Ingeniería Social

Uno de los sistemas mas usado es el llamado por los atacantes ingeniería social, *no es técnico* sino que se basa en descubrir la contraseña *directamente de los usuarios.* Los métodos pueden ser: observar el teclado cuando se introduce la contraseña, descubrirlo escrito en un papel, pedirlo por correo electrónico o teléfono haciéndose pasar por el administrador, etc… Aunque parezca imposible, las estadísticas dicen que es unos de los sistemas mas utilizados.

Eavesdropping y Packet Sniffing

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras maneras.
Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes.

Snooping y Downloading

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.
El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.
La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.
El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.
Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.
El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos.

Jamming o Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla. Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra tambien spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos host de Internet han sido dados de baja por el “ping de la muerte”, una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.
Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

Bombas Lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

Explotación de Errores de Diseño, Implementación u Operación

Muchos sistemas están expuestos a “agujeros” de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de “puertas invisibles” han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y toda clase de servicios en LAN o WANs.
Sistemas operativos abiertos como Unix tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows NT. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de datos de tests periódicamente.

Además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática.

Obtención de Passwords, Códigos y Claves

Este método (usualmente denominado cracking), comprende la obtención “por fuerza bruta” de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y “diccionarios” que prueban millones de posibles claves hasta encontrar la password correcta.
Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.
Por ser el uso de passwords la herramienta de seguridad mas cercana a los usuarios, es aquí donde hay que poner énfasis en la parte “humana” con políticas claras (como se define una password?, a quien se esta autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?)
No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

Eliminar el Blanco

Ping mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo el Windows 95).
TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como Ethernet o token ring, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un buffer en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el buffer del equipo de destino se desborda y el sistema se puede colgar.

Hackers, Crackers y Piratas

El término *hacker*, por ejemplo, se utiliza normalmente para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños.

Los *crackers*, en cambio, tienen como principal objetivo producir daños que en muchos casos suponen un problema de extrema gravedad para el administrador del sistema. En cuanto a los piratas, su actividad se centra en la obtención de información confidencial y *software* de manera ilícita.

Su principal motivación es la de acceder a sistemas protegidos de forma fraudulenta, en una escala que va desde la mera constancia de su éxito, hasta la destrucción de datos, obtención de información confidencial, colapso del sistema, etc. Normalmente los objetivos más apetecibles son los sistemas relacionados con la seguridad nacional, defensa e instituciones financieras, pero ante las posibles consecuencias legales de estos actos optan por otros organismos públicos, las universidades y las empresas.

Pasos para Hachear comúnmente utilizados

1. Introducirse en el sistema que se tiene como objetivo.
2. Una vez conseguido el acceso, obtener privilegios de root (superusuario).
3. Borrar las huellas.
4. Poner un sniffer para conseguir logins de otras personas.

3. Contramedidas ante las Vulnerabilidades y Amenazas

3.1. Tipos de Medidas de Seguridad o Contramedidas

Contramedida.

Técnicas de protección del sistema contra las amenazas.

La seguridad informática se encarga de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades. Una máxima de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. En relación a esto, también se hace obvio que a mayores y más Restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el uso de una política adecuada de passwords, con cambios de las mismas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales. Vamos a verlas con más detalle.

Medidas físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de seguridad en nuestro sistema.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas
- Los daños físicos por parte de agentes nocivos o contingencias
- Las medidas de recuperación en caso de fallo

Concretando algo más los tipos de controles que se pueden establecer, estos incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc.)
- Prevención de catástrofes

- Vigilancia
- Sistemas de Contingencia (extintores, fuente de alimentación ininterrumpida, estabilizadores de corriente, etc.)
- Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)
- Control de la entrada y salida de material (elementos desechables, consumibles, etc.)

Medidas lógicas

Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

- Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
- Definición de una política de instalación y copia de software.
- Uso de la Criptografía para proteger los datos y las comunicaciones.
- Uso de Cortafuegos para proteger una red local de Internet.
- Definición de una política de copias de seguridad.
- Definición de una política de monitorización y auditoria del sistema.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

- ¿A quién se le permite el acceso y uso de los recursos?
- ¿Qué recursos puede acceder cada usuario y qué uso puede hacer de ellos?
- ¿Cuáles son las funciones del administrador del sistema y del administrador de la seguridad?
- ¿Cuáles son los derechos y responsabilidades de cada usuario?

A la hora de responder a las preguntas anteriores hemos de diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema:

- El administrador del sistema y en su caso el administrador de la seguridad.
- Los usuarios del sistema.
- Las personas relacionadas con el sistema pero sin necesidad de usarlo
- Las personas ajenas al sistema

Medidas administrativas

Las medidas administrativas son aquellas que deben ser tomada por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

- Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
- Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.
- Establecimiento de un plan de formación del personal.
- Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento son fundamentales para evitar toda una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.
- Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.
- Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.
- Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

Medidas legales

Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori.

Este tipo medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales. Un ejemplo de este tipo de medidas es la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal).

Esta ley vincula a todas las entidades que trabajen con datos de carácter personal, define las medias de seguridad para su protección y las penas a imponer en caso de su incumplimiento.

¿Qué medidas de seguridad generales se pueden tomar localmente?

- Clarifique quién es responsable para que
- Asegúrese todos están claros de esto
- Capacite a los usuarios finales
- Capacite a los administradores de sistema
- Desarrolle una "Mejor práctica"

- Genere un formulario estándar para instalar las computadoras.
- Se asegura que las computadoras son parchadas regularmente y directamente cuando se encuentran nuevos agujeros de seguridad.

¿Qué medidas de seguridad técnicas usted puede tomar localmente?

- Nunca inicie servicios que usted no necesita en cualquier computadora
- Proteja los servicios que usted usa
  - Las envolturas de TCP
  - Los archivos de Deny/allow
  - El filtro del IP, el Filtro del Paquete, las tablas IP,
- Instale un cortafuego central o filtros en los routers.
- Instale los cortafuegos localmente en los servidores
- Instale los cortafuegos personales en las computadoras personales
- Inicie Logging apropiado
- Envíe los Logs a un Logserver.
- Haga comprobación automática de Log (Logchecking) usando Logparser.
- Instale hosts Sistemas de Descubrimiento de Intrusión (IDS)
  - Tripwire
  - Portsentry
  - Hostsentry
- Corrija sus backups

¿Qué medidas de seguridad generales usted puede llevar a cabo centralmente?

- Clarifique quién es responsable para que
- Asegúrese que todos están conscientes de esto
- Escriba reglas y políticas
- Escriba documentos guías, FAQs y "Mejor práctica"
- Entrene y eduque a administradores de sistemas
- Se asegura que las personas en la cima saben sobre los riesgos
- Intenta asegurarse que el presupuesto no se filtra a través de demasiadas manos. El dinero para la seguridad de computación es con suerte presupuestado centralmente como por otra parte más probablemente es que el dinero se pesa contra otras necesidades.
- Escriba reportes regulares y publique las estadísticas.

¿Qué medidas de seguridad técnicas usted puede tomar centralmente?

- Instale un ethernet-tap sobre la conexión de Internet
  - El equipo especializado
  - Hub
  - Spanport in the switch
- Instale una computadora para la vigilancia de la red
- Instale un cortafuego
  - Linux IPtables
  - Solaris/BSD IPfilter
  - OpenBSD PF
- Instale un Logservidor.
- Instale un Logparser.
  - Logchecker
  - Swatch
- Instale un IDS
  - Snort
- Instale un sistema del backend y herramientas estadísticas para los IDS
  - ACID
  - Demarc
- Instale un programa tráfico logging.
  - IPaudit
  - Argus
  - Netflow
- Instale un sistema de manejo de incidentes
  - Request Tracker (RT)
- Obtener las herramientas para analizar el tráfico
  - Ethereal
  - Snort
  - ngrep
  - Dsniff
- Obtener las herramientas para examinar su red para los servicios y agujeros de seguridad
  - nmap
  - Netcat (nc)
  - Nessus
- Obtener las herramientas para investigar las intrusiones
  - LSOF
  - The Coroners Toolkint
- Entrenar para usar las herramientas.

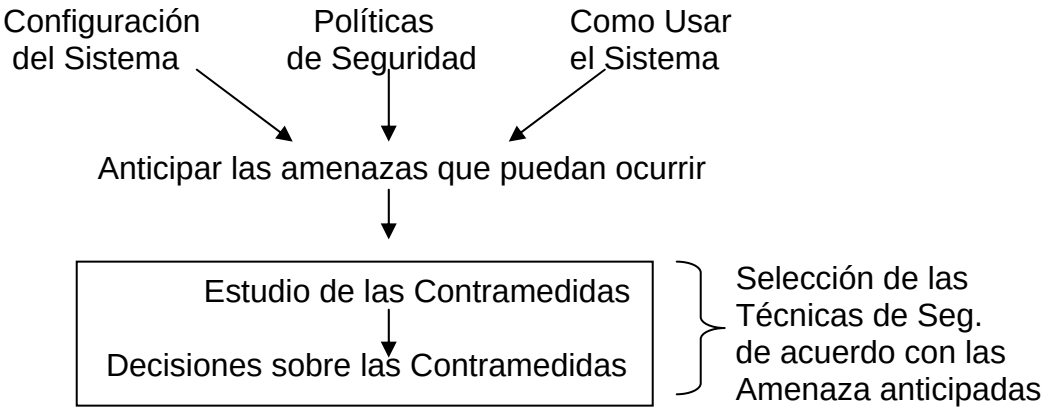
Medidas de Seguridad que debe seguir para asegurar que los datos no sean perdidos o alterados:

- Encripte todos los datos sensibles
- Borre los datos sensibles de la manera correcta
  - La Desfibradora del archivo
  - Sobrescriba
- Encripte el correo electrónico sensible
  - PGP
- Backup, Backup y Backup
  - El formulario una estrategia auxiliar
  - Se asegura que se crea correctamente
  - Corrija, incluso el último archivo
  - Intercambie sus cintas auxiliares regularmente
  - Haga que las bases de datos sean correctamente respaldadas
  - Mantenga el backup en un lugar seguro y no cerca de las computadoras.

4. Técnicas de Seguridad

Clasificación de las técnicas

Como ya hemos mencionado el propósito del diseño de seguridad es prevenir las amenazas y para minimizar el daño causado por una amenaza se están proporcionado las contramedidas las cuales deben ser consistentes con las características de cada sistemas de computadora. Después de estudiar y decidir sobre las contramedidas para el sistema, es necesario entender las técnicas de seguridad disponibles y que técnica es mas eficaz para las amenazas anticipadas.



Tipos de Técnicas de Seguridad

Técnicas para medidas de seguridad:

- Técnicas de **Prevención**: Técnicas para prevenir ocurrencia de amenazas o daño. Las medidas preventivas contra las amenazas deben ser consideradas primero como una medida de seguridad. Por ejemplo la técnica de autenticación por contraseñas para prevenir a una persona desautorizada de acceder el sistema corresponde a esta categoría.

- Técnicas de **Detección**: Las Técnicas de detección son para encontrar que un acceso ilegal ha sido hecho o probablemente será hecho. Esta información provee la base para tomar acciones que minimicen el daño resultante o prevenir que la amenaza ocurra. La adquisición de Logs de accesos y alarmas emitidas por herramientas de monitoreo entran en esta categoría.

- Técnicas de **Acción Subsecuente**: La técnicas de esta categoría se emplean para minimizar el daño. Los backup de sistemas y de bases de datos en caso de que ellos se estropean corresponden a esta categoría.

También dentro de esta clasificación tenemos las técnicas para analizar logs en orden para localizar la causa de recibir una amenaza y para prevenir que se repitan.

	Prevención	**Detección**	**Acción Subsecuente**
4.1 Red	4.1.1 Línea Dedicada 4.1.2 Call Back 4.1.3 Switching hub 4.1.4 Router 4.1.5 Firewall	▪ Firewall, router (log)	
4.2 BD	4.2.1 Control de acceso 4.2.2 Replica	▪ Logs de acceso	▪ Backup (Replica)
4.3 SO	4.3.1 Autenticación 4.3.2 Permisos	▪ Log	▪ Backup
4.4 Otros	4.4.1 Una contraseña de tiempo 4.4.2 Software Vacuna 4.4.3 Cifrado 4.4.4 SSL 4.4.5 VPN	▪ Vacuna (pattern match) ▪ Cifrado (Firma digital)	
4.5 Herramientas	▪ Herramienta de prueba	▪ Herramienta de supervisión	Herramientas de análisis

Tabla 2.1. Propósito de Diferentes Técnicas de Seguridad

Las técnicas concretas aplicables para diferentes propósitos están listada en la tabla anterior.
Construyendo un sistema en la práctica, las medidas de seguridad son implementadas a través de la combinación de esas técnicas en línea con las políticas de seguridad establecidas.

4.1. Técnicas Relacionadas a Redes

Una gran mayoría de los sistemas de computadoras de hoy están conectado una red de computadoras. Esto a incrementado el numero de accesos ilegales que son hechos en la red a través de sistemas remotos, o incluso desde dentro, mas que los accesos ilegales hecho directamente a la computadora.

Las técnicas de seguridad relacionadas a Redes están clasificadas en los siguientes dos tipos:

a) Control de Acceso Físico (Control de Seguridad en la capa física de OSI)

El control de acceso esta relacionado principalmente a una WAN. Esta técnica de prevención establece un circuito físico entre un sistema de computadora y una tercera parte no teniendo permiso para usarlo.
Es el control y monitoreo de la entrada (punto de acceso) de la red, apuntado a bloquear a los usuario sin permiso de acceso de acceder al sistema. La función de autentificación para permisos de conexión por medio de IDs y passwords corresponden a este tipo.
Los dispositivos de esta categoría son:

4.1.1 Línea Dedicada (para WAN)
4.1.2 Call back (para WAN)
4.1.3 Switching hub (para LAN)

b) Control de Acceso Lógico (Control de Seguridad en las capas sobre la capa del datalink o enlace de OSI)

El Control de acceso principalmente ejercido dentro de una LAN o el punto de interconexión una WAN y una LAN. Esta técnica chequea el contenido de la cabecera de cada paquete de dato para controlar el acceso a los recursos del sistema y la información.
El control de acceso lógico decide como los datos son recibidos por el equipo en la red, tal como un router, basado en la información de cabecera de los datos recibidos. Este tipo de control es designado para bloquear todos los accesos al sistema hecho a través de cualquier otro punto que no sea un punto de acceso autorizado. Uso de línea dedicada corresponde a este tipo.
Los dispositivos de esta categoría son:

4.1.4 Router (Filtrando paquetes)
4.1.5 Firewall

Para implementar medidas de seguridad, en la practica general se utilizan ambos tipos de control, en lugar de aplicar uno de ellos, aunque todo depende de la manera que es sistema va a ser operado.

4.1.1. Uso de Línea Dedicada:

Una línea dedicada es un servicio de red que proporciona un circuito físico fijo puesto entre dos puntos. Ningún acceso ilegal desde fuera puede tener lugar dentro de la red usando una línea dedicada.

4.1.2. Call Back

Solo los usuarios permitidos para acceder por IDs, etc., son autorizados para establecer un circuito.
Call back es una técnica de autenticación que es empleada en una red cuando las conexiones son preparadas por dialing a través de una red telefónica, etc.

Conforme este método, el servidor almacena los números de teléfonos de usuarios correspondientes a sus IDs, además de estos registra IDs y passwords. El cliente primero accede a el RAS (Sistema de Acceso Remoto) de la misma manera como a una conexión ordinaria, y busca una autenticación de el RAS usando un ID o password. Después de finalizada la autenticación, el RAS entonces hace búsquedas para el numero de teléfono de el usuario según la ID, y establece la conexión a ese cliente con ese numero de teléfono.

Cuando este método Call back es seguido, el cliente (numero telefónico) a quien el RAS hace callback a la conexión basada en el ID es el usuario propio de la ID. Una tercera parte puede prevenir que se hagan acceso ilegal al sistema a través de circuito telefónico, incluso si se roba la ID o password de el usuario apropiado.

4.1.3. Uso de Switching Hub

En un tipo de bus ordinario LAN, como Ethernet, los datos son transmitidos sobre la LAN por una computadora y es recibida por todas las computadoras que están conectadas al mismo segmento.

Si, en tal caso, un switching hub es introducido, una computadora directamente acoplada al switching hub puede transmitir datos solo a la computadora pensada, y los datos transmitidos no puede ser interceptados con un tapping dispositivo conectado a otro puerto de el switching hub.

4.1.4. Router (Filtrando paquetes)

Filtrando a través de router se llama filtración de paquetes y es implementada principalmente por el chequeo de las direcciones de la capa de red, la dirección IP de TCP/IP.

Mientras la técnica de filtrado de paquete chequea principalmente la fuente de la direcciones, algunos routers ofertan una función para determinar cuando los datos deben ser pasados, conforme a la dirección de destino.

Uso de router proporciona control de acceso entre una LAN y una WAN. No solo eso, cuando un router es instalado entre el cliente y el servidor dentro de una LAN, el puede también permitir el control de servicios que puede ser usado por

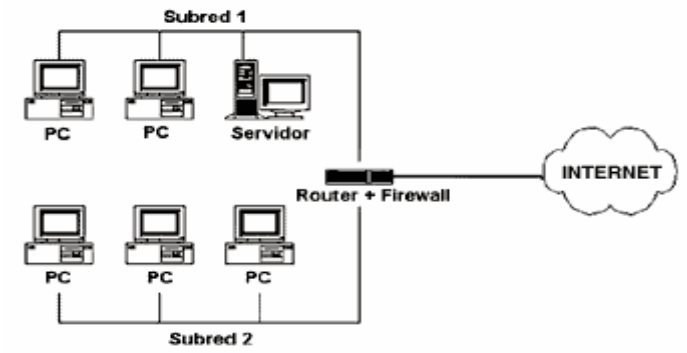
diferentes clientes a través de la combinación de la dirección IP origen y el numero de puerto de destino.

4.1.5. Firewall

¿Que es un Firewall y Como Trabaja?

Un Firewall (Cortafuego) es una entidad software o hardware que protege a una red de los intrusos exteriores regulando el tráfico que pasa por un router (enrutador) que la conecta con otra red. Un Firewall protege a los usuarios de una LAN contra los usuarios de otras LAN, conectados localmente o a través de una WAN. Si no existe el Firewall, los usuarios del exterior pueden acceder a los archivos de una red, introducir virus, usar los servidores para fines particulares e incluso borrar por completo las unidades de disco.

Un Firewall Constituye una especie de “barrera lógica” delante de nuestros sistemas que examina todos y cada uno de los paquetes de información que tratan de atravesarla. Un Firewall es solo un paso mas para crear un sistema seguro. También son necesarias las medidas de seguridad de alto nivel.



El Firewall se coloca "en medio" de las comunicaciones entre nuestro ordenador (o red local) e Internet, filtrando todo el tráfico que lo atraviesa y tomando decisiones de qué hacer con él en función de reglas establecidas.

Los servicios que se habilitan, además del Firewall, forman la base para la seguridad del sistema. Por ello debemos preocuparnos por deshabilitar servicio innecesarios, seleccionar servicios que se harán públicos e identificar los servicios locales peligrosos que debe proteger el Firewall.

Todas las comunicaciones de Internet se realizan mediante el intercambio de paquetes de información, que son la unidad mínima de datos transmitida por la red. Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se comunican, debe llevar aneja la información referente a la dirección IP de cada máquina en comunicación, así como el puerto a través del que se comunican.

Un Firewall intercepta todos y cada uno de los paquetes destinados a o procedentes de nuestro ordenador, y lo hace antes de que ningún otro servicio los pueda recibir. De esto extraemos la conclusión de que el Firewall puede controlar de manera exhaustiva todas las comunicaciones de un sistema a través de Internet.

La verdadera potencia de un Firewall reside en que al analizar cada paquete que fluye a través de el, puede decidir si lo deja pasar en uno u otro sentido, y puede decidir si las peticiones de conexión a determinados puertos deben responderse o no. Por ejemplo, de este modo podemos configurar un Firewall para que sólo permita las comunicaciones a través de los puertos de correo electrónico, FTP y HTTP, si esos son los únicos servicios que necesitamos.

Un Firewall puede tomar muchas formas en función del tamaño de nuestra red, de las funciones de nuestros equipos y del grado de riesgo. Un verdadero Firewall es un conjunto de directivas de seguridad que se puede implementar por medio de varios componentes diferentes de red que trabajan juntos no sólo para regular el tráfico de la entrada de red, sino también el tráfico de salida. Además de evitar que los usuarios de Internet accedan a los sistemas de nuestra red, se puede evitar que ciertos usuarios internos exploren la Web, aunque se le permite que usen correo electrónico de Internet.

Otra característica interesante que se refiere a la manera de intercambiar datos a través de TCP/IP es que, gracias al bit ACK de los paquetes, es fácil determinar si un paquete procede de una conexión ya establecida o es un intento de penetración externa. Así es relativamente sencillo que un Firewall pueda dejar pasar aquellas comunicaciones que el sistema interno haya establecido, impidiendo todas aquellas cuyo origen sea el exterior. Otra función útil de la mayoría de los Firewall es su capacidad para mantener un registro detallado de todo el tráfico e intentos de conexión que se han producido (lo que se conoce como un Log). Estudiando los Log es posible determinar los orígenes de posibles ataques, descubrir patrones de comunicación que identifican ciertos programas malignos (lo que se conoce como Malware), etc. Sólo los usuarios avanzados podrán sacar partido a estos registros, pero es una característica que se le puede exigir perfectamente a estas aplicaciones.

Algunos Aspectos (Características):

- Para que el *Firewall* sea efectivo, todo el tráfico hacia y desde Internet debe pasar a través de el, donde puede ser inspeccionado. El *Firewall* debe permitir únicamente el paso del tráfico autorizado, además de que debe ser por sí mismo inmune a la penetración.
- El *Firewall* es una parte de la política de seguridad que crea un perímetro de defensa diseñado para proteger los recursos de información de la organización.

- Los *Firewalls* de Internet administran el acceso entre Internet y una red privada organizacional. Sin un *Firewall* cada servidor de la red estará expuesto a los ataques de otros servidores dentro de Internet. Esto significa que la seguridad de la red privada dependería de las características de seguridad de cada servidor y sería tan insegura como el sistema más débil.
- Los *Firewalls* ofrecen un punto conveniente donde la seguridad de Internet puede ser monitoreada y pueden generarse alarmas.
- Finalmente, algunos pueden argumentar que el uso de *Firewalls* crea un sólo punto de falla. Debe enfatizarse que si la conexión a Internet falla, la red privada de la organización continúa operando y únicamente el acceso a Internet se pierde. Si existen múltiples puntos de acceso, cada uno se convierte en un punto potencial de ataque.

El propósito del Firewall es hacer cumplir unas determinadas directivas de seguridad. Estas directivas reflejan las decisiones que se han tomado sobre que servicios de Internet deben ser accesibles a los equipos, que servicios se quieren ofrecer al exterior desde los equipos, que servicios se quieren ofrecer a usuarios remotos o sitios específicos y que servicios y programas se quieren ejecutar localmente para uso privado.

Un Firewall de filtrado de paquetes IPFW consta de una lista de reglas de aceptación y denegación. Estas reglas definen explícitamente los paquetes que se permiten pasar y los que no a través de la interfaz de red. Las reglas del Firewall usan los campos del encabezado del paquete, para decidir si enlutar un paquete hacia su destino, eliminar el paquete o bloquear un paquete y devolver una condición de error a la maquina emisora. Las reglas se basadas en las cabeceras del protocolo de cada paquete, incluye los siguiente:

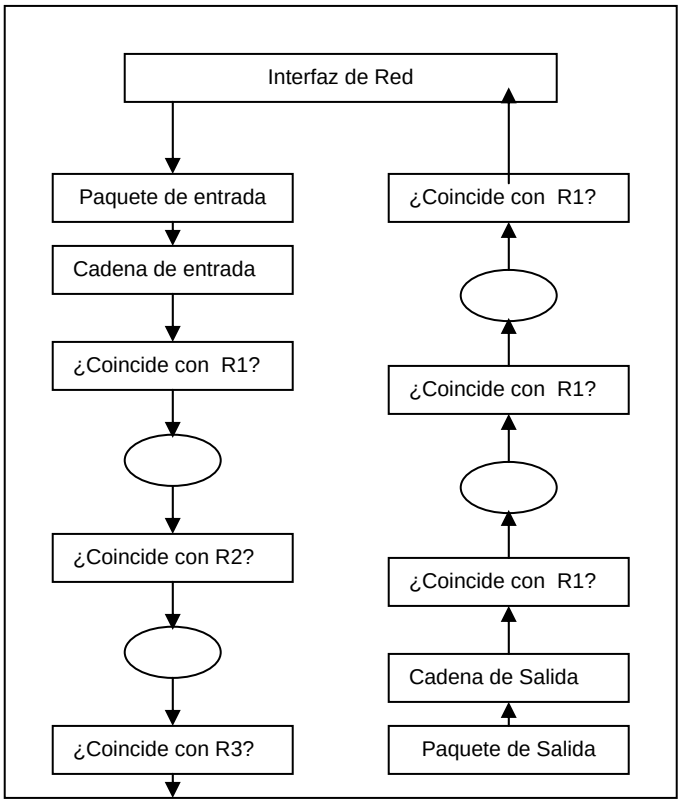
- Direcciones del origen y del destino
- Protocolo encapsulado
- Puerto de origen y de destino
- Tipo de mensaje ICMP
- Interfaz de llegada y de salida

Por medio de combinaciones de valores asignados a estos criterios, se pueden especificar condiciones precisas en las que los paquetes deben ser admitidos a través del Firewall.

Los filtros no dependientes del servicio se usan para evitar tipos específicos de intrusión que no se basan en un servicio particular.

El filtro de paquetes es una característica integrada en muchos router, de modo que la implementación de este tipo de protección no supone un coste monetario adicional, y no se requiere ninguna modificación del software.

La lista de reglas que definen lo que puede entrar y lo que puede salir se llaman cadenas. Las listas se llaman cadenas porque se compara un paquete con cada regla de la lista, una a una, hasta que se encuentra una coincidencia o la lista se termina, como se muestra en la figura a continuación:



Un IPFW funciona en las capas de red y de transporte. Se puede filtrar basándose en la dirección origen, dirección destino, el puerto origen, el puerto destino y el indicador de estado TCP.
La idea general es que el usuario debe controlar con mucho cuidado lo que sucede entre Internet y la maquina que se ha conectado directamente a Internet.

Sobre la interfaz externa a Internet, el usuario filtrará individualmente lo que proviene del exterior y lo que sale de la maquina de forma tan precisa y explicita como sea posible. El Firewall filtra independientemente lo que sale y lo que entra a través de la interfaz. El filtrado de entrada y el filtrado de salida pueden tener reglas completamente diferentes. La lista de reglas que definen lo que puede entrar y lo que puede salir se llaman cadenas. Las listas se llaman cadenas porque se compara un paquete con cada regla de la lista, una a una, hasta que se encuentra una coincidencia o la lista se termina.

Elección de la Directiva

Cada cadena del Firewall tiene una directiva predeterminada y una colección de acciones a realizar en repuesta a tipos de mensajes específicos. Cada paquete se compara, uno a uno, con cada regla de la lista hasta que se encuentra una coincidencia. Si el paquete no coincide con ninguna regla, fracasa y se aplica la directiva predeterminada del paquete.

Hay dos perspectivas básicas para un Firewall:

1. Denegar todo de forma predeterminada y permitir que pasen paquetes seleccionados de forma explicita.
2. Aceptar todo de forma predeterminada y denegar que pasen paquetes seleccionados de forma explicita.

La directiva denegar todo es la propuesta que se recomienda. Esta aproximación facilita la configuración de un Firewall seguro, pero es necesario habilitar específicamente cada servicio y la transacción de protocolo relacionada que quiera el usuario. Esto significa que debe comprender cada protocolo de comunicación para cada servicio que habilite. La propuesta denegar todo requiere preparar el terreno para habilitar el acceso a Internet. Algunos productos Firewall comerciales solo son compatibles con la directiva denegar todo.

La directiva aceptar todo facilita mucho la configuración y la puesta en funcionamiento de un Firewall, pero obliga a prever todo tipo de acceso imaginable que quiera deshabilitar. El peligro es que no preverá un tipo de acceso peligroso hasta que sea demasiado tarde, posteriormente habilitara un servicio no seguro sin bloquear primero el acceso externo al mismo. En definitiva programar un Firewall seguro para aceptar todo, implica mas trabajo, mayor dificultad y, por tanto es mas propenso a errores.

Rechazar Frente a Denegar un Paquete

El mecanismo de Firewall ofrece la opción de rechazar o denegar los paquetes. ¿Cuál es la diferencia?, cuando se rechaza un paquete, el paquete se descarta y se devuelve un mensaje de error al remitente. Cuando se deniega un paquete, simplemente se descarta sin ningún tipo de notificación al remitente.

La denegación es casi siempre la mejor elección. Hay tres razones para esto. Primero, enviar una respuesta de error duplica el trafico en la red. La mayoría de los paquetes se descartan porque son malévolos, no porque representen un intento inocente de acceder a un servicio que no se le ha ocurrido ofrecer. Segundo, cualquier paquete al que responda se puede usar en un ataque por denegación de servicio. Tercero, cualquier respuesta, incluso un mensaje de error, ofrece información potencialmente útil a quien podría ser un hacker.

El filtrado de puerto origen local: restringir los clientes a los puertos no privilegiados en las reglas del Firewall ayuda a proteger a otras personas de posibles errores en su extremo, asegurando que los programas cliente se comportan como se espera.. Si se restringen los servidores a los puertos asignados en el nivel del Firewall, se asegura que los programas de servidor funcionan correctamente.

Una forma de mantener seguro el equipo (local) es no albergar servicios de red en la maquina Firewall que no quiere que use el publico. Si el servicio no esta disponible, no existe forma posible de que un cliente remoto se conecte.

Un paquete puede que sea verificado contra muchas reglas dentro de la lista de reglas antes de llegar al final de una cadena. La estructura y propósito de estas reglas puede variar, pero normalmente buscan identificar un paquete que viene de o se dirige a una dirección IP en particular o un conjunto de direcciones al usar un determinado protocolo y servicio de red.

Existen 2 tipos de Firewall:

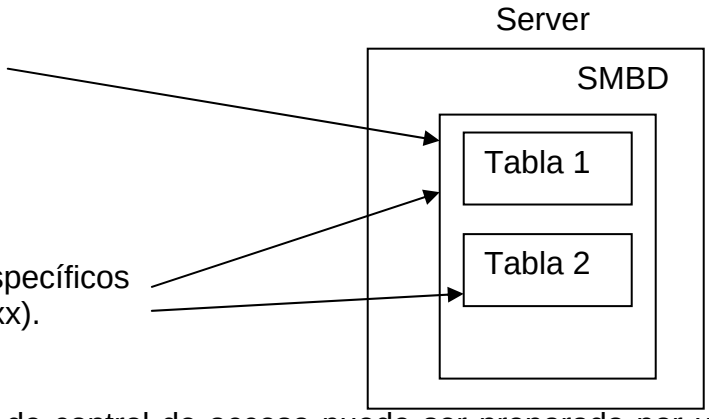
- Firewall Hardware: estos tipos de Firewall son rápidos, pero menos seguros que los Firewall Software.
- Firewall Software: estos Firewall son mas lentos que los Firewall Hardware, pero son mas seguros porque permiten mayor versatilidad.

4.2. Técnicas Relacionadas a Bases de datos

Las técnicas de seguridad relacionadas al equipo y redes son principalmente diseñadas para bloquear terceras partes de acceso al sistema. Pero, no todas las personas teniendo permiso para usar el sistema están permitidas para acceder a todos los datos. Todo depende de las políticas del sistema.

El formulario de control no puede ser logrado solamente por medio de control de flujo sobre la red, pero necesitan ser ejercido desde dentro del servidor. Hay dos caminos para este propósito, uno es para manejar cada transacción individual y el acceso de dato basado sobre una aplicación de programa, y la otra es para ejercer el control usando las funciones reciente de DBMS (Sistema de Manejo de Base de Datos).

4.2.1. Control de Acceso



- **Sistema de Seguridad**

Permisos para usar SMBD
(crea usuarios xxxx)

- **Seguridad de BD**

Permisos para usar recursos específicos
(concesión crear tabla para xxxx).

Generalmente, estos dos tipos de control de acceso puede ser preparado por un SMBD: uno es el sistema de seguridad relacionado a los permisos para usar el SMBD, y el otro, la seguridad de la BD.

El sistema de seguridad corresponde al registro de usuario que proveen permisos para usar el SMBD, y la seguridad de BD denota los permisos para acceder a las bases de datos y tablas de concesión para registrar usuario y grupos.
Prepare un servicio de acceso para cada base de datos o tabla para cada usuario individual o grupos de usuarios.

4.2.2. Replicas

La técnica de replicas de BD es utilizada para mejorar la actuación del sistema y costo, para hacer backups, y para una variedad de otros propósitos.
Crear copias (replicas) de bases de datos y tablas especificas, y coloque las copias sobre los sitios que están susceptibles para accesos ilegales y destrucción, o para el uso como un Backup.

4.3. Funciones de Seguridad de los SO

La mayoría de los SO que soportan multi-usuario, como UNIX, Windows NT, etc, proporcionan una variedad de funciones para la seguridad y, por consiguiente, permite la implementación de medidas de seguridad, sin necesidad de prepara un software especifico para este propósito.

Un tipo genérico de SO proporciona las siguientes funciones, entre otras:

4.3.1. Registración y Autentificación de usuario

Registra usuarios y las concesiones apropiadas para permisos, controlando los permisos para usar el sistema o las aplicaciones.
En caso de Windows NT, los usuarios son registrado con “Propiedades de usuario”, que es una de las herramientas administrativas.

4.3.2 Adquisición de Logs

Son archivos en los que se recogen las estadísticas de las visitas que tienen las páginas de un sitio Web. Es un registro donde quedan memorizadas todas y cada una de las visitas. El servidor Web, anota en un fichero log cada petición de archivo que se le formula, así como los posibles errores (URL incorrecta, error en CGI, etc.).

Los archivos Logs, además de emplearse para la detección y depuración de errores, son empleados por los programas de estadísticas. Si dispone de programas como Analog o Webalizer, obtendrá informes de uso del servidor, realmente útiles, pero que se verán limitados al período cubierto por el log disponible.

Registro LOG

CopiaSEC deja constancia de todas las operaciones y eventos que tienen lugar en referencia a las copias de seguridad, permitiendo al usuario consultar la historia del sistema. Concretamente existen dos registros (LOG): el **registro general** y el **registro de archivos copiados y restaurados**.

El registro general contiene anotaciones para arranque y cierre de **CopiaSEC**, creación, modificación y eliminación de cualquier proyecto, inicio y finalización de realización de copia de seguridad, inicio y finalización de restauración de copia de seguridad y errores por corte de suministro eléctrico, apagado del sistema inapropiado, etc. El registro de archivos copiados y restaurados contiene la lista detallada de archivos copiados y restaurados en cada ocasión para cada proyecto existente.

4.3.3. Setup de Permisos de Acceso

Asigna un permiso de acceso para cada usuario o cada grupo de usuario para archivos y carpetas.

Los accesos de permisos básicos son un juego de tres tipos, “Lectura”, “Escritura” y “Ejecución”. Sin embargo, el juego de acceso de permiso en el SO es hecho independientemente de la aplicación y el DBMS. Esto significa que, aun cuando un usuario es registrado en el DBMS, el usuario puede no ser capaz de usar el DBMS, a menos que al usuario se asigne permiso para la ejecución de un archivo (programa).

4.3.4. Backup

EL backup de dato y sistema es una técnica que sirve como remedio para la destrucción de archivos. Los archivos pueden ser respaldados usando el comando copy del SO. En este caso, sin embargo, es probable que el juego de permiso de acceso para cada archivo pueda ser cambiado. El uso de las funciones auxiliares proporcionado por los SO permite hacer un apoyo.

4.4 Otras Técnicas de Seguridad

Acciones o amenazas que no pueden ser totalmente defendidas por las contramedidas normales por accesos ilegales.

4.4.1 On-time password

Esta técnica esta clasificada dentro del método Challenge/ respuesta y el método S/Key.Cuando el método Challenge / respuestas es usado, el usuario prepara una computadora pequeña llamada HHA (Hand-Held Authenticator). Para el usuario poder acceder al sistema, el o ella primero accede al servidor y recibe un código challenge de el. Cuando el usuario ingresa ese código dentro de HHA, este dispositivo crea una contraseña según la lógica predeterminada.

Cuando el método S/Key es usado, el usuario primero adquiere y almacena muchas contraseñas como el numero prescrito de accesos del servidor.
Cualquier método usado, la misma contraseña no puede usarse dos veces. Por consiguiente, si la contraseña es robada durante la transmisión de datos por la red y el ladrón intenta ganar acceso ilegal con la contraseña, el servidor ya no aceptara la contraseña, pero aceptara la nueva contraseña.

La técnica one- time password requiere una cantidad considerable de dirección de la contraseña y, por consiguiente, no es empleada en ambientes de oficinas ordinarias. Es usada dentro de circunstancias que requieren acceso de fuera, donde las contraseñas son vulnerables al robo, o donde un usuario dado es proporcionado con un servicio especifico por un limitado numero de tiempo.

4.4.2 Software Vacuna

Programa vacuna detecta la invasión de virus y lo extermina.
Este programa es empleado como medida de seguridad contra los virus de computadora. Las vacunas realizan dos funciones, detectar que computadora contiene un archivo infectado con un virus, y exterminación de este.

Al usar el software vacuna, deben tenerse presente los siguiente aspectos:
1. Siempre usar la ultima información de virus.
2. Hacer respaldos de archivos

1. *Antivirus:* La eficacia de un antivirus depende de su actualización, es importantísimo actualizarlo al menos 1 vez al mes. Diariamente aparecen en Internet decenas de virus que podrán atacarnos hasta que, primero, los antivirus los detecten, y segundo, nosotros actualicemos el antivirus en nuestro PC.

2. Si nos llega un ejecutable por correo que no haya solicitado, NO LO EJECUTE: incluso aunque venga de una persona conocida, los últimos virus como el conocido Melisa usaban la agenda del equipo infectado para mandar mails con el virus contenido en un gracioso attach. Lo más recomendable es borrarlo (si no lo ejecuta no le infectara).

3. Abra los documentos de Office (Word, Excel...) sin macros: si cuando abre un fichero de este tipo, le avisa que el fichero tiene macros, ábralo sin macros, probablemente sea un virus.

4.4.3 Cifrado

¿Qué es la criptografía?

La criptografía (kryptos = oculto + graphe = escritura) es el arte de escribir en clave o de forma enigmática.
En principio se puede expresar como el conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido. En la actualidad estas técnicas permiten además, asegurar que el mensaje no se ha modificado, reconocer al emisor del mensaje, probar la emisión y recepción del mensaje, etc.

¿Qué es la encriptación o cifrado?

La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado permitirá hacer legible un mensaje que estaba cifrado.

El propósito de la encriptación de los datos es hacer el contenido de la información incomprensible cuando esta es robada. El cifrado puede hacerse utilizando sistemas criptográficos simétricos o asimétricos y se puede aplicar extremo a extremo o individualmente a cada enlace del sistema de comunicaciones.

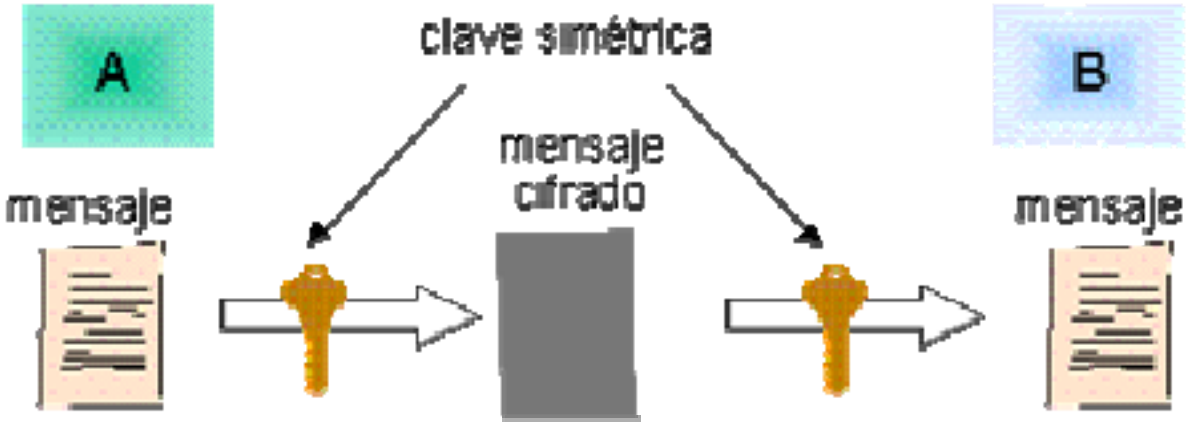
El cifrado garantiza que la información no es legible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública o asimétricos,

resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

- **Método de la Clave Privada.**

Los métodos de cifrado simétrico, por ejemplo el sistema DES, usan una misma clave para cifrar y descifrar. Suponiendo que dos interlocutores comparten una clave secreta y de longitud suficientemente grande, el cifrado simétrico permite garantizar la confidencialidad de la comunicación entre ellos. Este esquema es poco adecuado cuando una parte establece comunicaciones ocasionales con muchas otras con las que no tenía una relación previa, como ocurre frecuentemente en el comercio electrónico, ya que antes de poder establecer cada comunicación sería necesario intercambiar previamente por algún procedimiento seguro la clave que se va a utilizar para cifrar y descifrar en esa comunicación. Por ejemplo, un consumidor que quisiera comprar a través de Internet necesitaría intercambiar una clave secreta diferente con cada uno de los vendedores a los que quisiera acceder.

Esquema de Funcionamiento de Cifrado Simétrico:



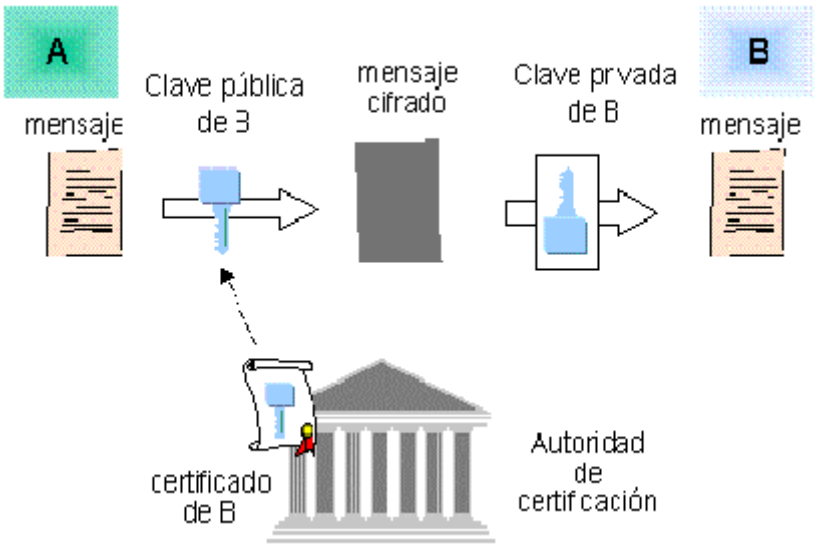
- **Método de la Clave Pública o Asimétrica**

Los esquemas de cifrado de claves públicas resuelven el problema del envío de las claves a los receptores de los mensajes. De hecho, permiten que una persona envíe un mensaje cifrado a otra sin que se haya realizado ningún intercambio previo. Ni siquiera es necesario que ninguna de las otras dos partes conozca a la otra, o que pertenezcan a la misma organización o estén conectadas a la misma red. Tan sólo es necesario que ambas partes tengan acceso a un servidor común que las gestione la seguridad de la clave pública.

Los sistemas de clave pública son más lentos que los simétricos y se utilizan para los servicios de autenticación, distribución de claves de sesión y firma digital.

El sistema de clave pública consta de dos claves. Cada usuario dispone de una clave privada junto con otra pública, que deja para que esté disponible en alguna ubicación pública. Cuando un usuario desea enviar un mensaje confidencial a otro usuario, cifra el mensaje con su propia clave privada. Los mensajes cifrados con clave pública tan sólo pueden ser descifrados con claves privadas.

Esquema de Funcionamiento del Cifrado Asimétrico:



Firma Digital

Esta técnica es usada por el método de Clave publica para prevenir la alteración y spoofing. Una firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

Las firmas digitales son métodos de cifrado que tienen dos propósitos:

- Validar el contenido de un mensaje electrónico y se puede utilizar posteriormente para comprobar que un emisor envió de hecho ese mensaje.

- Probar que no se ha falsificado un mensaje durante su envío. Las firmas digitales respaldan la autenticidad del correo electrónico, transacciones de contabilidad, órdenes de empresa, documentos para grupos de trabajo y otros mensajes y archivos que se trasladan entre sistemas, usuarios u organizaciones.

El firmante generará mediante una función, un 'resumen' o huella digital del mensaje. Este resumen o huella digital la cifrará con su **clave privada** y el resultado es lo que se denomina firma digital, que enviará adjunta al mensaje original.
Cualquier receptor del mensaje podrá comprobar que el mensaje no fue modificado desde su creación porque podrá generar el mismo resumen o misma **huella digital** aplicando la misma función al mensaje. Además podrá comprobar su autoría, descifrando la firma digital con la **clave pública** del firmante, lo que dará como resultado de nuevo el resumen o **huella digital** del mensaje.
Las firmas digitales autentifican los mensajes y se usan para validar compras, transferencias de fondos y otras transacciones de negocios. Un formulario con una firma digital debe incluir el nombre del emisor, la fecha y hora, junto con una secuencia numérica o identificación que identifique positivamente a la persona o a la transmisión.

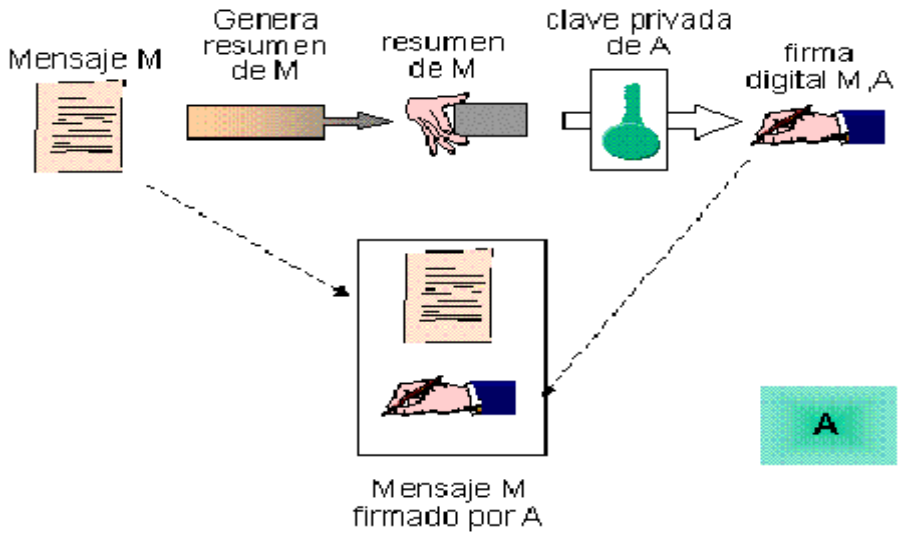
En resumen, el esquema de la firma electrónica sería el siguiente:

X elabora la síntesis del documento a enviar que es cifrado con su clave privada. Este resumen cifrado con su clave privada es de hecho su firma electrónica.

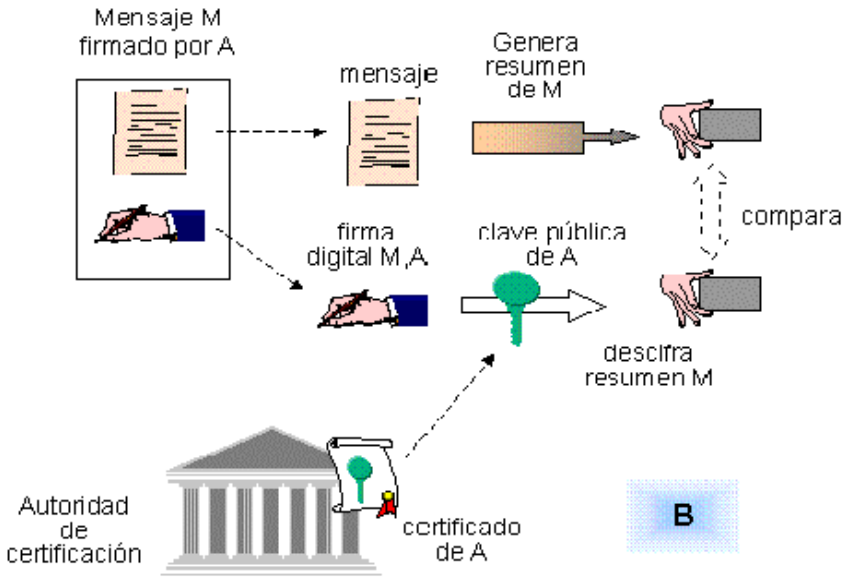
Y recibe el documento y genera un resumen del mismo usando la llamada función unidireccional de resumen. A continuación **Y** descifra con la clave pública de **X** que es conocida del resumen firmado por **X**.

Si este resumen firmado es coincidente con el que ha recibido la firma electrónica es válida ya que nadie excepto **X** podría haber firmado el documento. La integridad del documento queda también garantizada ya que si durante la transmisión hubiera sido alterado sería imposible generar la misma función de resumen que había sido firmada.

Generación de la Firma Digital de un Mensaje:



Comprobación de una Firma Digital:



4.4.4. SSL (Secure Socket Layer)

Es una técnica de encriptación desarrollada por Netscape y usada en Internet.

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP.

Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos. Primero se debe hacer una solicitud de seguridad. Después de haberla hecho, se deben establecer los parámetros que se utilizarán para SSL. Esta parte se conoce como *SSL Handshake*. Una vez se haya establecido una comunicación segura, se deben hacer verificaciones periódicas para garantizar que la comunicación sigue siendo segura a medida que se transmiten datos. Luego que la transacción ha sido completada, se termina SSL.

Solicitud de SSL:

Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio.

Una vez se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el *SSL Handshake*.

Intercambio de datos:

Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash de una vía acordado durante el handshake), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

Terminación de una sesión SSL:

Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente efectivamente desea abandonar la sesión SSL.

En una serie de sus procedimientos, las técnicas utiliza ambos métodos “Clave Secreta” y “Clave Publica”. El SSL puede ser usado por una variedad de servicios de Internet.

4.4.5. VPN (Virtual Private Network)

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos Firewalls y las VPN.

¿Para qué sirve una VPN?

La VPN es empleada para asegurar comunicaciones seguras dentro de una compañía o entre varias compañías, vía Internet.
Se utiliza para intercomunicar ordenadores y recursos mediante una transmisión remota, totalmente como si funcionáramos con una red local.

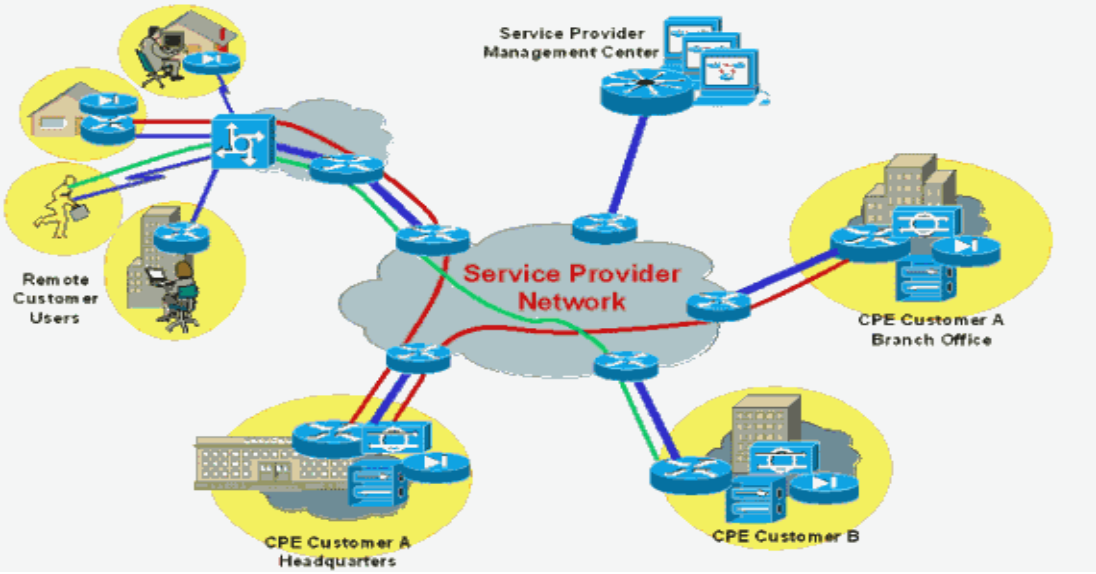
¿Por qué una VPN?

Cuando se desea enlazar oficinas centrales con alguna sucursal u oficina remota se tienen tres opciones:

MODEM: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

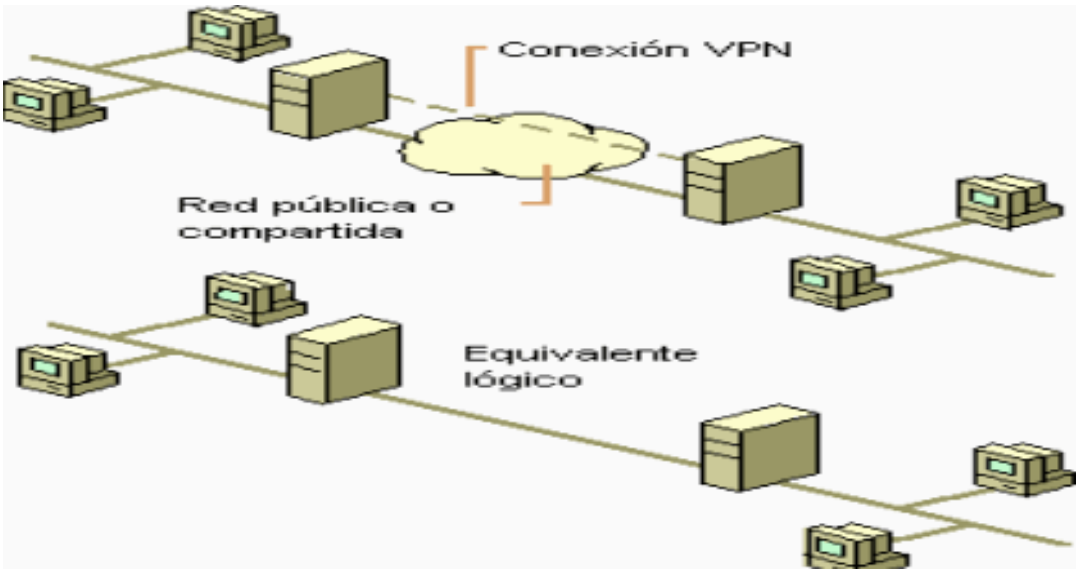
Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro.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

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



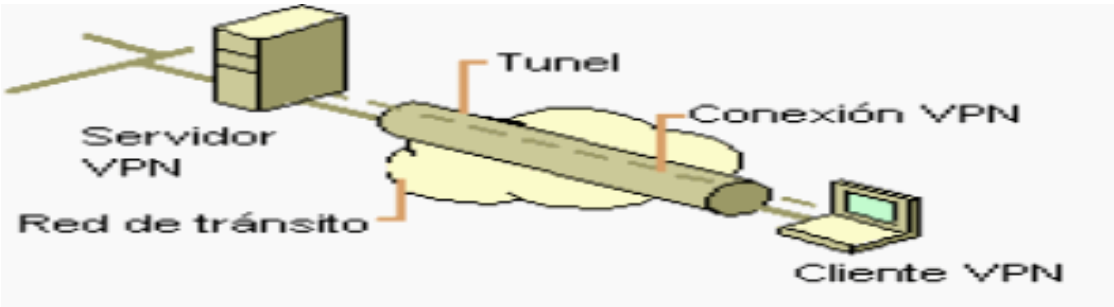
¿Que es una VPN?

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (ver figura siguiente)



Tecnología de túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.



¿Qué red pública usaremos?

Internet, es obviamente la red de redes que usamos todos. Es una red de carácter público. Se trata, como se mencionó anteriormente, de combinar recursos de red propios con recursos de redes públicas. El algunos casos especiales puede interesar no usar ningún recurso de Internet y usar otro tipo de recurso de red.

Ventajas de una VPN

Dentro de las ventajas más significativas podemos mencionar:

- La integridad, confidencialidad y seguridad de los datos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de acceso basado en políticas de la organización.
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el trafico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC remotas.
- Integrar todos sus servicios de voz en un plan de numeración privado
- Reducción de costos en los sistemas de comunicación de la empresa.
- Diversificación de conexiones con las que podemos trabajar, como telefonía fija, ADSL, RDSI...

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

4.5. Uso de Herramientas de Seguridad

Las herramientas pueden ayudarle a recoger la información y para reconocer las anomalías, examina, intrusiones y otros ataques. Usted puede usar que a las herramientas les gusta:

- Los sistemas de descubrimiento de intrusión (las IDENTIFICACIONES)
- La grabación de tráfico de red
- Las estadísticas de tráfico de red
- El Logparser
- Los olfateadores para las contraseñas, tráfico de la red y carga útil del paquete
- Los escáneres de vulnerabilidad

Cuando se encuentran los nuevos problemas de seguridad en programas es importante examinar la red e identificar las máquinas que son vulnerables a los ataques contra estos agujeros. Una idea buena para recomendar que en uno o más puertos estén cerrados para el tráfico externo.

Estas herramientas están ampliamente clasificadas dentro de tres tipos. Algunos productos ofrecen mas de una función mencionada aquí.

1. Herramientas de Prueba

Herramientas para localizar problemas relacionados con las áreas de seguridad cuando un sistema se introduce recientemente. Muchas de las herramientas de este tipo son ahora diseñadas para comprender el método de invasión de Hackers vía Internet. Para esto, la herramienta simula “ataques de penetración” en el sistema para descubrir los posibles agujeros de seguridad en el Firewall y el servidor.

2. Herramientas de Supervisión

Herramientas para monitorear o supervisar penetraciones ilegales por medio del chequeo de paquetes que atraviesen un firewall o que son transmitidos dentro de la LAN. Si se descubren paquetes ilegales, emitirá una alarma y entregara un log.

3. Herramientas de Análisis

Herramientas para detectar accesos ilegales y descubrir problemas relacionados con la seguridad analizando los logs entregados por la herramienta de supervisión.

5. PLANES DE CONTINGENCIA

Dentro de todo sistema de información responsable deben existir a demás de las políticas de seguridad (como normativas) un plan de contingencia (como medidas de acción). Al hablar de políticas de seguridad hay que contemplar tanto la prevención como la recuperación.

La mayor parte de las medidas de las que hemos hablado hasta este momento se refieren a la prevención ante posibles amenazas. Sin embargo, y como ya hemos comentado anteriormente, ningún sistema es completamente seguro, y por tanto hay que definir una estrategia a seguir en caso de fallo o desastre. De hecho los expertos de seguridad afirman sutilmente que hay que definir un plan de contingencia **para cuando falle** el sistema, no **por si falla** el sistema.

Llamaremos Plan de Contingencia a una estrategia planificada de acciones y productos que lleven a un sistema de información a sus centros de procesos de una situación inicial determinada (y a mejorar) a una situación mejorada. La realización de este no será presentada dentro de este trabajo debido a que sale del marco de desarrollo de nuestro trabajo investigativo; será presentado un cuadro de resumen con los aspectos mas importantes a tomar en cuenta.

La clave de una buena recuperación en caso de fallo es una preparación adecuada. Por recuperación entendemos tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo habiendo reemplazado o recuperado el máximo de los recursos y de la información.

Adicionalmente existen otros aspectos relacionados con la recuperación como son la detección del fallo, la identificación del origen del ataque y de los daños causados al sistema y la toma de medidas a posteriori contra el atacante. Todo ello se basa en buena medida en el uso de una adecuada política de monitorización y auditoria del sistema.

La recuperación de la información se basa en el uso de una política de copias de seguridad adecuada, mientras la recuperación del funcionamiento del sistema se basa en la preparación de unos recursos alternativos.

Las técnicas de seguridad son los elementos que nos ayudaran a solucionar con los aspectos antes mencionado.

Importancia de Contar con un Plan

- Además de seguridad, la empresa o institución gana en conocimiento real de sus fortalezas y debilidades.
- Si no lo hace se expone a sufrir una pérdida irreparable mucho más costosa que la implantación de este plan.

Algunas perdidas por no contar con un plan de contingencia serian:

- Pérdida de clientes
- Pérdida de imagen
- Pérdida de ingresos por beneficios
- Pérdida de ingresos por ventas y cobros
- Pérdida de ingresos por producción
- Pérdida de competitividad
- Pérdida de credibilidad en el sector

CAPITULO III. DISEÑO DEL MODELO DE SEGURIDAD DE LA UNAN-LEON

I. ELABORACION DE LAS POLÍTICAS GENERALES DE SEGURIDAD.

II. ANALISIS DEL SISTEMA.

III. ESTUDIO DE LAS CONTRAMEDIDAS.

IV. IMPLEMENTACION DE MEDIDAS Y TEST.

I. ELABORACION DE LAS POLÍTICAS GENERALES DE SEGURIDAD.

Para la elaboración de las políticas generales de seguridad se hizo un estudio general sobre el funcionamiento de la red, la estructura organizativa de la universidad, siguiendo el formato definido en el marco teórico, sobre los elementos que deben contener las políticas de seguridad.

El único que puede aprobar las Políticas de Seguridad de la UNAN-León es el Rector de la universidad.

A la División de Informática le corresponde desarrollar y operar los sistemas de informática académica y administrativa, así como la supervisión y control de las políticas de seguridad de la universidad. La división de informática está presidida por el Director General de Informática, contando además con un Sub Director.

1. Revisión de la Estructura de la División de Informática

En el grafico 3.1. se refleja de que la división de informática actualmente no cuenta con un área de seguridad, por lo que se procedió a su revisión y propuesta de reorganización.

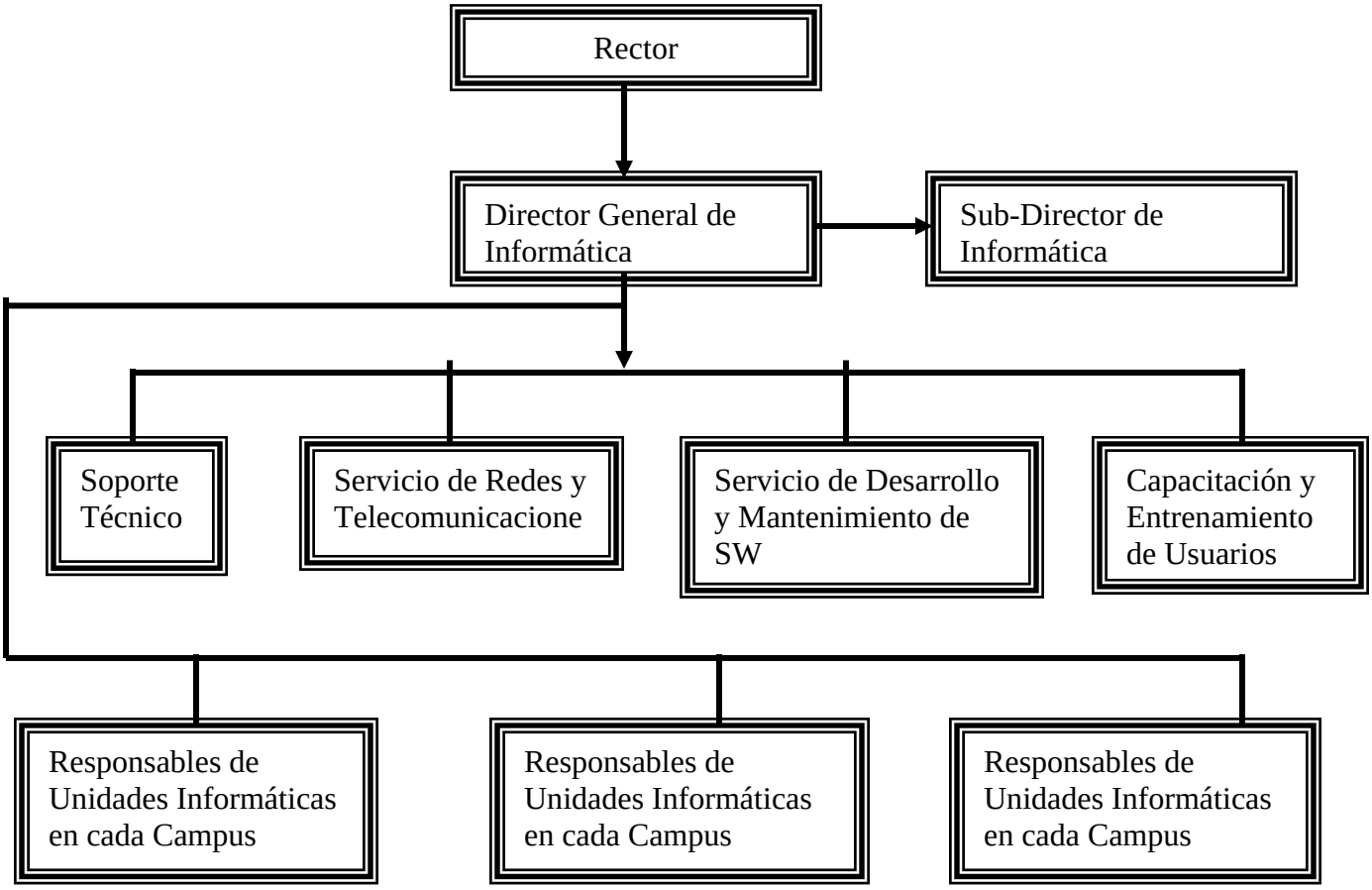


Gráfico 3.1. Estructura Actual de la División de Informática

Una vez realizado el análisis general, se discutió junto con la división de informática una nueva estructura organizativa de la universidad, tomando en cuenta nuevas ramas para una mejor estructura como son: La Auditoria informática, La Seguridad y Contingencias. Como se muestra en el siguiente organigrama.

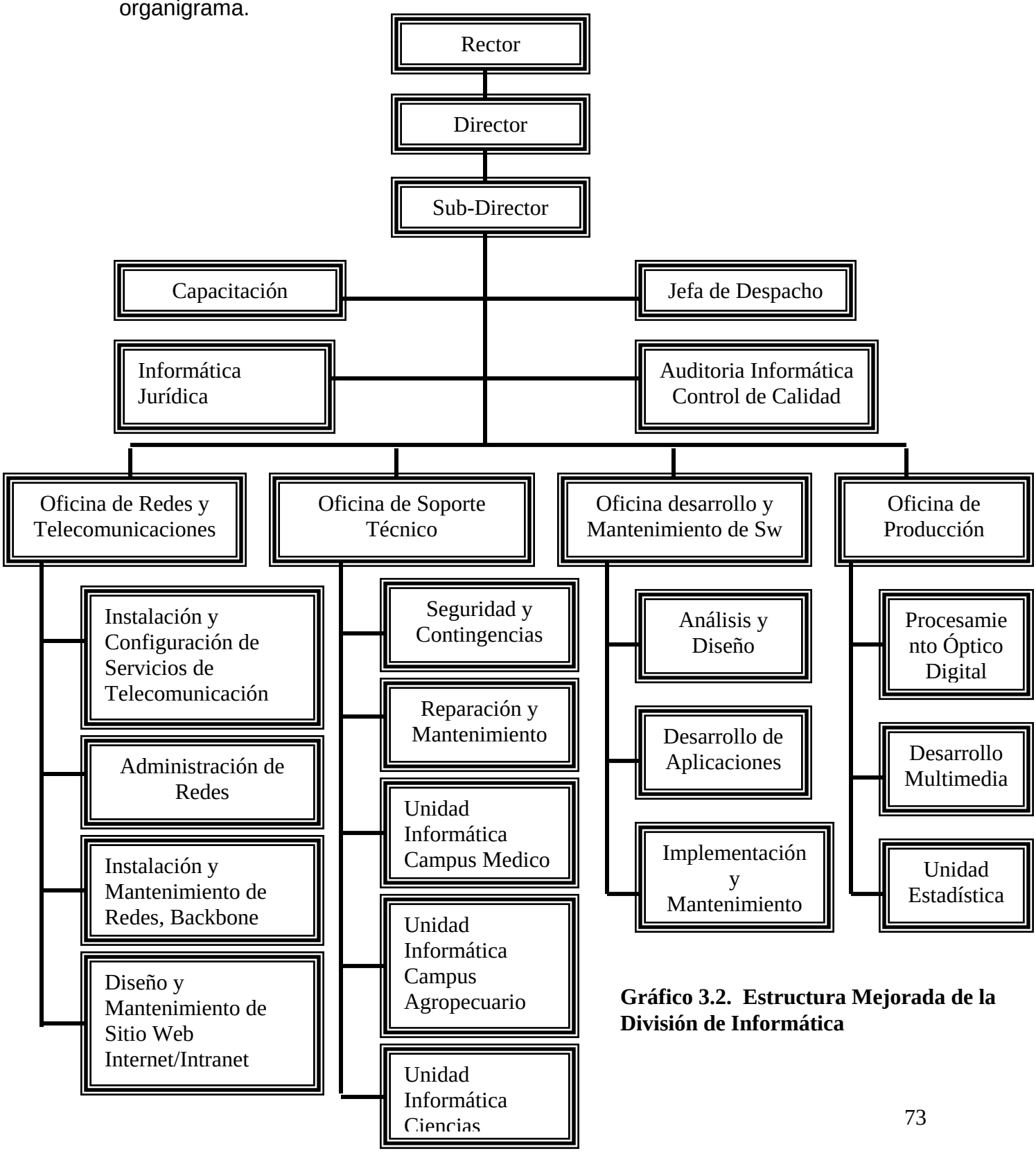


Gráfico 3.2. Estructura Mejorada de la División de Informática

2. Definición de los Niveles de Acceso a la Información

La seguridad es una obligación de todos, con diferentes niveles de acceso a la información. La información hay que priorizarla y jerarquizarla, es por eso que se definen varios niveles de acceso a la información dependiendo del valor de la información. Estos niveles de acceso deberán ser configurados en el servidor Intranet que es donde se guarda la información vital de la institución.

Rectoría	Nivel 1
Vice Rectorías	Nivel 2
Decanos	Nivel 3
Directores Departamentos Administrativos	Nivel 4
Directores Departamentos Académicos	Nivel 5
Personal Docente	Nivel 6
Personal Administrativo	Nivel 7
Gremios	Nivel 8
Estudiantes	Nivel 9

3. Estándares de Redes y Seguridad Informática

Aunque la Política de Seguridad de la institución establece la necesidad de la seguridad de la información, no especifica lo que se debe hacer para implementarla. Ésta es la función de los Estándares de Seguridad de la Información, y establecen lo siguiente:

- Lo que se debe hacer
- Los controles de seguridad que se requieren
- Controles de seguridad adecuados que se apliquen a cada elemento del entorno de protección de la información

Para ayudarle a las instituciones a desarrollar estándares de seguridad de la información, dos organismos de estándares han definido lo que deben considerar las instituciones para definirlos. El Instituto de Estándares Británico publicó la norma BS-7799 en 1995. Este documento fue presentado a aprobación por la Organización Internacional de Estándares (ISO) para producir un estándar internacional de seguridad de la información. En el año 2000, la ISO publicó una versión internacional de la BS-7799, conocida como ISO-17799.

La ISO también desarrollo la norma ISO-15408 en 1999, que define estándares de medidas de seguridad que se implementan en el hardware o software.

Los Estándares de Seguridad de la Información deben respaldar únicamente los requerimientos especificados en la Política de Seguridad de la Información. Si se exige el cumplimiento de la Política de Seguridad de la Información, también se exigirá el cumplimiento de los Estándares de Seguridad de la Información relacionados.

Para la elaboración de las políticas de seguridad del SI de la UNAN-León se tomó como base:

Organismos Internacionales que Norman los Estándares en Redes y Seguridad informática

ISO (International Organization for Standardization)
ITU-T (International Union of Telecommunications)
CCITT (Comite Consultivo Internacional Telefonico y Telegrafico)
IEEE (Institute of Electrical and Electronics Engineers)
RFC (Request For Comments)
ANSI (American National Standards Institute)
IEFT Security area (Internet Engineering Task Force)

Organismos Similares de Algunos Países en el Mundo

UK ITSec Scheme (UK)
CSRC (US)
Communication Security Establishment (Canada)
National Security Institute (US)
European Committee for Standardization
European Telecommunications Standards Institute
NOM (Norma Oficial Mexicana*****)

Regulaciones Nacionales

La Ley de Derechos de Autor y Derechos Conexos resguarda los derechos tanto morales como patrimoniales de los autores, entre las que se comprenden los programas de computación. Así, la Ley brinda a los autores, entre otros, los derechos de reproducción, distribución al público, alquiler e importación de las obras protegidas.

Ello significa que un programa de computación no puede ser copiado (excepto para propósitos de archivo), ni alquilado, distribuido al público, ni importado sin autorización del autor; sin embargo, las condiciones bajo las cuales puede ser utilizado un programa de computación dependen de la licencia de uso del programa específico.

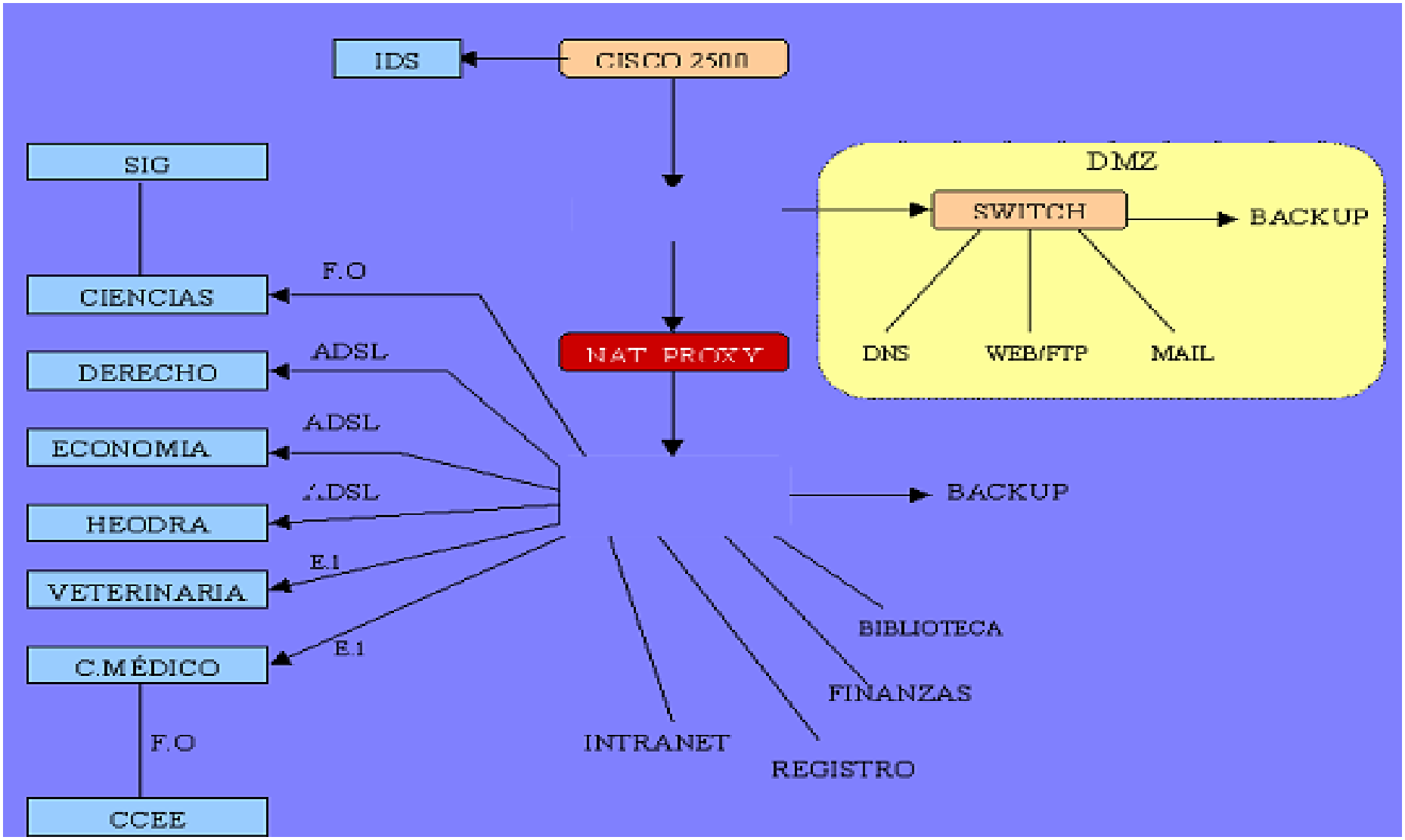
Ver Estándares Internacionales en Anexo Nº 4 . "Estándares Internacionales en Redes y Seguridad Informática"

II. ANALISIS DEL SISTEMA

Para la obtención de mejores resultados se realizo un análisis exhaustivo de la red de la universidad en dos partes:

1. **Análisis del diseño lógico de la red actual**: para el análisis de la red se requirieron la ayuda de herramientas de administración de redes como el Whats up, con el cual se determinaron los puntos y equipos de red conectados en la UNAN-León.

“Diseño Lógico Actual de Seguridad del SI de la UNAN-León”



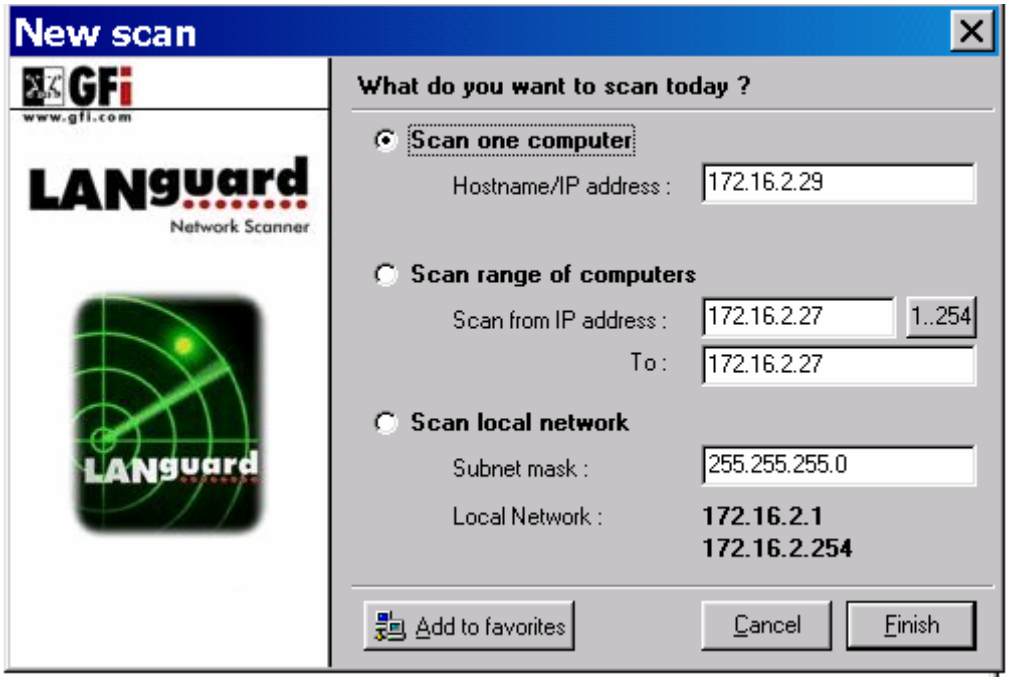
2. **Análisis de las vulnerabilidades y amenazas de la red**: Las herramientas utilizadas para esta etapa del análisis fueron:

   - El Sniffer, para olfatear el tráfico que circula por la red.

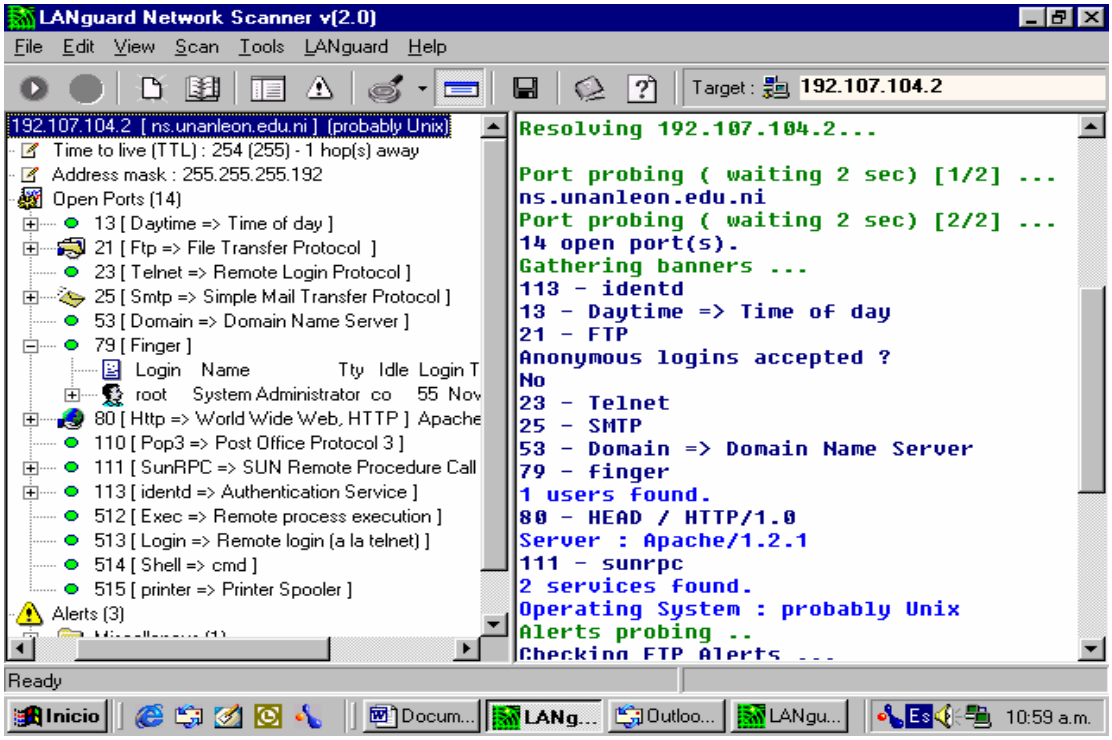
   - Herramientas Hackers como el LC3 y LC4 que permite obtener las contraseñas que existen en nuestro PC y las de otros ordenadores de la red, incluso para máquinas con Windows 2000 y Windows XP.

   - GetAdmin que permite darles los derechos de administrador a la cuenta de cualquier usuario en Windows 2000.

   - Otra herramienta utilizada es el LanportScan o Languard Network Scanner para detectar los puntos vulnerables de los servidores de la red.



En la imagen que se mostrara a continuación, se tomo como muestra el DNS 192.107.104.2 para hacer una representación del análisis de la red, y de esta manera se pueda entender mejor la forma como han sido analizados cada uno de los datos obtenidos.



Al observar los datos, se verá que existen 14 puertos abiertos.
Para la seguridad de nuestra red es importante que solo estén abiertos como máximo 4-7 puertos (por ejemplo DNS, SMTP, FTP y HTTP) y si esto no es así, como es en este caso, tenemos que proceder a cerrar los puertos que no son necesarios que estén abiertos.

Además se utilizó otra herramienta que es muy importante para el análisis de la red como es el IPTools.

Ver Resultados Anexos Nº 1. "Herramientas Utilizadas"

3. Problemas relacionados con el Protocolo TCP

En la RED UNAN, existen dos protocolos principalmente usados: Microsoft Net (Netbios) y TCP/IP. Existen muchos servicios corriendo en la red: Terminal server con NT, Servicios de bases de datos. En el nodo, Servidores web, dns, nat proxy, correo (smtp, pop, imap), servidores de tiempo NTP, servidores DHCP y acceso remoto.

Ataque al servidor web de la UNAN-León:

Como sabemos el servidor web escucha conexiones en el puerto 80, a continuación se muestra una pequeña parte de uno de los logs en el webserver, eso es persistente, todos los días.

[Sun Dec 22 04:39:03 2002] [error] [client 24.101.103.121] File does not exist: /usr/share/squirrelmail/scripts/..Á../winnt/system32/cmd.exe
[Sun Dec 22 04:39:04 2002] [error] [client 24.101.103.121] File does not exist: /usr/share/squirrelmail/scripts/..%5c../winnt/system32/cmd.exe
[Sun Dec 22 04:39:04 2002] [error] [client 24.101.103.121] File does not exist: /usr/share/squirrelmail/scripts/..%2f../winnt/system32/cmd.exe
[Sun Dec 22 05:27:14 2002] [error] [client 66.132.6.241] File does not exist: /usr/share/squirrelmail/c/winnt/system32/cmd.exe

En el texto del log, el atacante desde la maquina 24.101.103.121(puede ser un gusano en esa maquina y que el dueño ni se da cuenta por que fue hackeado) cree que el servidor es windows NT, pide ejecutar el comando cmd.exe. Pero se equivoca por que es UNIX.

Posiblemente algunas maquinas corriendo Windows 2000 o NT están expuestas (porque existen algunas sirviendo localmente).

Ataque al Mail Exhanger de la UNAN-León:

Qmail esta corriendo como MTA. Y no a diario pero esporádicamente hay algunas bombas de correo que llegan al server un ejemplo es el siguiente correo generado por el mismo sistema, enviado al administrador del correo (admin) reportando la falla.

Lo que sigue es un pedazo de un simple correo que llega al server desde **Alisha543@jax-inter.net** para **tonyramirez@unanleon.edu.ni**, este debería enviarse sin problemas porque el tal tony existe en el server,(como todo no?.)

Return-Path:<**Alisha543@jax-inter.net**>
Delivered-To:**tonyramirez@unanleon.edu.ni**
Received: (qmail 7411 invoked from network); 19 Mar 2003 00:35:08 -0000
Received: from unknown (HELO jax-inter.net) ([218.72.4.3])
(envelope-sender <**Alisha543@jax-inter.net**>)
by 0 (qmail-ldap-1.03) with SMTP
for <**tonyramirez@unanleon.edu.ni**>; 19 Mar 2003 00:35:08 -0000
From:Liza654 <**Alisha543@jax-inter.net**>
To:<**tonyramirez@unanleon.edu.ni**>
Subject:hey
Date: Wed, 19 Mar 2003 00:34:14 2003 00:34:14 +0000
Mime-Version:1.0
X-Priority:3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2911.0)
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

El server lo envía a tony como se lo pide el remitente pero aparentemente el encabezado del correo es malicioso y contiene una bomba para tony, el servidor luego tratara de enviar la bomba a tony, pero la cuenta de tony tiene un limite máximo de espacio consumido y se llena.

El servidor se da cuenta y regresa el correo a la dirección especificada en el campo Reply-To del remitente <**Alisha543@jax-inter.net**> pero esa es la mas maliciosa!. Trae quien sabe cuantos miles de Reply-To!. Así el servidor pasa como loco enviando correo a <**Alisha543@jax-inter.net**>. Una maquina con un MTA (Mail transfer Agent) se bloquearía (seria un DOS : Deny Of Service) enviando correos y botando las nuevas peticiones de otros clientes.

Pero el MTA utilizado en la universidad trae esa defensa así que después de 50 envíos, repetitivos de la bomba descubre que es un Loopback (lazo) y deja de hacerle caso. Bota ese proceso.

Aquí una copia del mensaje de error que llega al administrador del sistema:

127.0.0.100 failed after I sent the message.
Remote host said: 554 too many hops, this message is looping (#5.4.6)

Ese tal remote host es el mismo servidor que descubre este mensaje es looping (lazo).

Copia del mensaje:

From: **MAILER-DAEMON@aoc950.unanleon.edu.ni**
To: **postmaster@aoc950.unanleon.edu.ni**
Subject: failure notice

Hi. This is the qmail-send program at aoc950.unanleon.edu.ni.
I tried to deliver a bounce message to this address, but the bounce bounced!

<**Alissa969@jax-inter.net**>:
127.0.0.100 failed after I sent the message.
Remote host said: 554 too many hops, this message is looping (#5.4.6)

--- Below this line is the original bounce.
Return-Path: <>
Received: (qmail 8643 invoked from network); 17 Mar 2003 18:05:10 -0000
Received: from unknown (HELO aoc950.unanleon.edu.ni) ([127.0.0.100])
(envelope-sender <>)
by 0 (qmail-ldap-1.03) with SMTP
for <**Alissa969@jax-inter.net**>; 17 Mar 2003 18:05:10 -0000
Received: (qmail 8639 invoked from network); 17 Mar 2003 18:05:09 -0000
Received: from unknown (HELO aoc950.unanleon.edu.ni) ([127.0.0.100])
(envelope-sender <>)
by 0 (qmail-ldap-1.03) with SMTP
for <**Alissa969@jax-inter.net**>; 17 Mar 2003 18:05:01 -0000
Received: (qmail 8579 invo

--- End of message stripped.
---- End forwarded message -----

4. Resumen de las Vulnerabilidades y Amenazas de la Red

A partir del estudio realizado del análisis del sistema se creó una tabla llamada “Vulnerabilidades, Amenazas y Contramedidas del SI de la UNAN-León”, la cual esta dividida en 8 categorías, como se menciono en el marco teórico.

Procedimientos: Visitas al nodo y subnodos, entrevistas e informes de la división de informática.

A continuación se mostrará una tabla para hacer una representación de las vulnerabilidades mas graves que presenta la red de la UNAN-León.

Vulnerabilidades y Amenazas	Contramedidas
Acceso no autorizado a los nodos de telecomunicaciones y procesos.	**Crear un área u oficina exclusiva para los nodos de telecomunicaciones.**
Diseño General de la Red (HW)	**Crear el diseño general de la red.**
Hardware de Respaldo	**Tener dispositivos de respaldo.**
Equipos de Protección	**Adquisición de equipos Protectores**
Acceso desautorizado de usr externos a través de la red.	**Configuración de un firewall**
Agujeros de Seguridad	**Actualización de SW**
Problemas en el desarrollo del sistemas de inf. p/ la Universidad	**Implementación de la política de seguridad.**
Virus de Computadoras	**Usar el software de la vacuna**
Robo de dispositivos	**Inventario y sellos de seguridad**
Robo de datos bajo transmisión	**Encriptamiento de los datos**
Hackers	**Ver políticas de seguridad**

Tabla 3.1. Resumen de las Vulnerabilidades y Amenazas de la Red

Una de las vulnerabilidades más grandes, encontradas es que no existe un diseño lógico de la red, debido al crecimiento desordenado de la misma. Además que existen problemas en el desarrollo de sistemas de Información y esto es debido a que no existen políticas de seguridad en la universidad.

Con los resultados del análisis del sistema, se procedió a la inclusión de nuevas políticas de seguridad, que dio como resultado un documento final llamado “Políticas de Seguridad del SI de la UNAN-León”, en el cual como se mencionó en el marco teórico, establecen las normas y reglas que deben seguir los usuarios y administradores, así como las responsabilidades de cada una de las personas que utilizan la red. Estas políticas de seguridad son la base para establecer el modelo de seguridad de forma exitosa.

III. ESTUDIO DE LAS CONTRAMEDIDAS

Luego de un estudio y un análisis concreto logramos determinar las diferentes vulnerabilidades y amenazas que presenta nuestro sistema. Este estudio nos llevó a determinar los problemas específicos que presenta, tanto el sistema de información como la institución, en lo que a seguridad se refiere.

Las vulnerabilidades y amenazas que presenta el sistema pueden ocasionar fallas graves, el modelo de seguridad propuesto da respuesta a estas debilidades, de tal forma que a la par de cada vulnerabilidad encontrada se especifica la o las contramedidas que se deben realizar para contrarrestarla y se van completando las políticas de seguridad.

1. Vulnerabilidades, Amenazas y Contramedidas del SI de la UNAN-León

VULNERABILIDADES Y AMENAZAS	M	R	B	E	OBSERVACIONES	CONTRAMEDIDAS
1. FISICAS						
Acceso de usuarios no autorizados a los centros de telecomunicaciones y de procesamiento de datos.			X		Esto es debido a que los locales donde se encuentran los nodos no están separados de las oficinas de atención al público	- Crear una sala de computadoras u oficina exclusiva para los nodos de telecomunicaciones donde solo tenga acceso el personal autorizado.
2. NATURALES						
- Mala ambientación en los locales donde se encuentran los dispositivos	X				Demasiada humedad debido a Huracanes. Algunos locales tienen poca refrigeración	- Proteger los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- Corte de energía eléctrica					Debido al mal servicio que brinda la empresa de energía Unión FENOSA	- Usar protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles. - Tomar medidas para separar las actividades de electricistas, personal de tendido y mantenimiento de tendido de líneas telefónicas.
- Vulnerabilidad ante Incendios		X			No hay extinguidores	- Deben existir extinguidores de incendios en las salas de comunicaciones.
- Vulnerabilidad ante Tormentas eléctricas		X			No hay suficientes equipos de protección	- Deben existir equipos de protección como protectores de voltaje, estabilizadores, etc. - Deben de desconectar los equipos.

VULNERABILIDADES Y AMENAZAS	M	R	B	E	OBSERVACIONES	CONTRAMEDIDAS
- Vulnerabilidad de suciedad y Polvo		X				- Deben existir reglamentos dentro de cada oficina de trabajo de modo que no se permite fumar, comer o beber mientras se está usando un PC. - Deben existir procedimientos de limpieza de equipos.
3. HARDWARE						
Equipos de PC		X			No hay una estandarización del HW	- El HW y SW deben de estar estandarizados.
	X				Equipos obsoletos dentro de las LAN.	- Adquisición de equipos actualizados.
					Equipos de servidores son clones y sin certificación.	- Actualización de los servidores.
Diseño General de la Red	x				Ausencia de un diseño general de la red debido al crecimiento desordenado.	- Crear el diseño general de la red según los procedimientos establecidos.
Equipos de Protección		X			No hay suficientes: Protectores de voltaje, Protectores de Línea, Backups y estabilizadores	- Deben existir equipos de protección como protectores de voltaje, protectores de líneas, backup y estabilizadores.
Hardware de Red de Respaldo		x			No existen suficientes tarjetas de red, cable, servidores, hubs, routers, switch.	- Deberá de existir respaldos de tarjetas de red, cables, hub, router, switch. - Deberá existir alternativas de respaldo de comunicaciones, considerando la seguridad física de estos lugares.

VULNERABILIDADES Y AMENAZAS	M	R	B	E	OBSERVACIONES	CONTRAMEDIDAS
4. SOTFWARE						
Agujeros de Seguridad		x			No todos los responsables realizan las actualizaciones de SW, patches, service pack.	- En las computadoras deberán de instalarse patches, service pack para la detección de los agujeros de seguridad. Se deberán de hacer actualizaciones de éstas.
Problemas en el desarrollo de sistemas para la Universidad	X				No hay una política de auditoria al momento del desarrollo de los SW.	-Implementación de la política de auditoria.
SW no actualizado		X			Poca actualización de los SW, versión.	- Todos los SW instalados en los computadores deberán de ser actualizados constantemente.
Virus de Computadoras		X			Destrucción del sistema o datos por el correo o la descarga archiva de los sitios de Internet con los virus de computación	- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto. - No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa.

VULNERABILIDADES Y AMENAZAS	M	R	B	E	OBSERVACIONES	CONTRAMEDIDAS
5. DISPOSITIVOS						
Vulnerabilidad ante el Robo de dispositivos como diskets, CD de copias de seguridad. Robo de Disco Duro		x			En algunas oficinas las PC tiene su disco duro muy accesible al público, de tal forma que su extracción no sería nada difícil.	- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
6. COMUNICACIONES						
Vulnerabilidad de Robo o alteración de datos durante la transmisión	X					- La información de la universidad clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas.
Vulnerabilidad de acceso a la red a través de ordenadores	X					- Deben prohibirse introducir programas personales o conectar equipos privados a la red local. - Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

VULNERABILIDADES Y AMENAZAS	M	R	B	E	OBSERVACIONES	CONTRAMEDIDAS
Acceso de usuarios externos a la red interna a través de Internet		x			No existía un Firewall para toda la institución.	- Instalación y configuración de Firewall - Todos los accesos no autorizados están bloqueados. En equipos activos de comunicaciones, como puentes, encaminadores, conmutadores, etc.
7. HUMANAS						
Vulnerabilidad de Robo de documentos descartados (incluso los desechados) debido al acceso inadecuado.					- Recogiendo los documentos de una caja de la basura.	- No deben desatenderse las impresoras, sobre todo si se esta imprimiendo (o se va a imprimir) información confidencial de la Universidad. - Los archivos de registro son revisados, si es posible a través de herramientas automáticas, diariamente, vigilando intentos impropios de acceso. - Al desechar los documentos viejos, nunca simplemente los tire. Siempre póngalos a través de una desfibradora.
Errores de Administrador			x		Toda la seguridad del sistema descansa sobre el administrador que tiene acceso al máximo nivel y sin restricciones al mismo.	- Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas.
Errores de Usuarios		x			Ellos son los que pueden acceder a la red, tanto físicamente como mediante conexión.	- Los usuarios de PC son responsables de proteger los programas y datos contra pérdida o daño.

VULNERABILIDADES Y AMENAZAS	M	R	B	E	OBSERVACIONES	CONTRAMEDIDAS
8. INTERNET						
Hackers	x				Ataques por los Hackers	- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PC que tengan también conexión a la red local (LAN). Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Universidad. - Periódicamente se ejecuten ataques para descubrir vulnerabilidades, que los resultados se documenten y se corrijan las deficiencias observadas.

2. Políticas de Seguridad

La base para el modelo de seguridad son las políticas de seguridad, para lo cual se elaboró un documento llamado “Políticas de Seguridad del SI de la UNAN-León”. Este documento deberá ser firmado por el rector de la universidad para su aprobación e implementación. El cumplimiento de estas políticas de seguridad quedará en manos del encargado (jefe de seguridad) quien será designado por el director general de informática.

Recomendamos aplicar algunas de las contramedidas mencionadas en el apartado 3 del marco teórico, y técnicas de seguridad mencionadas en el apartado 4 del marco teórico.

UNIVERSIDAD NACIONAL AUTONÓMA DE NICARAGUA-LEÓN

(UNAN-LEÓN)

POLÍTICAS DE SEGURIDAD DE LA UNAN-LEÓN

León, 2003

CONTENIDO

La instancia encargada de la supervisión y control de las presentes Políticas de Seguridad es la División de Informática de la UNAN-León, estas serán aprobadas por el Rector de la universidad.

I. POLITICAS DE SEGURIDAD DE LA UNAN-LEON

1.1 Estructura Orgánica Para La Implementación De Las Políticas

1. **La División de Informática** monta los procesos informáticos seguros. La división general de Informática está integrada por las siguientes oficinas:

- Soporte Técnico.
- Servicio Redes y Telecomunicaciones.
- Servicio de Desarrollo y Mantenimiento de Software.
- Capacitación y Entrenamiento a Usuarios.
- Responsables de Unidades Informáticas en cada Campus.
- Unidad de Servicios Externos.

- La División de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos. El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito.

- El comité de seguridad Informática está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones

trimestrales, el Comité efectuará la evaluación y revisión de la situación de la Universidad en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad. En caso de no existir, debe ser creado.

2. **El Control Interno Informático**

- Tiene funciones propias (administración de la seguridad lógica, etc).
- Definición de propietarios y perfiles según "Clasificación de la Información".
- Administración delegada en control dual de la seguridad lógica.
- Responsable del desarrollo y actualización del plan de contingencias, manuales de procedimientos y plan de seguridad.
- Promover el plan de seguridad informática al comité de seguridad.
- Dictar normas de seguridad informática.
- Definir los procedimientos y plan seguridad.
- Control del entorno de desarrollo.
- Control de soportes magnéticos según la clasificación de la información, control de soportes físicos.
- Control de información comprometida o sensible.
- Control de microinformática y usuarios.
- Control de calidad de software.
- Control de calidad del servicio informático.
- Contactos externos con entidades relacionadas con la seguridad de la información.
- Definición de requerimientos de seguridad en proyectos nuevos.
- Vigilancia del cumplimiento de las normas y controles.

- Control de medidas de seguridad física o corporativa en la informática.

- Control de los responsables de oficinas.

3. **Los usuarios** son responsables de cumplir con todas las políticas de la Universidad relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Universidad a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Universidad a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Universidad.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Universidad y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

4. **La Auditoria Informática**

- Tiene la función de vigilancia y evaluación mediante dictámenes.
- Evalúan la eficiencia, costo y seguridad en su más amplia visión, esto es todos los riesgos informáticos, o los costos y los jurídicos.
- Utilizan metodologías de evaluación.
- Establecen planes quinquenales como ciclos completos.
- Sistemas de evaluación de repetición de la auditoria por nivel de exposición del área auditada.
- La función de soporte informático de todos los auditores.
- El director y subdirector de informática son los encargados de elaborar el plan de auditoria así como determinar el responsable encargado de realizarla.

1.2. Definición De Las Políticas De Seguridad

1.2.1 POLÍTICAS DE SEGURIDAD FÍSICA

Objetivos:

- Controlar las áreas para los equipos de comunicaciones y equipos TIC en general.
- Proteger y tender adecuadamente los cables y líneas de comunicaciones.
- Atender la recuperación de los sistemas de comunicación de datos en el plan de contingencia.
- Controlar las líneas telefónicas normales con acceso a la red de datos.

Alcance:

Esta política se aplica a las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y por supuesto a todo el personal de la Universidad.

Definiciones:

- **TIC:** Tecnología de la Información y Comunicaciones.
- **Hardware:** Técnica, equipos (computadoras y periféricos).
- **Software:** Conjunto de programas que se instalan a las computadoras para que realicen funciones determinadas.
- **Plan de Contingencia:** Estrategia planificada de acciones que llevan a un sistema de información a sus centros de procesos de una situación inicial determinada a una situación mejorada.
- **Servidor Web:** Servidor que permite la navegación por Internet por medio del www (World Wide Web) o telaraña amplia mundial, utilizando enlaces entre paginas con un formato definido, dichas paginas se encuentran alojadas en computadoras llamadas servidores Web.
- **Servidor DNS:** (Domain Name Server) Servidor de nombre de dominio.
- **Servidor FTP:** (File Transfer Protocol) Servidor que utiliza del servicio FTP o protocolo de transferencia de archivos.

Declaración de políticas:

1.2.1.1. Los computadores de la Universidad sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

1.2.1.2. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

1.2.1.3. Deben de desconectarse todos los equipos de la sala de comunicaciones u oficinas cuando haya tormenta eléctrica.

1.2.1.4. Deben existir extinguidotes de incendios en las salas de comunicaciones.

1.2.1.5. La seguridad física de los equipos de comunicaciones, tales como controladores de comunicaciones, dentro de las salas de computadores debe ser adecuada.

1.2.1.6. Deben de existir procedimientos para la protección de cables y bocas de conexión que dificulten el que sean interceptados o conectados por personas no autorizadas.

1.2.1.7. Los equipos de la Universidad sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

1.2.1.8. Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática.

1.2.1.9. Deben existir reglamentos dentro de cada oficina de trabajo de modo que no se permite fumar, comer o beber mientras se está usando un PC.

1.2.1.10. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

1.2.1.11. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

1.2.1.12. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla.

1.2.1.13. Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

1.2.1.14. Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

1.2.1.15. El equipo de comunicaciones se mantiene en habitaciones cerradas con acceso limitado a personas autorizadas.

1.2.1.16. Sólo personas con responsabilidad y conocimientos están incluidas en la lista de personas permanentemente autorizadas para entrar en las salas de equipos de comunicaciones.

1.2.1.17. No pueden moverse los equipos o reubicarlos sin permiso.

1.2.1.18. Tomar medidas para separar las actividades de electricistas, personal de tendido y mantenimiento de tendido de líneas telefónicas, así como sus autorizaciones de acceso, de aquellas del personal bajo control de la gerencia de comunicaciones.

1.2.1.19. En las zonas adyacentes a las salas de comunicaciones, todas las líneas de comunicaciones deben estar fuera de la vista.

1.2.1.20. Las líneas telefónicas usadas para datos, cuyos números no deben ser públicos, tienen dispositivos/procedimientos de seguridad tales como retrollamada, códigos de conexión o interruptores para impedir accesos no autorizados al sistema informático.

1.2.1.21. Las líneas de comunicaciones, en las salas de comunicaciones, armarios distribuidores y terminaciones de los despachos, estarán etiquetadas con un código gestionado por la división de informática, y no por su descripción física o métodos sin coherencia.

1.2.1.22. Las computadoras y equipos electrónicos deben tener sellos de seguridad.

1.2.1.23. Revisar periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.

1.2.1.24. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicación de datos deben tener propósitos y funciones definidos.

1.2.1.25. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados para monitorizar líneas y fijar problemas incluyendo procedimiento restringido, facilidades de traza y registro del tráfico de datos, procedimientos de aprobación y registro.

1.2.1.26. En el plan de contingencia para servicios de información presta adecuada atención a la recuperación y vuelta al servicio de los sistemas de comunicación de datos.

1.2.1.27. Deben existir planes de contingencia para desastres que sólo afecten a las comunicaciones, como el fallo de una sala completa de comunicaciones.

1.2.1.28. Las alternativas de respaldo de comunicaciones, bien sea con las mismas salas o con salas de respaldo, consideran la seguridad física de estos lugares.

1.2.1.29. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

1.2.1.30. Deberá de existir respaldos de tarjetas de red, cables, hub, router, switch, disco duro.

1.2.1.31. Deben existir equipos de protección como protectores de voltaje, protectores de líneas, backup y estabilizadores.

1.2.1.32. Deben existir Backup de los servidores DNS, FTP, Web y MAIL.

1.2.2 POLÍTICAS DE SEGURIDAD LÓGICA

Objetivos:

- Marcar la existencia de contraseña y otros procedimientos que limiten y detecten cualquier intento de acceso no autorizado a la red de comunicaciones.
- Facilitar el control de errores para detectar errores de transmisión.
- Asegurar que las transmisiones van solamente a usuarios autorizados.
- Registrar las actividades de la red.
- Marcar las técnicas de cifrado de datos.
- Controlar adecuadamente la importación o exportación de datos.

Alcance:

Estas políticas se aplican a cada usuario que pueda acceder a los recursos, empleados, contratistas, consultores, personal temporal de la Universidad.

Definiciones:

- **Cifrado:** Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.
- **Hardware:** Técnica, equipos (computadoras y periféricos).
- **Software:** Conjunto de programas que se instalan a las computadoras para que realicen funciones determinadas.
- **Servidor Web:** Servidor que permite la navegación por Internet por medio del WWW (World Wide Web) o telaraña amplia mundial utilizando enlaces entre páginas con un formato definido, dichas páginas se encuentran alojadas en computadoras llamadas servidores Web.
- **Cortafuegos:** Es un sistema o un grupo de sistemas que decide que servicios pueden ser accedidos desde el exterior de una red privada.
- **Intranet:** Es la propia red interna. Es una extensión de esta para ofrecer una interfase de fácil utilización en toda la información pública y privada (utilizando las posibilidades de exploración grafica de Internet).
- **Internet:** Red de comunicaciones que une entre si millones de ordenadores en todo el mundo cuyos usuarios pueden recibir y enviar información, noticias o imágenes de cualquier otro ordenador de la red.
- **LAN:** Local Área Network – Red de Área Local.
- **Hackers:** Personas que acceden a un sistema protegido como si se tratara de un reto personal, sin intentar causar daños.

Declaración de políticas:

1.2.2.1. El software de comunicaciones, para permitir el acceso, exige código de usuario y contraseña.

1.2.2.2. Revisar el procedimiento de conexión de usuario y comprobar que no puedan acceder a ningún sistema antes de haberse identificado, que sea incapaz de dar la contraseña, a cambiar la contraseña regularmente, estas no son mostradas en pantalla cuando se teclean.

1.2.2.3. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

1.2.2.4. El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas

1.2.2.5. La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión.

1.2.2.6. Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

1.2.2.7. Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Universidad, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Universidad sin la debida aprobación.

1.2.2.8. No debe concederse una cuenta a personas que no sean empleados de la Universidad a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días, a menos que sea bajo contrato.

1.2.2.9. Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

1.2.2.10. No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Director de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

1.2.2.11. Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.

1.2.2.12. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días, sin incluir vacaciones y días feriados.

1.2.2.13. Cuando un empleado es despedido o renuncia a la Universidad, debe desactivarse su cuenta antes de que deje el cargo.

1.2.2.14. Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

1.2.2.15. Para el acceso remoto a los recursos informáticos de la universidad, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

1.2.2.16. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Universidad está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

1.2.2.17. Cualquier procedimiento del fabricante, mediante Hardware o Software, que permita el libre acceso y que haya sido utilizado en la instalación original, ha de haber sido inhabilitado o cambiado.

1.2.2.18. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.

1.2.2.19. Deben prohibirse introducir programas personales o conectar equipos privados a la red local.

1.2.2.20. Los usuarios no deben copiar a un medio removible (como un disquete), el software o los datos residentes en las computadoras de la Universidad, sin la aprobación previa de la División de Informática.

1.2.2.21. No deben usarse disquetes u otros medios de almacenamiento en cualquier computadora de la Universidad a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

1.2.2.22. No pueden extraerse datos fuera de la sede de la Universidad sin la aprobación previa de la División de Informática. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

1.2.2.23. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

1.2.2.24. No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

1.2.2.25. El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

1.2.2.26. Siempre que sea posible, deba eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la universidad.

1.2.2.27. No deben desatenderse las impresoras, sobre todo si se esta imprimiendo (o se va a imprimir) información confidencial de la Universidad.

1.2.2.28. Deben de existir procedimientos de registro para capturar y ayudar a reconstruir todas las actividades de las transacciones.

1.2.2.29. El personal que utiliza un computador portátil que contenga información confidencial de la universidad, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

1.2.2.30. La información de la universidad clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la División de Informática.

1.2.2.31. Si se utiliza cifrado debe de existir procedimientos de control sobre el intercambio de claves, estás deben de ser cambiadas regularmente.

1.2.2.32. Los canales de comunicación que unen diversos edificios de la misma universidad, y sobre los cuales circulen datos sensibles, estos canales se cifran automáticamente, para evitar que una interceptación sistemática a un canal comprometa a todas las aplicaciones.

1.2.2.33. Si se utiliza la transmisión de datos sensibles a través de redes abiertas como Internet, comprobar que estos datos viajan cifrados.

1.2.2.34. Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña.

1.2.2.35. Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

1.2.2.36. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

1.2.2.37. Las herramientas antivirus deben actualizarse constantemente.

1.2.2.38. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos o facultades de la universidad.

1.2.2.39. Se deben tomar estadísticas que incluyan tasas de errores y de retransmisión.

1.2.2.40. Los protocolos utilizados, revisados con el personal adecuado de comunicaciones, deben disponer de procedimientos de control de errores con la seguridad suficiente.

1.2.2.41. Los mensajes lógicos transmitidos identifican el origen, la fecha, la hora y el receptor.

1.2.2.42. Deben de existir controles para que los datos sensibles sólo puedan ser impresos en las impresoras designadas y vistos desde los terminales autorizados.

1.2.2.43. Los archivos de registro son revisados, si es posible a través de herramientas automáticas, diariamente, vigilando intentos impropios de acceso.

1.2.2.44. Si en una red local existen computadores con módems, se debe revisar los controles de seguridad asociados para impedir el acceso de equipos foráneos a la red local.

1.2.2.45. Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PC que tengan también conexión a la red local (LAN). Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Universidad.

1.2.2.46. Todos los accesos no específicamente autorizados están bloqueados. En equipos activos de comunicaciones, como puentes, encaminadores, conmutadores, etc. Esto significa que los accesos para servicio remoto están inhabilitados o tienen procedimientos específicos de control.

1.2.2.47. Periódicamente se ejecuten, mediante los programas actualizados y adecuados, ataques para descubrir vulnerabilidades, que los resultados se documenten y se corrijan las deficiencias observadas. Estos ataques deben realizarse independientemente a:
- Servidores, desde dentro del servidor.
- Servidores, desde la red interna.
- Servidores Web, específicamente.
- Intranet, desde dentro de ella.
- Cortafuegos, desde dentro de ellos.
- Accesos desde el exterior y/o Internet.

1.2.2.48. Deben existir reglamentos dentro de cada oficina de trabajo de modo que no se permite fumar, comer o beber mientras se está usando un PC.

1.2.2.49. Debe de existir procedimientos de limpieza de las PC.

1.2.3 POLÍTICAS DE SEGURIDAD DE APLICACIONES

Objetivos:

- Verificar el grado de fiabilidad.
- Determinar la idoneidad del SCA de la aplicación.

Alcance:

Esta política es aplicable a cada uno de las personas que utilizan el sistema de información de la Universidad.

Definiciones:

- **SCA** (Sistema de control de acceso): controles referentes a la identificación de usuarios y posibles intentos reiterados de accesos no autorizados.

Declaración de políticas:

1.2.3.1. Asegurar la eficacia y seguridad del SCA.

1.2.3.2. Si el SCA no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

1.2.3.3. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Universidad, pudiendo ser causal de despido.

1.2.3.4. Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

1.2.3.5. Las asignaciones de perfiles a usuarios responden a los puestos que ocupan y se evita la asignación de perfiles a usuarios únicos en cada centro operativo.

1.2.3.6. La asignación de operaciones y funcionalidades permitidas a cada uno de los perfiles de usuario diseñado responde a criterios de necesidad para el desempeño del trabajo y segregación de funciones.

1.2.3.7. Eficacia de los controles manuales y programados de entrada, proceso y salida.

1.2.4 POLÍTICAS DE SEGURIDAD DE LOS DATOS

Objetivo:

- Garantizar la protección de datos, de forma que los datos viajen desde su origen hasta si destino sin alteración alguna.
- Detener el acceso desautorizado a datos que usa la red.

Alcance:

Estas políticas son aplicables a Servidores, los PC que conforman la red y cualquier dispositivo utilizado para la seguridad de datos.

Definiciones:

- **Cifrados:** Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado.
- **PC:** Personal Computer - Computadora Personal.

Declaración de políticas:

1.2.4.1. Periódicamente debe hacerse el respaldo de los datos guardados en PC y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de la Universidad debe guardarse en otra sede, lejos del edificio.

1.2.4.2. Los usuarios de PC son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los responsables de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

1.2.4.3. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los encargados de los distintas áreas son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

1.2.4.4. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

1.2.4.5. En el proceso de los datos se deben controlar la validación, integridad, almacenamiento, que existan copias suficientes, sincronizadas y protegidas.

1.2.4.6. Se debe de detectar errores e intentos de fraudes.

1.2.4.7. Retención de la información y protección en función de su clasificación.

1.2.4.8. Clasificación de los datos.

1.2.4.9. No debe de haber más de cuatro o cinco niveles de clasificación de datos.

1.2.4.10. Aquellos soportes que contengan datos o información de los niveles más críticos estarán especialmente protegidos, incluso cifrados.

1.2.4.11. Restricción de su uso para pruebas.

1.2.4.12. Algunas entidades deben de tener etiquetas o carátulas para diferenciar soportes, listados y documentos cuyo contenido es clasificado.

1.2.4.13. El transporte de datos clasificado debe realizarse por canales seguros, por transmisión deben ir cifrados, cerrados y que la llave no éste en poder de los transportistas o esté protegida.

1.2.4.14. Los datos ubicados en los servidores de la institución son patrimonio de la misma y no podrán ser facilitados a entidades externas sin la autorización de la dirección superior.

1.2.5 POLÍTICAS DE SEGURIDAD EN COMUNICACIONES Y REDES

Objetivos:

- Marcar la existencia de un departamento de comunicaciones con autoridad para establecer procedimientos y normativas.
- Marcar la existencia de procedimientos y registros de inventarios.
- Determinar funciones de vigilancia del uso de la red de comunicaciones, ajuste de rendimiento, registro de incidencias y resolución de problemas.
- Asegurar la participación activa del departamento de comunicaciones en el diseño de las nuevas aplicaciones online para asegurar que se siga la normativa de comunicaciones.
- Establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la Universidad al estar conectada a la red.

Alcance:

Esta política es aplicable a todas las dependencias de la UNAN-León y personal temporal de la Universidad.

Definiciones:

- **Sniffers:** Este método es utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan al ingresar a sistemas de acceso remoto.
- **Sistemas OnLine:** Sistemas en líneas
- **UNAN-Léon:** Universidad Nacional Autónoma de Nicaragua -León
- **FO:** Fibra Óptica - es un fino filamento de material transparente utilizado como guía de onda para luz, la cual a su vez es portadora de información.
- **ATM** (Modo de Transferencia Asíncrona): Es un protocolo nuevo para las Interredes de alta velocidad. La arquitectura sobre la maquina del usuario es similar a la arquitectura TCP/IP.
- **Servidor Web:** Servidor que permite la navegación por Internet por medio del WWW (World Wide Web) o telaraña amplia mundial, utilizando enlaces entre paginas con un formato definido, dichas paginas se encuentran alojadas en computadoras llamadas servidores Web.
- **Servidor DNS:** (Domain Name Server) Servidor de nombre de dominio.
- **Servidor FTP:** (File Transfer Protocol) Servidor que utiliza el protocolo de transferencia de archivos.
- **Firewall:** (Cortafuegos) Es un sistema o un grupo de sistemas que decide que servicios pueden ser accedidos desde el exterior de una red privada.
- **HW:** (Hardware) equipos (computadoras y periféricos).

- **SW:** (Software) Conjunto de programas que se instalan a las computadoras para que realicen funciones determinadas.

Declaración de políticas:

1.2.5.1. Los sistemas de comunicación de la Universidad generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la Universidad.

1.2.5.2. Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

1.2.5.3. La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Universidad y en tal sentido deben usarse las horas no laborables.

1.2.5.4. De manera consistente con prácticas generalmente aceptadas, la Universidad procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica, contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

1.2.5.5. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

1.2.5.6. Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

1.2.5.7. Los servidores de red y los equipos de comunicación (PBX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso

de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

1.2.5.8. Los empleados y funcionarios de la Universidad no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan.

1.2.5.9. Debe de existir una coordinación organizativa entre la comunicación de datos y la de voz (en caso de estar separados).

1.2.5.10. Deben de existir descripciones del puesto de trabajo, competencias, requerimientos y responsabilidades para el personal involucrado en las comunicaciones.

1.2.5.11. Establecer normas en comunicaciones (tipos de equipamiento, planes y procedimientos de autorización para la introducción de líneas y equipos, control físico de sniffers, etc).

1.2.5.12. Existir planes de comunicaciones a largo plazo, incluyendo estrategia de comunicaciones de voz y datos.

1.2.5.13. Planes de comunicaciones de alta velocidad, como FO, ATM, etc.

1.2.5.14. Planificar redes de cableado integral para cualquier nuevo edificio o dependencia que vayan a utilizar la universidad.

1.2.5.15. El plan de contingencia considera el respaldo y recuperación de los sistemas de comunicaciones.

1.2.5.16. Las listas de inventario cubren todo el equipamiento de comunicaciones de datos, incluyendo módems, controladores, terminales, líneas y equipos relacionados.

1.2.5.17. Mantener los diagramas de red que documentan las conexiones físicas y lógicas entre las comunicaciones y otros equipos de proceso de datos.

1.2.5.18. Reflejar en el registro inventario y en los diagramas de red, una muestra seleccionada de equipos de comunicaciones, de dentro y de fuera de los laboratorios.

1.2.5.19. Los procedimientos de cambio para equipos de comunicaciones, así como para añadir nuevos terminales o cambios en direcciones, deben

ser adecuados y consistentes con otros procedimientos de cambio en las operaciones de proceso de datos.

1.2.5.20. Establece ratios de rendimiento que cubren áreas como la de tiempos de respuesta en los terminales y tasas de errores.

1.2.5.21. Vigilar la seguridad dentro de los sistemas online y realizar los ajustes de acciones correctivas ante cualquier fallo de comunicaciones.

1.2.5.22. Los gestores de comunicaciones están informados y participan en la planificación pre-implementación de los nuevos sistemas de información que puedan tener impacto en las comunicaciones.

1.2.5.23. Las consideraciones de planificación de capacidad en comunicaciones son tomadas en cuenta en el diseño e implementación de nuevas aplicaciones.

1.2.5.24. Cada usuario solo debe de recibir en el menú lo que puede seleccionar realmente. Esto quiere decir que cualquier usuario tan solo debe poder acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

1.2.5.25. Los usuarios tendrán restricción de acceso según dominios, únicamente podrán cargar los programas autorizados y solo pondrán variar las configuraciones y componentes los técnicos autorizados.

1.2.5.26. Todos los SW instalados en los computadores deberán de ser actualizados constantemente.

1.2.5.27. El HW y SW de debe de estar estandarizado.

1.2.5.28. En las computadoras deberán de instalarse patches, service pack para la detección de los agujeros de seguridad. Se deberán de hacer actualizaciones de éstas

1.2.5.29. Instalación y configuración de Firewall.

1.2.5.30. Debe de existir un diseño general de las redes.

1.2.5.31. Establecer normas y procedimientos para la instalación de redes locales.

1.2.6 POLÍTICAS DE SEGURIDAD DE LA CONTINUIDAD DE LAS OPERACIONES

Objetivos:

- Implementar un plan de contingencia eficaz, que permita una rápida y eficiente toma de decisiones.
- Estandarizar y ampliar las políticas de seguridad.
- Fomentar en la comunidad universitaria el mejor aprovechamiento de las nuevas tecnologías de información y políticas de seguridad.
- Garantizar la divulgación, conocimiento y actualización de las políticas de seguridad.

Alcance:

Esta política se aplica a toda la comunidad universitaria.

Declaración de políticas:

1.2.6.1. Los docentes y estudiantes deben tener mas acceso a la tecnología de información e Internet, para lo cual se debe crear mas puntos de acceso, como apoyo a la docencia e investigaciones con los debidos controles de acceso.

1.2.6.2. Impulsar el avance y la cultura tecnológica en la universidad mediante seminarios, talleres y charlas, en las cuales se aborden temas técnicos y de seguridad.

1.2.6.3. Capacitar permanentemente en diversas modalidades y aplicaciones de seguridad a informáticos.

1.2.6.4. Actualizar permanentemente las políticas de seguridad de la UNAN-León.

1.2.6.5. Realizar simulaciones y pruebas periódicas de implementación de los planes de contingencia.

II. ASPECTOS LEGALES

La institución garantizara que docentes, estudiantes y trabajadores administrativos se rijan por las normas nacionales e internacionales para el uso de redes.

Se prestará especial atención a la seguridad, confidencialidad, derechos de autor sobre la información que se maneje a lo interno.

El software que se adquiera a partir de la fecha deberá tener licencia de uso.

III. RECOMENDACIONES

- Definir las responsabilidades de los involucrados en cada política.

- Definir las sanciones a realizar en caso de incumplimiento de alguna de las políticas por cualquier usuario de o responsable de la red. Estas puede ir desde llamado de atención verbal o por escrito hasta una sanción monetaria o despido de trabajador, dependiendo de la gravedad de la falta y sus consecuencias en el sistema.

- Garantizar el cumplimiento y normativas de cada uno de los sistemas que conforman la red de la Unan-León.

- Es importante que todos los usuarios de la red tengan acceso fácil a las reglas y políticas para que nadie puede decir que ellos no supieron de estas, hay que "Publicar las Políticas de seguridad" dentro de la institución.

- Monitorizar el cumplimiento de la política y revisarla y mejorarla cada vez que se detecte un problema.

3. Nuevo Diseño Lógico con Medidas de Control y Seguridad

Debido a la ausencia de un diseño general de la red, se creó un diseño idóneo para la red, con ayuda de herramientas de red como el Whats up, Visio y algunas herramientas de simulación y test.

Algunos aspectos importantes que tuvimos en cuenta para la realización de dicho diseño son:

- Seguridad de la información que viaja por la red así como la seguridad de la red misma (físicamente).
- Respaldo de la información.
- Prevención de problemas.

Topología De Red.

La topología para el diseño de la red es estrella, la red se une en un único punto, normalmente con un panel de control centralizado (en nuestro caso un core switch). Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. La ventaja al tener este esquema es que al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red aunque se caiga la comunicación entre uno de los puntos de conexión.

Componentes De La Red

Para una mejor compresión del diseño explicaremos éste, segmentándolo en 3 zonas:

- Barrier Segment
- Demilitarized Zone (DMZ)
- Zona LAN

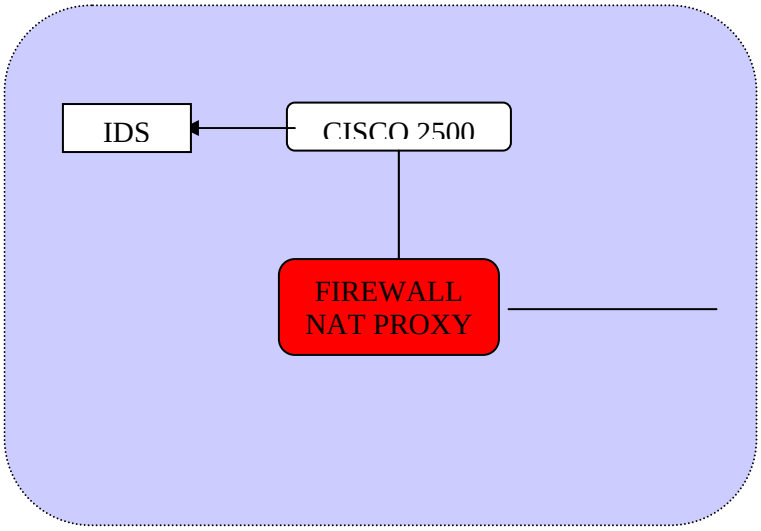
Estas tres zonas están conectadas entre si por un dispositivo que controla el filtrado de información, por lo tanto se convierte en un elemento crítico dentro del diseño, podríamos decir que es corazón de nuestra red. Otros elementos catalogados como críticos dentro del diseño son los servidores que se encuentran dentro de la Zona DMZ, ya que de estos dependen la disponibilidad de los servicios de Internet, así como también los servidores situados dentro de la zona LAN, de estos depende la funcionalidad de los sistemas de la Intranet. Si cualquiera de estos dispositivos se daña obstaculizaría el buen funcionamiento de del sistema.

Por último tenemos las líneas de comunicación dentro de estos elementos cítricos, quizás no en el mismo nivel de importancia que los anteriores debido a que las consecuencias en caso de fallos son menores (un segmento de la red). De estas líneas de comunicaciones (en algunos casos antenas de radio enlace) dependen la conexiones de las diferentes facultades y edificios de la universidad de modo que si una de ellas es dañada, quedaría aislado el segmento de red que conecta dicha línea.

Luego de determinar los puntos críticos que presenta el diseño hemos propuesto el respaldo de estos dispositivos de manera que estos garanticen la disponibilidad de todos los servicios de red.

Cada zona esta formada por una serie de dispositivos que veremos a continuación.

I. Zona Barrier Segment o Segmento de Barrera.



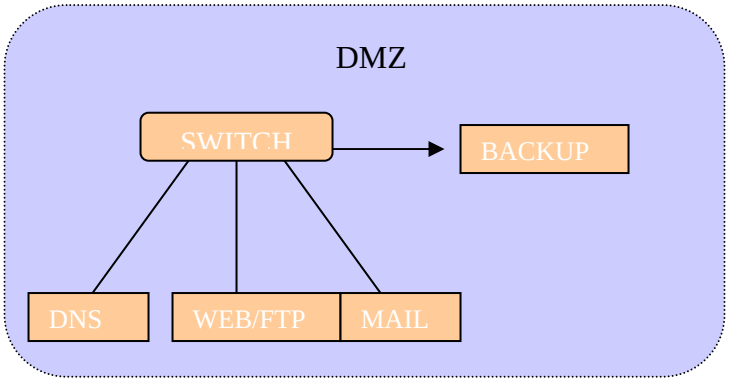
Dispositivos dentro del segmento de Barrera

- **IDS. Intruder Detection System.** Este puede ser una PC sencilla con LINUX.

- **Router.** Este dispositivo nos permitirá encaminar los paquetes de nuestra red hacia el exterior.

- **Firewall.** Un sistema básico de **Seguridad**, que debemos utilizar para nuestra conexión a Internet, es la instalación de de un cortafuego. Un Firewall es un sistema de defensa que se basa en la instalación de un barrera entre nuestra red e Internet. Con la instalación de un Firewall conseguiremos hacer nuestro sistema mucho menos vulnerable a intrusos.

II. ZONA DMZ



Dispositivos dentro de DMZ

- **Los servidores (Web, Mail, Ftp, DNS).** La zona DMZ es el área que se encuentra separada de la red interna en la que situaremos los servidores que deben ser visible desde Internet. Esta nos proporciona un punto adecuado para establecer medidas de control y seguridad, al control del tráfico entrante y saliente entre Internet y la red Interna.

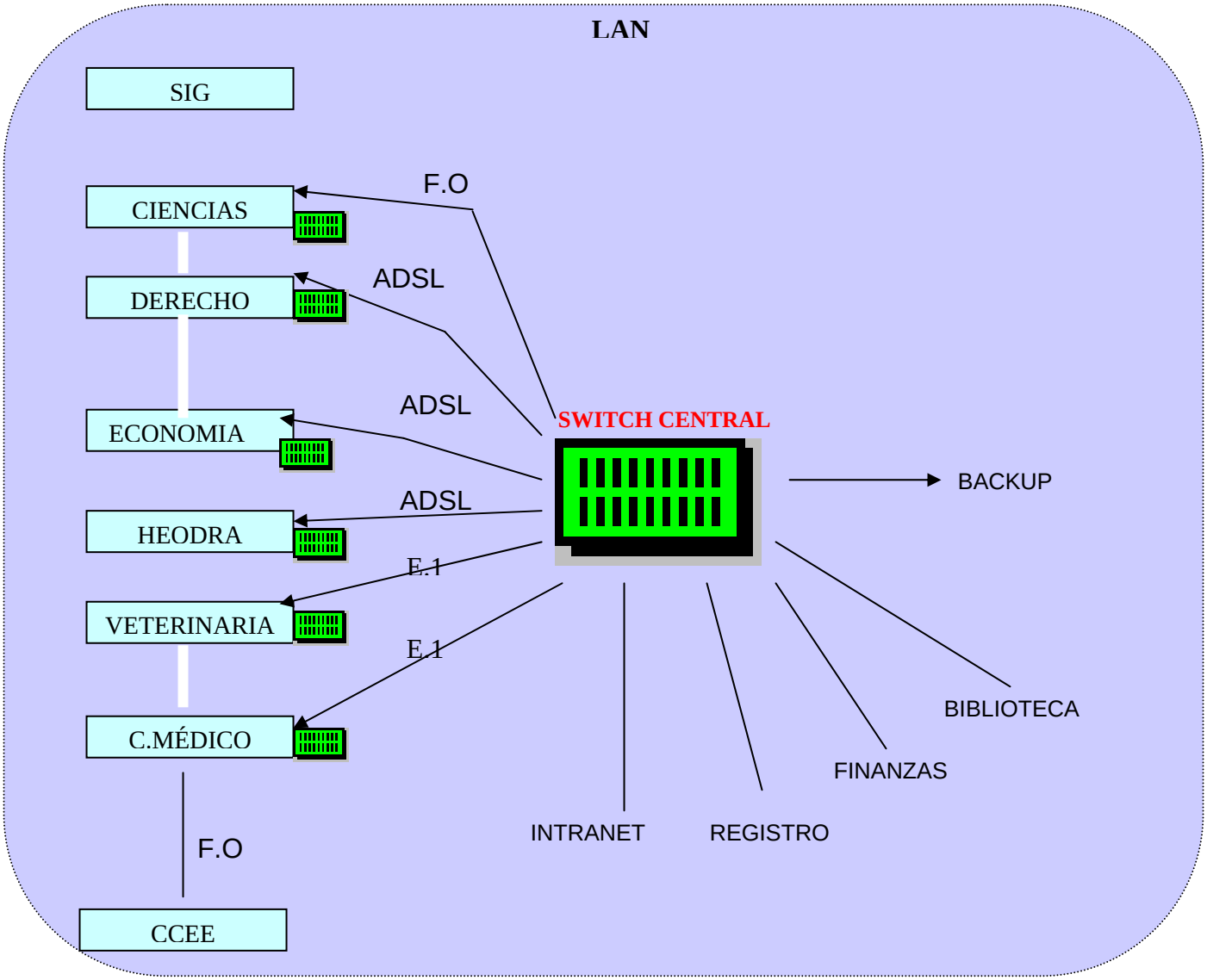
- **Backup (Respaldo de la información).** El Backup es uno de los dispositivos más importantes para cumplir con la **confiabilidad** que debe proporcionar la red. Un detalle importante que no se aprecia en el diseño es que este dispositivo si bien se encuentra conectado al mismo switch que los otros servidores, este no se encuentra situado físicamente en la misma oficina ya que en caso de algún problema con el lugar donde están los servidores el backup no se vera afectado y será quien nos responda.

- **DNS SECUNDARIO.** Este dispositivo nos resuelve un poco lo que es la parte de **Disponibilidad**, ya que al caer el servidor DNS queda de respaldo el DNS Secundario.

- **Log server y un log parser**

- **Servidor Antivirus**

III. ZONA LAN: Conformada por cada una de las LAN dentro de cada edificio. Como hemos dicho anteriormente la topología que utilizaremos para estas subredes será la Estrella.



Dispositivos dentro de las LANs:

- **Las PCs** (Estaciones de trabajo).
- **Core Data switch.** Un Conmutador de núcleo o switch manejable con alta capacidad de administración de red, filtrado de paquetes y filtrado de

  IP.(capa 2 y 3), soporte VLAN, flow control, soporte software de network manager. Se recomienda el switch 3 com 4900.

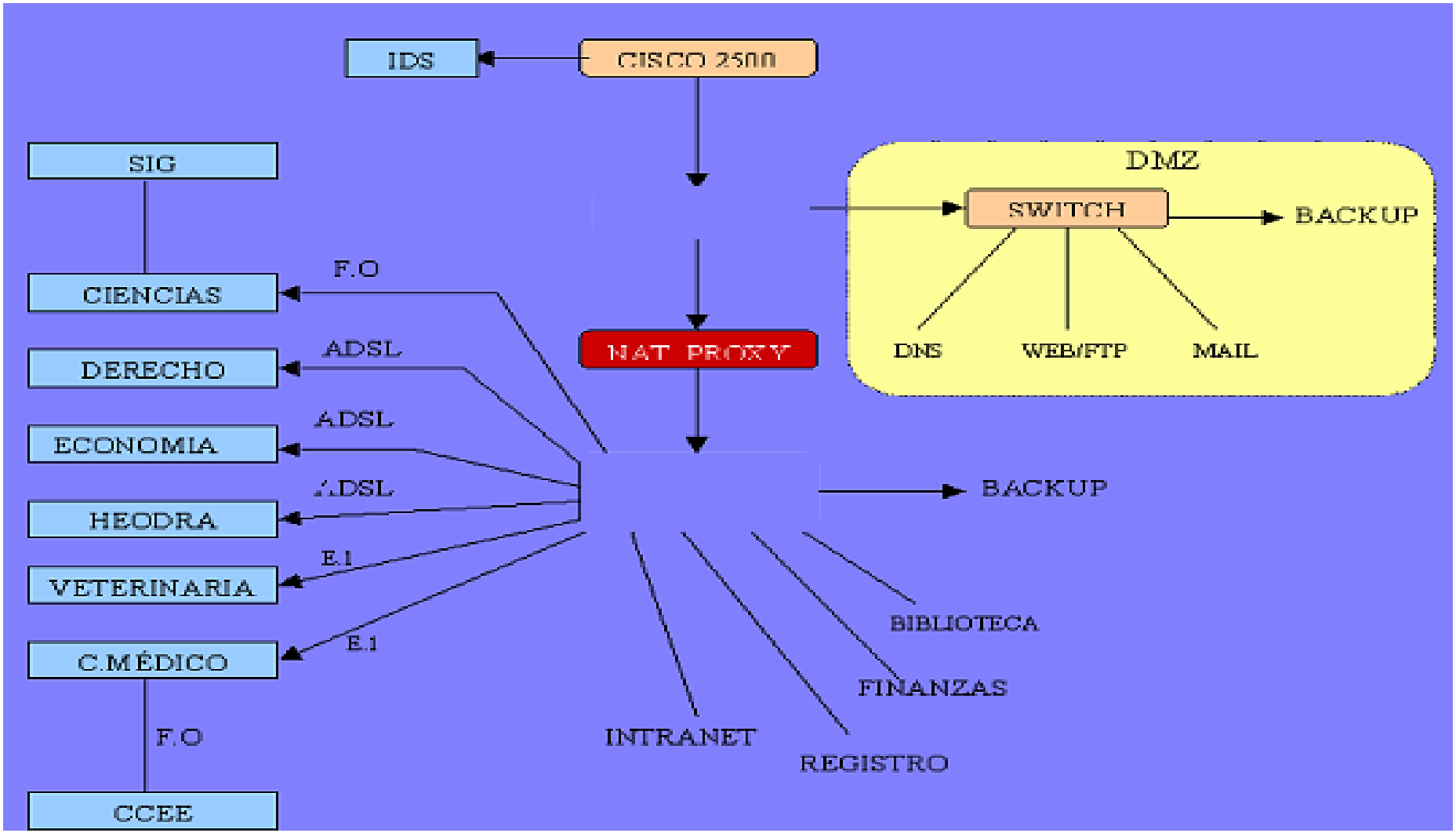
- **Switches manejables de menor capacidad** en cada uno de los campuses. (Interconectan dispositivos de la red).

- Servidores de Intranet, SOROLLA, Académico, Biblioteca, Recursos humanos, Backups.

- **Net traffic Monitor y log server.**

- **Redundancias de comunicaciones.**

"Nuevo Diseño Lógico de Seguridad de la UNAN-León"



4. Recomendaciones Para la Implementación del Nuevo Diseño Lógico

Para que este diseño tenga un nivel de rendimiento más alto y efectivo, presentamos algunas recomendaciones que se deben tener en cuenta dentro de los proyectos del departamento de informática, estas son:

a. **Números Privados sean Clase A:** Recomendamos la utilización de estos números para que exista una jerarquía muy bien definida y ordenada de tal forma que el numero IP de una maquina se suficiente para saber a que facultad y departamento pertenece.
   A cada facultad se le asignará un número que corresponde con el primer número decimal de la dirección IP este número identificara a cada facultad dentro de la red. De igual forma cada departamento tendrá asignado un número correspondiente al segundo decimal de la dirección IP. El resto serán los números de las PC de trabajo.
b. Instalar una especie de **Net Traffic Monitor y Log Server** para el control de eventos de la red.
c. **Respaldos:** En los puntos críticos que presenta el diseño estos son:
   Firewall, Core Switch, Servidores Internet (Zona DMZ) y servidores Intranet(zona LAN).
4. **Redundancia de comunicaciones:** La redundancia de comunicaciones que proponemos es entre los siguientes edificios: Ciencias-Derecho, Derecho-Economía, Veterinaria-Campus Medico. Esto permitirá mantener un respaldo en las comunicaciones, por ejemplo si las líneas telefónicas de la conexión HDSL que comunican a la Facultad de derecho con el edificio central se dañan, ésta utilizaría la línea que lo comunica con el edificio de Ciencias para la misma comunicación.

IV. IMPLEMENTACIÓN DE MEDIDAS Y TEST

Para que el modelo de seguridad sea efectivo implementaremos las contramedidas propuestas, tal como se expresó en la tabla de vulnerabilidades, amenazas y contramedidas del SI de la UNAN-León. Recomendamos el uso de algunas herramientas de seguridad.

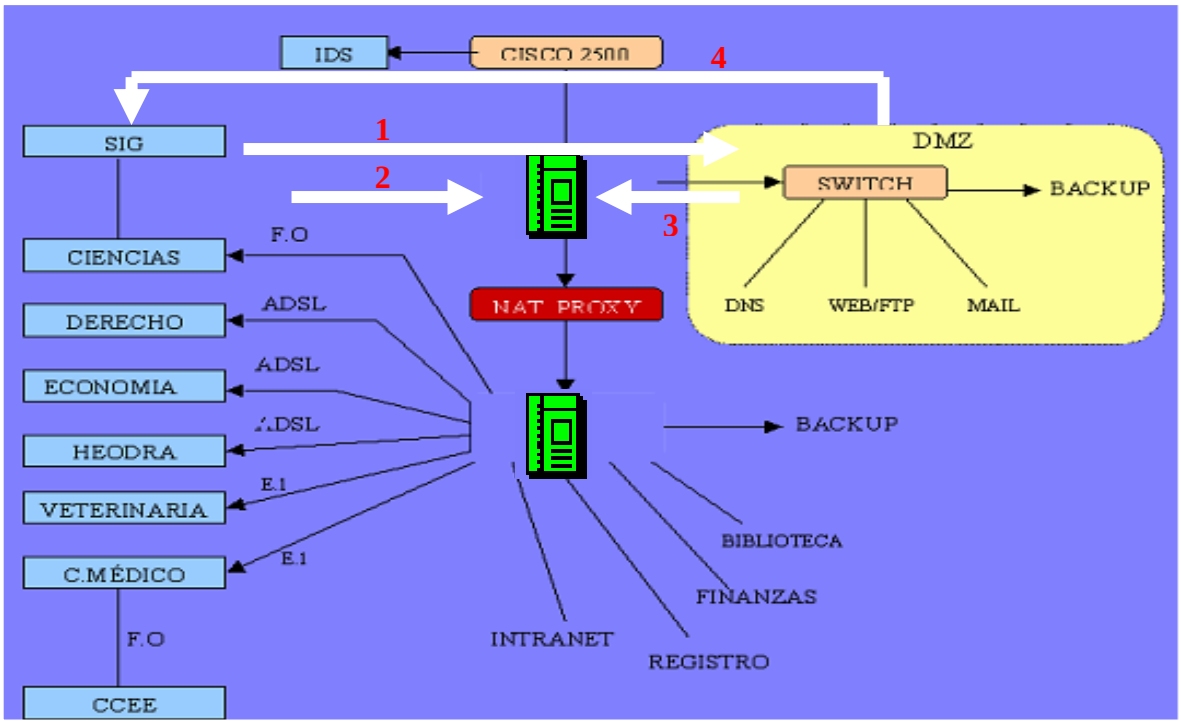
Además se recomienda la utilización de algunas de las técnicas de seguridad desarrolladas en el marco teórico: El Firewall es una de las mas importantes.

Configuramos un Firewall de filtrado de paquetes, el cual se encontrará en medio de nuestra LAN e Internet, filtrando todo el tráfico de la red.

Para configurar el Firewall se determinaron tres elementos principalmente:

1. **La directiva** con la cual trabaja, en nuestro caso la directiva elegida es la de "Denegar Todo de Forma Predeterminada y Permitir que Pasen Paquetes Seleccionados de Forma Explicita".
2. **El algoritmo** que utiliza el Firewall para trabajar, que es el siguiente:

3. Reglas del Firewall:



No.	Pass	Origen	Destino	Aplicación
1	Aceptar	LAN	DMZ	http / ftp, mail(POP3,SMTP)
2	Denegar	LAN	Firewall	
3	Denegar	DMZ	Firewall	
4	Aceptar	DMZ	LAN	http / ftp, DNS, mail(POP3,SMTP)
5	Drop	ANY	ANY	

Tabla 3.2. Reglas del Firewall

Ver Resultados en Anexos Nº 2 . "Configuración del Firewall"

CAPITULO V. RECOMENDACIONES Y CONCLUSIONES

I. RECOMENDACIONES.

II. CONCLUSIONES.

III. BIBLIOGRAFIA.

IV. ANEXOS.

I. RECOMENDACIONES

- Divulgación Actualización e Implementación de las Políticas de Seguridad.
- Implementación del Diseño Lógico de la Red.
- Implementación de las otras contramedidas propuestas en el Anexo Nº 2.
- Delegar un equipo de seguridad y auditoria informática cuya función sea asegurar el cumplimiento de dichas políticas.
- Elaborar un Plan de Contingencia.
- Capacitar y actualizar a los especialistas en tecnologías de la información y comunicación de la institución.
- Que todos los especialistas TIC de la institución lean el presente trabajo y vayan mejorando y/o actualizándolo.
- Invertir más en herramientas preventivas de seguridad.

II. CONCLUSIONES

Con la implementación del nuevo diseño del SI propuesto, las políticas de seguridad y las herramientas se garantiza una mayor confiabilidad en la red determinado por el modelo RASIS. Lográndose un mayor MTBF (Tiempo Medio Operacional) y un menor MTTR (Tiempo Medio de Recuperación).

La disponibilidad del modelo del SI propuesto será aproximadamente de un 99.7%.

Existen varios elementos para implementar una red segura, pero ninguno por si solo puede brindarnos la suficiente seguridad, sino que es la combinación de todos estos elementos junto con una acertada planeación de políticas de seguridad, unos requerimientos específicos y las características propias de la universidad, son los que podrían ayudarnos a definir una eficiente estrategia de seguridad sin que todo esto interrumpa las actividades de los usuarios.

III. BIBLIOGRAFIA

- Alexander H.
  "MÉTODOS Y MODELOS DE LA INVESTIGACIÓN"

- *V.I DMITRIEV*
  "TEORÍA DE LA INFORMACIÓN APLICADA"

- *Magnus Persson*
  "COMPUTER SECURITY ON A SHOESTRING BUDGET"
  Lund University Computing Center, Seminar 21 march 2002

- Shigeki Thsuchiya
  "SECURITY"

- *"INTERNET SECURITY FUNDAMENTALS "*
  Okinawa Internacional Centre.
  Japan Internacional Cooperation Agency.

- *"SECURITY DESIGN "*
  Okinawa Internacional Centre.
  Japan Internacional Cooperation Agency.

- *"NETWORK OPERATING SYSTEM SECURITY"*
  Okinawa Internacional Centre.
  Japan Internacional Cooperation Agency.

- *"REALIABILITY DESING"*
  Okinawa Internacional Centre.
  Japan Internacional Cooperation Agency.

- *"FIREWALLS"*
  Okinawa Internacional Centre.
  Japan Internacional Cooperation Agency.

- Robert L. Ziegler.
  "GUÍA AVANZADA FIREWALLS LINUX"
  PRENTICE HALL IBERIA, Madrid, 2000.

- Internet.

ANEXOS

1. Herramientas Utilizadas
2. Configuración del Firewall
3. Lista de otras Herramientas de Seguridad Sugeridas
4. Estándares Internacionales en Redes y Seguridad Informática

HERRAMIENTAS UTILIZADAS.

Estos programas fueron probados en las siguientes maquinas:

1. PC perteneciente a la red de la Unan-León, con el S.O Windows 2000.
2. PC Portátil conectada a la red de la Unan-León, con el S.O Windows XP.

ANT (Anvanced Net Tools) 2.7

GetAdmin

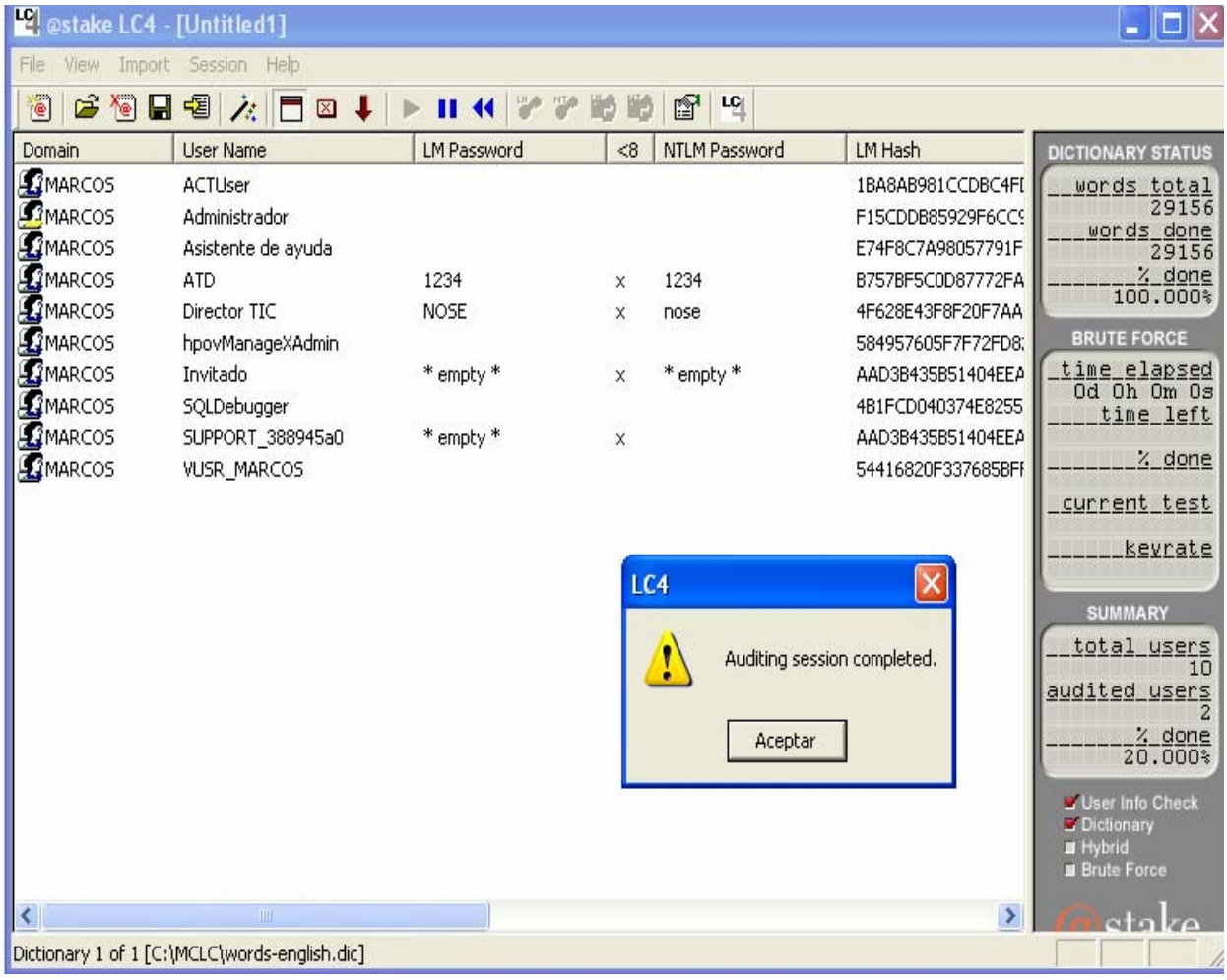
Esta es una herramienta Hackers que permite darles los derechos de administrador a la cuenta de cualquier usuario.

Este programa no se puede ejecutar si el Norton Antivirus esta tiene activada la autoprotección, ya que automáticamente detecta esta herramienta y no deja instalarlo en el PC, pero al desactivar la opción nos permite ejecutarlo.

Una vez iniciada la cuenta de usuario y deshabilitada la opción del Norton Antivirus, se ejecuta la herramienta desde A:\GetAdmin Cuenta_Usuario. Automáticamente se les concede los derechos de administrador a la cuenta de usuario.

LC4

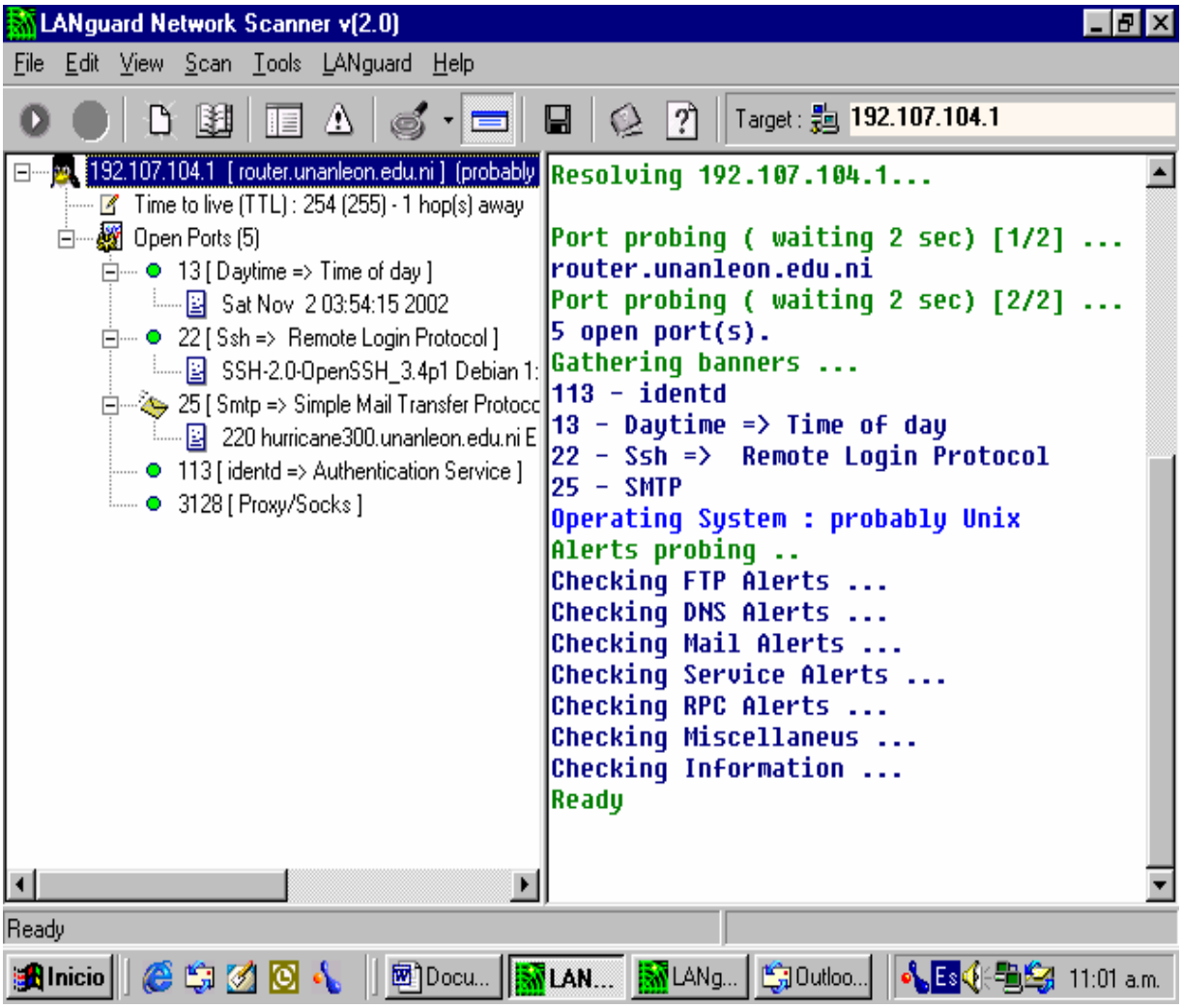
Esta es una herramienta Hackers para obtener las contraseñas que existen en nuestro PC, así como las de otros ordenadores de nuestra propia red como de otras redes remotas.



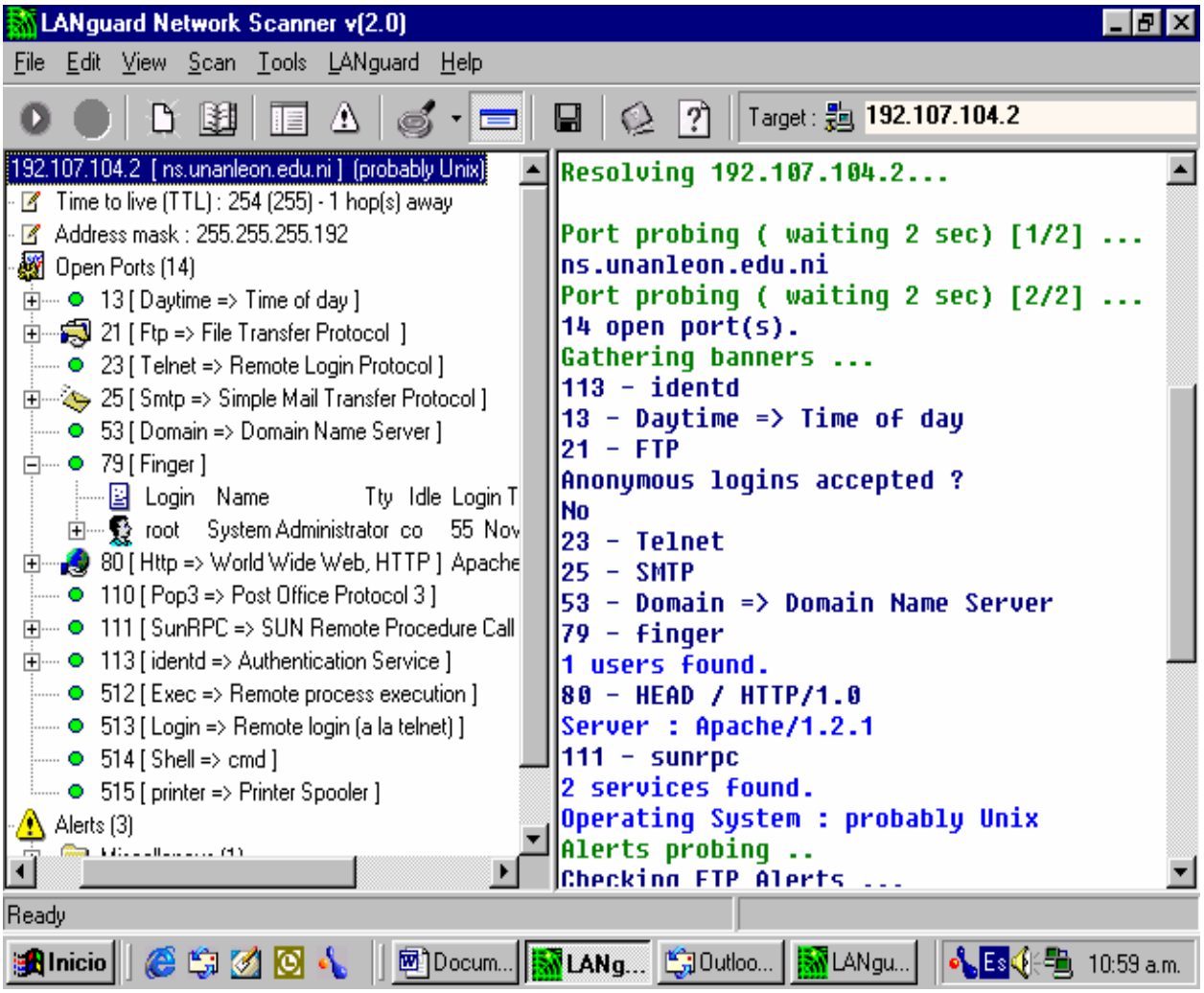
Languard Network Scanner V 2.0

Esta herramienta es muy importante para la seguridad de nuestra red, ya que con ella podemos detectar el número de puertos abiertos, además de la lista de los puertos abiertos, ya que para la seguridad de nuestra red es importante que solo estén abiertos como máximo 8 puertos y si esto no es así tenemos que proceder a cerrar los puertos que no son necesarios que estén abiertos.

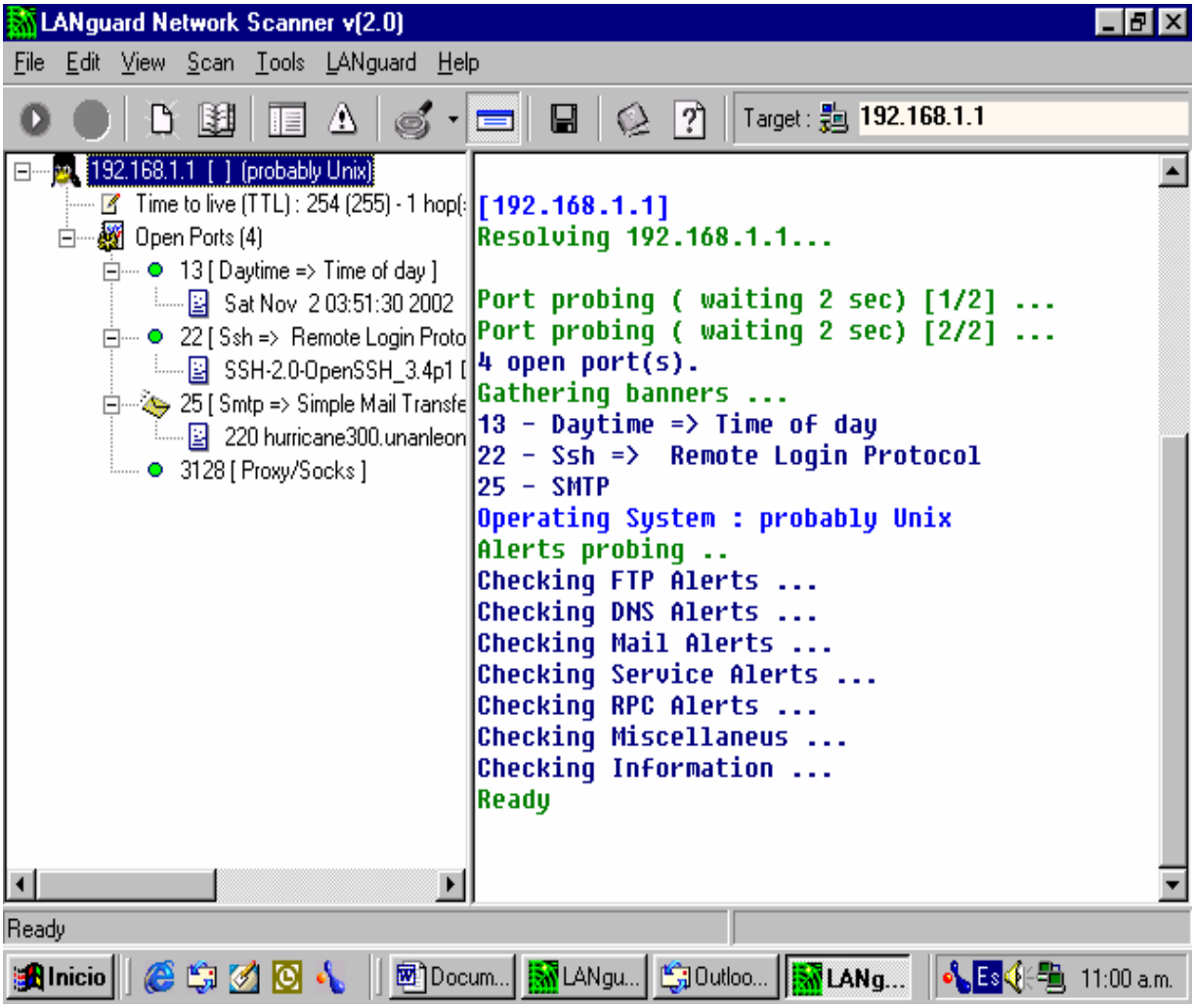
ROUTER 192.107.104.1



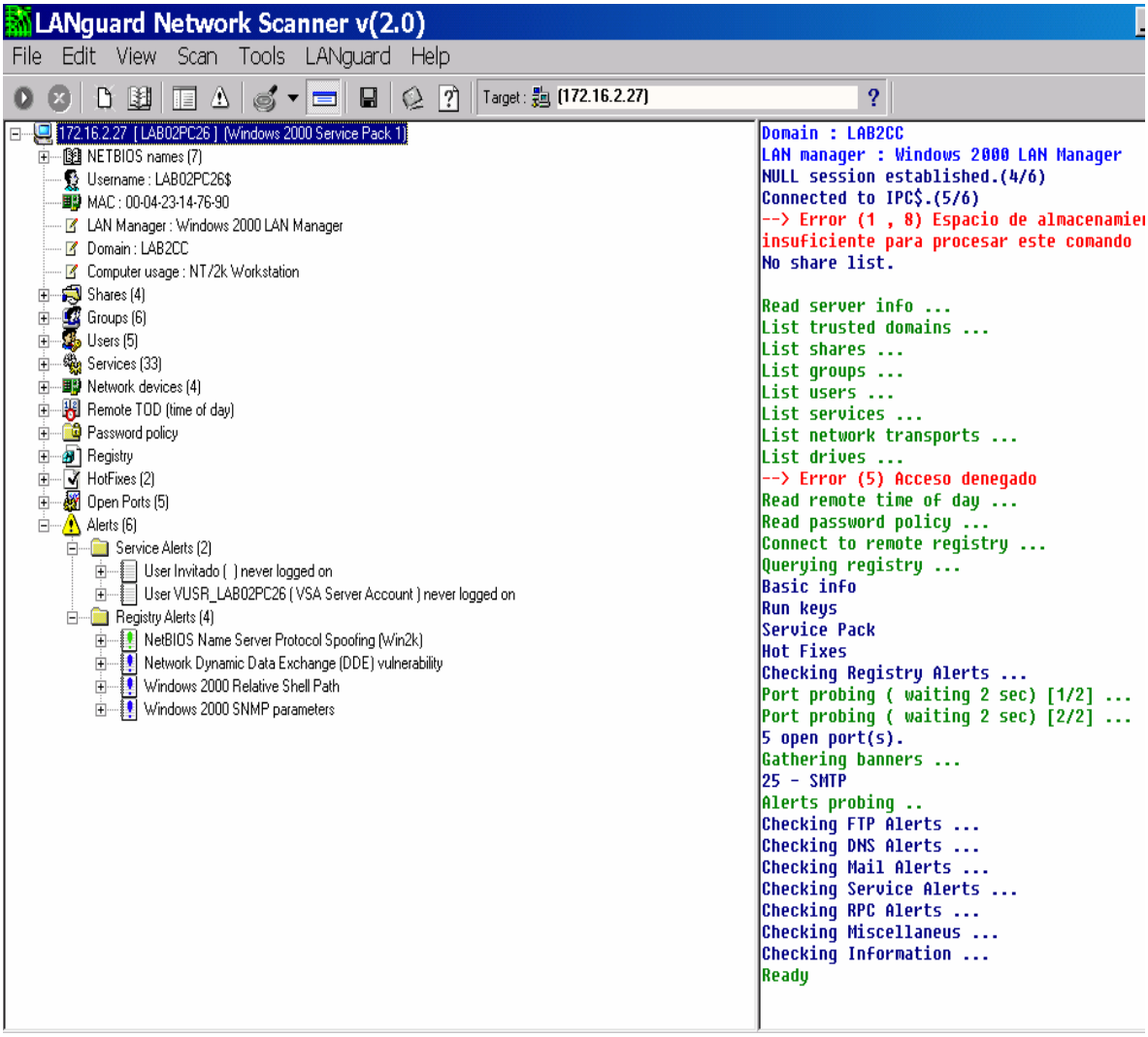
DNS 192.107.104.2



CIENCIAS 192.168.1.1



HOSTS 172.26.2.27



CONFIGURACIÓN DEL FIREWALL DE FILTRADO EN LINUX

1. Elementos Hardware:

1. Un Pentium III con 64 megas de memoria.
2. Un disco duro con dos 4.5 GB para almacenar todas las operaciones de registro.
3. Conexión a la red.

2. Elementos Software:

Software de filtración de paquetes incluido en el sistema Linux 8.0

Ventajas de configurar una maquina Linux como Firewall:

- Linux es un sistema operativo gratuito.
- La máquina donde correrá el Firewall necesita requerimientos mínimos: Podría ser un Pentium 133 con 32 megas de RAM, incluso con menos.
- Alta fiabilidad, ya que linux presenta gran calidad y estabilidad : muchas empresas están eligiendo opciones de este tipo.
- Sobre el sistema operativo Linux se puede montar múltiples servicios tales como:
    - Servidor Proxy HTTP y FTP con caché de disco para acelerar la navegación por Internet.
    - Informes generados en forma automática que permiten ver y evaluar el uso que se le esta dando a la Internet al interior de la universidad. Se podrá controlar por donde navegan los usuarios.
    - Bloqueo opcional para la navegación en mas de 30.000 sitios.
    - Conversión de las direcciones IP de su red privada (NAT)

3. Preparación del Sistema Linux para Trabajar con Firewall

Se instaló el SO Linux deshabilitando todos los servicios, instalando únicamente el Firewall y sus reglas por defecto. Luego realizamos la configuración de las tarjetas de red y el DHCP en base a la red con la cual se estaba trabajando. Finalmente se procedió con la creación de las reglas de filtración con la herramienta respectiva.

4. Esquema

Para nuestro trabajo seleccionamos el esquema siguiente:

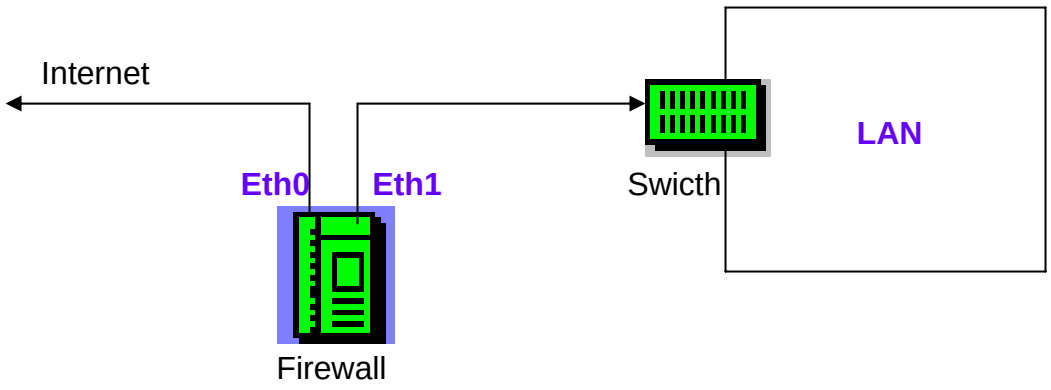
Un computador con dos tarjetas de red, una conectada a la red interna y la otra a Internet. De las cuales una estaba conectada a la red interna y a Internet:
Eth0: La interfaz externa, conectada a la red de Internet.
Eth1: La interfaz interna, conectada a la red local (LAN).

El equipo 192.107.104.3 representa en nuestro esquema un red publica. Al igual que todas las direcciones validas que se encuentran en Internet. Nuestra red interna trabaja con asignación dinámica de direcciones IP (DHCP).

Direcciones IP con que trabaja el Firewall:

Dirección pública asignada a la Eth0: 192.107.104.3
Dirección privada asignada a red local: 192.168.50.0
Dirección privada asignada a la Eth1: 192.168.50.1

El esquema es el siguiente:



5. Trabajo Realizado

1. Configuramos las tarjetas de red así:

Eth0: IP:192.107.104.3
Mascara de red: 255.255.255.0
Gateway: 192.107.104.1

Eth1: IP: 192.168.50.1
Mascara de red: 255.255.255.0
Gateway: 192.107.104.3

2. Configuramos las direcciones IP en el archivo dhcp.conf para que los paquetes se enrutarán siempre por nuestro Firewall.

```
subnet 192.168.50.0 netmask 255.255.255.0 {
range 192.168.0.3 192.168.0.255;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.50.255;
option routers 192.168.0.2;
option domain-name-servers 192.168.0.3,
option domain-name "chartermi.net";
}
```

3. Creamos las reglas de filtración con las cuales trabaja nuestro Firewall así:

El iptables trabaja con tres cadenas llamadas cadenas de Firewall : **INPUT:** Cuando llega un paquete, esta cadena decide si es malicioso o no. Si no lo es, entonces el kernel lo rutea, dependiendo de si su destino final es otra máquina (con lo que se activa la cadena de FORWARD)

FORWARD: Esta dedicada exclusivamente a enviar paquetes de una máquina hacia otra, o si es la máquina en sí misma. Si el paquete es considerado dañino, se realiza con él un DROP (paquete denegado), o un REJECT (paquete devuelto)

OUTPUT: Esta cadena es traspasada por cada paquete que desea salir al mundo exterior, o sea, otra máquina.

Algoritmo del Filtrado de Paquete (Firewall)

- Cuando llega un paquete el núcleo mira primero su destino: a esto se le llama encaminamiento (routing)
- Si está destinado a esa misma máquina, el paquete entra en el diagrama hacia la cadena INPUT. Si pasa de aquí, cualquier proceso que esté esperando por el paquete, lo recibirá
- En caso contrario, si el núcleo no tiene las capacidades de reenvío activadas, o no sabe hacia donde reenviar el paquete, se descarta el paquete. Si esta activado el reenvío, y el paquete esta destinado a otra interfaz de red, entonces el paquete pasa directamente a la cadena FORWARD de nuestro diagrama. Si es Aceptado, entonces saldrá de la máquina.
- Finalmente, si un programa que se ejecuta en la máquina puede enviar paquetes de red. Estos paquetes pasan por la cadena OUTPUT de forma inmediata: si los acepta (ACCEPT), entonces el paquete continúa hacia fuera, dirigido a la interfaz a la que estuviera destinada.

6. Creación de Reglas y Cadenas

#Interfaces
#eth0: interfaz pública (Red Externa) => 192.107.104.3
#eth1: interfaz privada (Red Interna) => 192.168.50.0/24

 # Activar reenvío de paquetes
echo 1 > /proc/sys/net/ipv4/ip_forward

#Instalar modulos necesarios
insmod ip_tables

#Borramos todo
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT
iptables -F POSTROUTING -t nat
iptables -F PREROUTING -t nat

#Politicas por defecto -> nada permitido
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

 # Activar la protección anti spoofing del núcleo
for x in lo eth0 eth1
do
        echo 1 > /proc/sys/net/ipv4/conf/${x}/rp_filter
done

#Permitir reenviar todo desde la Intranet hacia Internet
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

#Permitimos reenviar todo desde Internet hacia la Intranet
iptables -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

#NAT
#Traducción de dirección pública a direcciones privadas
iptables -A PREROUTING -t nat -i eth0 -j DNAT --to 192.168.50.1-192.168.50.254

#Traducción de direcciones privadas a dirección pública
iptables -A POSTROUTING -t nat -s 192.168.50.0/24 -o eth0 -j SNAT --to 192.107.104.3

#LOGs
iptables -A INPUT -j LOG --log-prefix "FILTER INPUT:"
iptables -A FORWARD -j LOG --log-prefix "FILTER FORWARD:"
iptables -A OUTPUT -j LOG --log-prefix "FILTER OUTPUT:"
iptables -A POSTROUTING -t nat -j LOG --log-prefix "SNAT:"
iptables -A PREROUTING -t nat -j LOG --log-prefix "DNAT:"

Si queremos denegar el paso de paquetes ICMP hacemos lo siguiente.

a) ping 192.168.50.1 (o sea, hacer un ping hacia nuestra dirección de red interna). Veremos como los paquetes de TCP/IP pasan con total libertad dentro de nuestra maquina.
b) Ahora, le decimos a la cadena de entrada (opción –A input), que los paquetes que vengan desde 192.168.50.0 (-s 192.168.50.0), y que se envíen a través del protocolo ICMP (-p ICMP), sean derivados en forma automática a un DROP (-j DROP)

    $ iptables -I INPUT -s 192.168.50.0/24 -p icmp -j DROP

c) Finalmente, intentemos nuevamente el ping, veremos que los paquetes no pasan a través de nuestra propia dirección interna.

El /24 significa en el modelo TCP/IP, sabemos que cada uno de los campos es una transformación de ocho cifras en binario, a una en decimal. Bien, lo que le especificamos a ipchains, es cuántas cifras debe tener en cuenta, y cuantas debe barrer de punta a punta...por eso, 3 x 8 = 24, con lo que los primeros tres octetos (192.9.200) se mantendrán intactos, barriendo todos los números del cuarto octeto (de 0 a 255).

Si queremos denegar el paso de paquetes ICMP desde un origen o destino hacemos lo siguiente:

a) Colocamos una estación de un lado del Firewall (será nuestro ejemplo de red publica) y del otro, otra estación (será nuestro caso de red privada).
b) Sabemos que la estación pública tiene la dirección 192.107.104.3, y que la privada tiene la dirección 192.168.50.2 la regla seria:

    $ iptables -I INPUT -s 192.107.104.3 -p icmp -j DROP

c) Intente hacer un ping desde la estación pública: $ ping 192.168.30.17

Notamos que la estación privada ya no es vista por la pública.

Si queremos denegar el servicio teniendo en cuenta el destino:

a) Si queremos denegar el acceso de la estación 192.168.50.2 a una pagina en particular, por ejemplo www.ciudadfutura.com , usamos los comandos -s o source (origen) en este caso la estación y -d destination (destino) , el protocolo que denegaremos es iso-ip (protocolo de pagina web: http) con -p.

$ iptables -I INPUT -s 192.168.50.2 -d www.ciudadfutura.com –p iso-ip -j DROP

Si queremos establecer reglas para un conjunto de estaciones o subredes hacemos lo siguiente:

Si por ejemplo las direcciones de las estaciones van desde la 192.168.30.2 hasta la 192.168.30.255

$ iptables -I INPUT -s 192.168.50.0/24 -d www.ciudadfutura.com -p iso-ip -j DROP

Y si queremos denegar algún servicio a un conjunto de estaciones exceptuando una, hacemos lo siguiente:

$ iptables -I INPUT -s !192.168.50.2 -d www.playboy.com –p iso-ip -j DROP.

Lista de Otras Herramientas de Seguridad Sugeridas

1. Red que Supervisa las Herramientas

    a. Argus
    b. Tcpdump
    c. swatch

2. Herramientas de Autentificación/Password

    a. Crack
    b. Passwords Sombra

3. Herramientas de Servicio-Filtrado

    a. Programa de capa TCP/IP

4. Herramientas para Examinar Hosts para Vulnerabilidades Conocidas

    a. ISS (Internet Security Scaner)
    b. SATAN (Security Administrator Tool for Analyzing Networks)

5. Herramientas Multi-Propósitos

    a. COPS(Computer Oracle and Password System)

6. Herramientas de Control de Integridad

    a. MD5
    b. Tripwire

7. Herramientas Complementarias

    a. lsof
    b. ifstatus
    c. smrsh

Nota

Asegure que el uso de la herramienta se adapte a las políticas y procedimientos de su organización.

1. Red que Supervisa las Herramientas

a. Argus

Argus es una red que supervisa la herramienta que utiliza un modelo cliente-servidor para capturar los datos y asociarlos en "transacciones." La herramienta proporciona la revisión del nivel de red; puede verificar la complacencia a un archivo de configuración de ruta, y la información puede ser fácilmente adaptada al análisis del protocolo, detecciones de intrusión, y a otras necesidades de seguridad. Argus está disponible en muchos sitios, incluyendo **ftp://ftp.andrew.cmu.edu/pub/argus /**

b. Swatch

Swatch, Simple WATCHer Program, es un fichero de registro filtro/monitor fácilmente configurable. Swatch supervisa archivos de registro y actúa para filtrar hacia afuera datos no deseados y tomar uno o más usuarios especificando acciones basadas en modelos del registro. Swatch está disponible: **ftp://ftp.stanford.edu/general/security-tools/swatch /**

2. Herramientas de Autentificación/Password

a. Crack

Crack es un programa libremente disponible diseñado para identificación, por el estándar que conjeturan las técnicas, UNIX DES encripta passwords que se pueden encontrar en diccionarios extensamente disponibles. Muchos administradores del sistema ejecutan el Crack como un sistema regular de procedimiento de administración y notifica a dueños de cuentas a quienes les han "crackeado" passwords. El Crack está disponible: **ftp://coast.cs.purdue.edu/pub/tools/unix/crack /**

b. Passwords Sombra

Si su sistema UNIX tiene una capacidad de password sombra, debería usarla. Bajo un sistema de password sombra, el archivo /etc/passwd no tiene passwords encriptados en el campo password. En cambio, los passwords encriptados se sostienen en un archivo sombra que no es mundialmente legible. Consulte sus manuales del sistema para determinar si una capacidad de password sombra está disponible en su sistema y para obtener los detalles de cómo levantarlo y manejarlo.

3. Herramientas de Servicio-Filtrado

a. Programa de capa TCP/IP

El programa de capa TCP/IP proporciona la información de registro de una red adicional y le da la habilidad a un administrador del sistema de negar o de permitir el acceso de ciertos sistemas o dominios al host en el que el programa esta instalado. La instalación de este software no requiere ninguna modificación en el software existente de la red. Este programa está disponible: **ftp://ftp.porcupine.org/pub/security**

4. Herramientas para Examinar Hosts para Vulnerabilidades Conocidas

a. ISS (Internet Security Scanner)

ISS es un programa que interrogará a todas las computadoras dentro de un rango específico de direcciones IP, determinando la postura de seguridad de cada una con respecto a varias vulnerabilidades comunes del sistema. ISS está disponible de muchos sitios, incluyendo: **ftp://coast.cs.purdue.edu/pub/tools/unix/iss**

b. SATAN (Security Administrator Tool for Analyzing Networks)

SATAN es una herramienta de prueba y reporte que colecciona una gran variedad de información sobre los hosts conectados a una red de computadoras. SATAN está disponible de muchos sitios, incluyendo: **ftp://ftp.porcupine.org/pub/security**

5. Herramientas Multi-Propósitos

a. COPS(Computer Oracle and Password System)

COPS son una colección de programas públicamente disponibles que procuran identificar problemas de seguridad en un sistema de UNIX. COPS no intentan corregir cualquier diferencia encontrada; él simplemente produce un informe de sus resultados. Los COPS están disponibles de: **ftp://coast.cs.purdue.edu/pub/tools/unix/cops**

6. Herramientas de Control de Integridad

a. MD5

MD5 es un programa de checksum criptográfico. MD5 toma como entrada un mensaje de longitud arbitraria y produce como salida una "huella digital" de 128 bits o un o "mensaje asimilado" de la entrada. Se piensa para ser computacional mente no factible para producir dos mensajes teniendo el mismo mensaje asimilado o para producir cualquier mensaje que tiene un objetivo específico dado en el mensaje asimilado. MD5 se encuentra en RFC 1321. Vea **ftp://coast.cs.purdue.edu/pub/tools/unix/md5**

b. Tripwire

Tripwire verifica la integridad de archivos y directorios; es una utilidad que compara un conjunto designado de archivos y directorios con la información almacenada en una base de datos previamente generada. Cualquier diferencia es señalada por medio de una bandera y se registra, incluyendo entradas agregadas o suprimidas. Cuando corre contra los archivos del sistema sobre una base regular, Tripwire le permite que descubra los cambios en los archivos del sistema críticos y toma inmediatamente medidas apropiadas de los daños. Tripwire está disponible de muchos sitios, incluyendo:

ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire /

7. Otras Herramientas

a. **lsof**

lsof lista los archivos abiertos y qué procesos de UNIX hacen que se abran. lsof está disponible: **ftp://vic.cc.purdue.edu/pub/tools/unix/lsof /**

b. **ifstatus**

El programa ifstatus puede correrse en los sistemas UNIX para identificar interfaces de red que estén en depuración o en modo promiscuo. Las interfaces de red en estos modos pueden ser una señal que un intruso está supervisando la red para robar passwords y otras estaciones. El programa no imprime ninguna salida (a menos que -v este dada) a menos que encuentra las interfaces en "malos" modos. Así que, es fácil correr el ifstatus del cron una vez por hora mas o menos. Si tiene un cron moderno que manda por correo el rendimiento de trabajos del cron a su propietario, utilice una linea como esta: 00 * * * * / el usr / local / el etc / el ifstatus. Si tiene una versión de cron que no hace esto, utilice el shell script "run-ifstatus" (revise el script para utilizar la ruta correcta para el comando): 00 * * * * / el usr / local / el etc / corra - el ifstatus. ifstatus está disponible en muchos sitios, incluyendo:

ftp://coast.cs.purdue.edu/pub/tools/unix/ifstatus /

c. **Smrsh**

Con todas las versiones de sendmail, nosotros recomendamos que usted utilice el programa shell restringido de sendmail, smrsh, creado por Eric Allman (el autor original de sendmail). Cuando está configurado correctamente, el programa smrsh puede ayudar a proteger contra una vulnerabilidad que pueda permitir que los usuarios remotos o locales desautorizados ejecuten programas como cualquier usuario del sistema con excepción de raíz. Por ejemplo, el smrsh puede evitar que un intruso use los tubos (|) para ejecutar comandos arbitrarios en su sistema. El smrsh está disponible de muchos sitios, incluyendo: **http://www.sendmail.org/**

Advertencia: Si se está ejecutando una versión vieja del sendmail tal vez usted deba instalar el smrsh por separado, los intrusos continuarán pudiendo explotar las vulnerabilidades que fueron fijadas en versiones posteriores de sendmail. Se sugiere que se actualice la versión del correo del sendmail y después ejecute las herramientas, que se incluyen con la distribución.

ESTÁNDARES INTERNACIONALES EN SEGURIDAD INFORMÁTICA

Normas	
Código	**Título**
NOM-019-SCFI-1994	Norma Oficial Mexicana relativa a seguridad de equipo de procesamiento de datos.
FIPS 180-1	Estándar de conmistión segura
FIPS 186	Estándar de firma digital
FIPS 191	Directrices para el análisis de redes de área local (LAN)
FIPS 31	Directrices para la seguridad física y gestión del riesgo en el procesado automático de datos
FIPS 81	Estándar de encriptación de datos (DES) - Modos de operación
IEEE 802.10B	Estándares de seguridad en redes locales - Seguridad en el Intercambio de datos
ISO/IEC 10164-7	Gestión de sistemas OSI. Parte 7: Función de alarma de seguridad
ISO/IEC 10164-9	Gestión de sistemas, Parte 9: Objetos y atributos para control de acceso
ISO/IEC 9596-1	Protocolo de gestión común de información (CMIP)
ISO/IEC 9804	Definición de elementos de servicios de Recuperación, Concurrencia y Compromiso (CCR)
ISO 11577	Protocolo de seguridad de nivel de red (NLSP)
ISO 9594-8	El directorio: Procedimiento de autenticación
ISO SC27/WG2 N294	Firma digital con apéndice - Parte 1 : General
SSL	Secure Sockets Layer

NOM-019-SCFI-1994

Ámbito: Seguridad

Establece los requisitos de seguridad que deben cumplir los equipos integrados de procesamiento de datos de fabricación nacional e importados, o sus partes en forma individual. Aplica a distintos tipos de equipo tales como: máquinas electrónicas de procesamiento de datos, microcomputadoras, sistemas personales, computadoras de uso personal y servidores, y periféricos asociados a los equipos antes mencionados. Excluye equipos de procesamiento de datos que son altamente especializados y que no son comerciables directamente al público en general.

FIPS 180-1

Ámbito:

SERVICIOS DE SEGURIDAD
Integridad
Técnicas de integridad de datos

Este estándar especifica un algoritmo de conmistión segura (SHA) que puede usarse para generar una representación comprimida de un mensaje, llamada recopilación del mensaje. Se requiere SHA siempre que se use el algoritmo de firma digital (DSA), especificado en el estándar de firma digital (DSS), y siempre que se requiera un algoritmo de conmistión segura para aplicaciones federales. Cuando se utiliza este algoritmo, tanto el receptor como el emisor, han de usarlo en el procesado y verificado de un mensaje. Su uso se encuentra muy extendido ya que todas agencias y los departamentos federales estadounidenses han de utilizarlo en el intercambio de información.

FIPS 186

Ámbito:

SERVICIOS DE SEGURIDAD
Integridad

Esta publicación define el algoritmo de firma digital (DSA) para la creación y verificación de firmas digitales. Cuando se recibe un mensaje, el receptor debe verificar que éste no se ha modificado desde que fue emitido, además querrá estar seguro de la identidad del emisor. Para ello el receptor puede usar de prueba una firma escrita por la signatura digital o una tercera parte del mensaje consignada por el emisor. Las firmas digitales pueden también crearse para datos

almacenados y programas de manera que la integridad de los mismos pueda ser verificada en cualquier instante posterior. En suma, da el criterio requerido para las claves públicas o privadas.

El uso de esta norma es obligatorio en las comunicaciones de datos desclasificados para las agencias y departamentos federales estadounidenses. Su uso por compañías y organizaciones privadas está recomendado por el NIST.

FIPS 191

Ámbito:

SERVICIOS DE SEGURIDAD
Seguridad en la gestión del sistema
Gestión de riesgos de seguridad

Estas directrices versan sobre amenazas y vulnerabilidades y consideran servicios de seguridad técnicos y mecanismos de seguridad. El uso de la gestión de riesgos se presenta para ayudar al lector a determinar los activos de la red de área local (LAN), para identificar amenazas y vulnerabilidades, para determinar el peligro de esas amenazas para la red y para determinar los servicios de seguridad y mecanismos que deben de usarse para reducir los riesgos de la red de área local. Se trata de un conjunto de directrices que no son de obligado cumplimiento, pero sí recomendables para reducir riesgos en las comunicaciones.

FIPS 31

Ámbito

SERVICIOS DE SEGURIDAD
Seguridad en la gestión del sistema
Gestión de riesgos de seguridad

Provee de un conjunto de directrices para el desarrollo de seguridad física y de programas de gestión de riesgos en el procesado automático de datos. Este estándar puede usarse como guía para planificar y evaluar la seguridad de los sistemas informáticos. Es de obligado cumplimiento en las agencias y departamentos federales.

FIPS 81

Ámbito:

SERVICIOS DE SEGURIDAD
Confidencialidad
Seguridad de datos encriptados

El estándar de encriptado de datos federales (DES) (FIPS 46) especifica un algoritmo criptográfico que es usado para la protección de datos informáticos desclasificados, pero sensibles. Este estándar lo complementa, definiendo cuatro modos de operación para el DES que pueden usarse en distintos tipos de aplicaciones. Los modos especifican como deben de ser encriptados los datos (protección criptográfica) y desencriptados (regreso al estado original). Los modos incluidos en este estándar son el modo de código electrónico, modo de encadenado de bloques de cifras, modo de realimentación de cifras y modo de realimentación de salida. La selección de uno u otro modo, dependerá de la aplicación particular de que se trate. Este estándar se usa en todas las agencias y departamentos federales estadounidenses y el NIST recomienda su uso a organizaciones y compañías privadas.

IEEE 802.10B

Ámbito:

SERVICIOS DE SEGURIDAD

Control de acceso

Control de acceso en redes

Esta norma desarrolla todos los aspectos relativos a los sistemas de seguridad en redes de Área local (LAN). Define un protocolo para la seguridad en el intercambio de datos.

ISO 10164-7

Ámbito:

SERVICIOS DE SEGURIDAD
Arquitecturas y aplicaciones de seguridad
Seguridad de sistemas operativos

Esta norma, define la función de alarma de seguridad. Es esta una función de gestión del sistema que debe de ser usada como una aplicación de proceso en un entorno de gestión descentralizado o centralizado, para intercambiar información con el propósito de gestionar el sistema tal y como define la norma ISO 7498-4.

Los sucesos relacionados con la seguridad son de relevancia, ya que cuando uno de ellos ocurre, el sistema de seguridad determina las acciones que deben llevarse a cabo. Este sistema especifica, por ejemplo, que debe crearse una función de alarma de seguridad, que se registre el suceso en una pista de verificación de seguridad, que aumente el contador, que se ignore el suceso o se lleve a cabo unas combinación de todas estas acciones.

Además, este estándar:

- Establece los requisitos del usuario para la función de alarma.
- Define el servicio que realiza la función de seguridad.
- Especifica el protocolo necesario para utilizar esta función.
- Define la relación entre el servicio y las notificaciones de gestión.
- Define las relaciones con otras funciones de gestión.
- Especifica los requisitos de conformidad.

ISO 10164-9

Ámbito

SERVICIOS DE SEGURIDAD
Control de acceso
Control de acceso de sistemas

Describe un modelo de seguridad en el control de acceso, y la información de gestión necesaria para crear y administrar el control de acceso en los sistemas OSI. Es aplicable a la gestión de seguridad de muchos tipos de aplicaciones.

ISO 9596-1

Ámbito:

SERVICIOS DE SEGURIDAD
Seguridad en la gestión del sistema
Gestión de riesgos de seguridad

Esta norma describe el protocolo que utilizan los niveles del sistema para intercambiar información de gestión. Especifica los procesos de transmisión de

información de gestión, las reglas de codificación de la gestión común de información y los procesos para la correcta interpretación de la información de control del protocolo.

ISO 9804

Ámbito:

SERVICIOS DE SEGURIDAD

Arquitecturas y aplicaciones de Seguridad

Seguridad de bases de datos

Establece los principios generales para el uso coordinado de los servicios CCR cuando mas de dos aplicaciones están envueltas en una misma acción simple o cuando se requiere recuperación después de un error. Define los servicios que se usan en una asociación sencilla para coordinar dos aplicaciones implicadas en una misma acción.

ISO 9979

Ámbito:

SERVICIOS DE SEGURIDAD

Confidencialidad

Registro de técnicas criptográficas

Procedimientos para el registro de algoritmos criptográficos

Especifica los procedimientos y la forma, del registro de entrada. Esta norma, tiene dos anexos, uno de los cuales (el anexo B) es puramente informativo (no normativo).

ISO 11577

Ámbito:

SERVICIOS DE SEGURIDAD

Confidencialidad

Este estándar especifica un protocolo para uso en sistemas intermedias y finales, que provee de servicios de seguridad a la capa de red (definidos en ISO 8348 e ISO 8648). Este protocolo no es otro que el protocolo de seguridad de niveles de red (NLSP).

Especifica:

1. Los siguientes servicios definidos en ISO 7498-2:
   - Autenticación de origen de datos
   - Control de acceso
   - Confidencialidad de la conexión y la desconexión
   - Integridad de la conexión y la desconexión
2. Los requisitos funcionales para implementaciones que sigan este estándar.

Los procedimientos de este protocolo están definidos en términos de :

- requisitos de las técnicas criptográficas que pueden usarse en una circunstancia de este protocolo.
- requisitos de la información transportada en la asociación de seguridad usada en un caso de comunicación.

Aunque el grado de protección ofrecido por algunos mecanismos de seguridad depende del uso de algunas técnicas criptográficas específicas, el uso correcto de este protocolo no depende de la elección de ningún algoritmo particular de cifrado y descifrado.

ISO 9594-8 Idéntica a ITU-T X.509

Ámbito:

SERVICIOS DE SEGURIDAD

Autenticación

La norma 9594 especifica como obtiene el directorio la información de autenticación y como obtener del mismo esos datos. Expone, así mismo, las

suposiciones que hay que hacer sobre como se forma y aloja la información de autenticación en el directorio. Define tres caminos en los que las aplicaciones deben usar esta información para realizar la autenticación y describe como otros servicios de seguridad, deben de ser sostenidos por la autenticación.

Describe dos niveles de autenticación; la autenticación simple que usa una contraseña como verificación de la identidad y la autenticación fuerte que implica credenciales y usa técnicas criptográficas. Mientras la autenticación simple ofrece una protección limitada contra accesos no autorizados, solo la autenticación fuerte debería usarse como base para un servicio seguro.

En la norma, se especifica la forma de autenticación de la información que tiene el directorio, describiendo como obtener del mismo los datos necesarios. Incluye además un ejemplo de algoritmo criptográfico de autenticación, así como de función conmistión (con una introducción a este tipo de funciones.

La autenticación sólo se proporciona en el contexto de un sistema definido de seguridad, por lo que debe de ser el usuario de una aplicación determinada el que ha de establecer dentro del estándar su propio sistema de seguridad. El protocolo usado por las aplicaciones para obtener credenciales del directorio es el protocolo de acceso al directorio definido en ISO 9594-5.

ISO 10118-1

Especifica las funciones conmistión y es por tanto aplicable a los servicios de provisión de autenticación, integridad y no repudio. Contiene definiciones, símbolos, abreviaturas, y requisitos comunes para todos ellos.

ISO 10164-9, ITU-T X.741

Describe un modelo de seguridad en el control de acceso, y la información de gestión necesaria para crear y administrar el control de acceso en los sistemas OSI. Es aplicable a la gestión de seguridad de muchos tipos de aplicaciones.

ISO 10181- (1-8)

Se desarrollan en esta norma todas las estructuras de seguridad en un entorno de sistemas abiertos, entendiendo como tales, no solo la interconexión de sistemas abiertos (OSI), sino también áreas como bases de datos , aplicaciones y procesos distribuidos. Se especifican estructuras para la autenticación, el control de acceso, no repudio, sistemas confidenciales, servicios integrados, alarmas y verificación y manejo de claves.

La estructura de seguridad, concierne a la provisión de seguridad de sistemas, objetos del sistema, y de la interacción entre ellos, no a la metodología de construcción del sistema y mecanismos. La estructura de seguridad, dirección a los elementos de datos y secuencias de operaciones que se usan para obtener servicios de seguridad específicos.

ISO 11586-1

Este estándar define una serie de posibilidades genéricas para asistir en la provisión de servicios de seguridad en los niveles superiores.

Esto incluye:

- Un conjunto de herramientas para sostener la especificación de los requisitos de protección selectiva de campo y para proveer la especificación de seguridad y de intercambios de seguridad.
- Una definición de servicio y especificación de protocolo para dotar de servicios de seguridad a la capa de aplicación de OSI.
- Una especificación para la sintaxis de transferencia de seguridad asociada con el soporte de la capa de presentación para servicios de seguridad en la capa de aplicación.

Define:

- Modelos generales de funciones de seguridad en el protocolo de intercambio y transformaciones de seguridad, basada en los conceptos descritos en el modelo de seguridad de capas superiores OSI (ISO/IEC 10745).
- Un conjunto de directrices informativas para la aplicación de posibilidades de seguridad de las capas superiores genéricas reguladas por este estándar

ISO 13594

Esta norma describe los aspectos relativos a la seguridad de los niveles inferiores en el modelo de referencia OSI (de interconexión de sistemas abiertos). Desarrolla los conceptos estructurales comunes a estos niveles, las bases para la interacción relativa a la seguridad entre ellos y los protocolos de ubicación.

ISO 17799

La estructura de la normativa de gestión en seguridad de sistemas / información, ISO 17799, queda especificada en 10 elementos. Los mismos incluyen:

1. Planificación en Continuidad de la Empresa

Contrarrestar interrupciones a las actividades de la empresa y sus procesos de los efectos creados por un desastre o falla de sistema(s) de comunicación / informática.

2. Control de Acceso a Sistema

(1) Control de acceso a la información, (2) Prevenir acceso sin autorización (intrusión) a sistemas de información, (3) Asegurar la protección de los servicios de red, (4) Prevenir acceso sin autorización a computadores y redes, (5) Detectar actividades no autorizadas (intrusión al sistema), y (6) Igualmente asegurar proteger la información cuando esta en uso móvil y telecomunicación (en línea por acceso externo).

3. Desarrollo y Mantenimiento de Sistema

(1) La seguridad sea parte integral del sistema de las gestiones en la organización, (2) Durante uso/acceso a información prevenir perdida, modificación o mal uso de la misma y datos, (3) Proteger la confidencia, autenticidad e integridad de la información, (4) Asegurar proyectos de informática y actividades de soporte se realicen de manera segura, (5) Mantener la seguridad de las aplicaciones y plataforma operativa en el uso de datos, información y "software".

4. Seguridad de Ambiente y Física

Prevenir acceso no autorizado, daño o interferencia a las premisas y por ende a la información. Prevenir daño y perdida de información, equipos y bienes tal que no afecten las actividades adversamente. Prevenir extracción de información (robo) y mantener la integridad de la información y sus premisas donde se procesa información.

5. Conformidad / Cumplimiento

(1) Prevenir brechas de seguridad por actos criminales o violación de ley civil, regulatoria, obligaciones contractuales u otros aspectos de impacto a la seguridad, (2) Asegurar un sistema (de gestión) cumpliendo con políticas de seguridad y normativas (ISO 17799, ISO 9001 y otras, también considerar guías ISO 13335 o ISO 15408), (3) Optimizar la efectividad con el proceso de verificar / auditar el sistema.

- ISO 13335 - Guías para Administración de Seguridad (de Información)
- ISO 15408 - Criterio para Seguridad (Informática)

6. Seguridad del Personal

Reducir el riesgo de errores inadvertidos, robo, fraude o mal uso de la información. Mediante conocimiento y prácticas, asegurar que los usuarios conocen de las amenazas y las inquietudes en materia de seguridad de sistema, y los mismos están apoyados por políticas para seguridad efectiva. Las políticas y su aplicación son para asegurar reducir incidentes de seguridad y funcionamiento inadecuado.

7. Seguridad de la Organización/Empresa

(1) Administrar la información de forma efectivamente segura, (2) Mantener seguridad de bienes y de las actividades en el procesado de información y sus premisas cuando accesan otras partes (externos, contratistas), (3) Mantener la integridad de la información cuando se utilicen servicios externos (de apoyo y extensión de servicios).

8. Administración de Sistemas y Redes

(1) Asegurar premisas y operaciones efectivas a la seguridad durante uso y retención de la información, (2) Minimizar las probabilidades de fallas en sistema ("Hardware"), (3) Proteger la integridad del "software" y la información que esta retiene, (4) Mantener integridad y disponibilidad de información en las redes y su comunicación, (5) Asegurar salvaguardar información en red y la protección de su *infraestructura*, (6) Prevenir daños a los bienes (inmoviles y otros) + el potencial de interrupciones a las actividades de la organización, (7) Prevenir perdida, modificación o mal uso de información cuando la misma se comunica entre organizaciones (clientes, proveedores, *infraestructura*).

9. Control y Clasificación de Bienes

Mantener protección apropiada de los bienes de la empresa, asegurando que la información reciba un nivel de protección apropiado (a la naturaleza de las actividades).

10. Política de Seguridad

Proveer dirección y apoyo por la seguridad de información.