ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

"POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD PARA OPTIMIZAR LA OPERATIVIDAD DE LOS SISTEMAS DE REDES UNIVERSITARIAS ECUATORIANAS CONECTADAS AL INTERNET"

Autor: María Elena Vallejo Samaniego

Tutor: Patricio Moreno MsC.

Tesis previo a la obtención del Grado de Master en

INFORMÁTICA EDUCATIVA

Riobamba - Ecuador

2004

AGRADECIMIENTO

A la Escuela Superior Politécnica de Chimborazo, al personal Docente por compartir sus conocimientos durante el desarrollo de la Maestría, que me ha permitido mejorar mis conocimientos en el área de la informática.

Mi profundo agradecimiento al Ing. M.Sc. Patricio Moreno, Director de la Tesis, por su preocupación, orientación y guía en el desarrollo y culminación de este trabajo.

A todas las personas que con sus palabras de aliento hicieron posible el éxito de la investigación.

María Elena

Dedicatoria

A Dios por estar presente en mi vida.

A mis hijos: Giovanna Elena, Silvana Patricia y Patricio Xavier

A mi esposo: por la paciencia y la ayuda permanente que me ha brindado en la culminación de este trabajo

A mi padre por siempre inculcar en todos sus hijos el amor al estudio.

RESUMEN

La presente investigación busca optimizar la operatividad de los sistemas de redes Universitarias Ecuatorianas que se encuentran conectadas al Internet y que están ubicadas en las provincias de Bolívar, Chimborazo, Cotopaxi, Guayas, Pichincha y Tungurahua a través de políticas y procedimientos de seguridad que se ajusten a su realidad.

El grupo de Universidades y Escuelas Politécnicas en las que se lleva adelante la investigación está formado por 25 instituciones distribuidas por provincias de la siguiente manera: una en Bolívar, dos en Chimborazo, una en Cotopaxi, ocho en Guayas, once en Pichincha y dos en Tungurahua, en las que se recolecta la información a través de encuestas, entrevistas y sesiones de trabajo; con esta información se procede a hacer el análisis de las seguridades que se han implementado en las mismas.

Del análisis realizado en las Universidades y Escuelas Politécnicas se determinó los problemas que en ellas existen debido a la falta de políticas y procedimientos de seguridad y que están afectando a la operatividad de sus redes. La propuesta que se plantea en esta tesis busca dar solución a los problemas encontrados a través de políticas de seguridad; a nivel físico en lo referente al control de acceso al sitio, el lugar de trabajo y ubicación de equipos, el control del personal que trabaja en los centros de cómputo y laboratorios, la protección de los datos en los medios de almacenamiento; a nivel lógico relacionado con los respaldos de los datos, las cuentas y contraseñas, la detección de cambios que se producen en la información, la manera de utilizar las bitácoras para mantener segura la red de intrusos, las políticas a seguir para ofrecer servicios de red seguros, las políticas que permitirán que los firewalls cumplan eficientemente su función y los procedimientos de seguridad que están sistematizados para las páginas Web que poseen las universidades y los sistemas operativos que son utilizados en ellas

SUMMARY

The present investigation looks for to optimize the operability of the systems of Ecuadorian University nets that they are connected to the Internet and that they are located in the counties of Bolivar, Chimborazo, Cotopaxi, Guayas, Pichincha and Tungurahua through political and procedures of security that are adjusted to its reality.

The group of Universities and Polytechnic Schools in those that it is taken the investigation ahead are formed by 25 institutions distributed by counties in the following way: one in Bolívar, two in Chimborazo, one in Cotopaxi, eight in Guayas, eleven in Pichincha and two in Tungurahua, in those that the information is gathered through surveys, interviews and work sessions; with this information you proceeds to make the analysis of the securities that have been implemented in the same ones.

Of the analysis carried out in the Universities and Polytechnic Schools it was determined the problems that exist due to the lack of political in them and procedures of security and that they are affecting to the operability of their nets. The proposal that she thinks about in this thesis she looks for to give solution to the opposing problems through political of security; at physical level regarding the access control to the place, the work place and location of teams, the personnel's control that works in the computation centers and laboratories, the protection of the data in the storage means; to logical level related with the backs of the data, the bills and countersigns, the detection of changes that they take place in the information, the way to use the binnacles to maintain sure the net of intruders, the politicians to continue to offer sure net services, the politicians that will allow that the firewalls completes their function and the procedures of security that are systematized for the pages Web that possess the universities and the operative systems that are used in them efficiently

INDICE

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCION

En las Universidades y Escuelas Politécnicas del Ecuador no se ha dado la debida importancia al dictado de políticas y procedimientos de seguridad lo que ha provocado una deficiente administración de las redes universitarias tanto en el aspecto físico como lógico del manejo de la red interna como de la conexión hacia el Internet.

Los usuarios de las redes universitarias se han venido manejando a su libre albedrío o con recomendaciones que se han originado para tratar de contrarrestar problemas que han ido surgiendo en determinados lugares de la red, las cuales se han transmitido de forma verbal y no están explícitas en un documento que permita el conocimiento por parte de todos los usuarios.

A nivel administrativo tampoco existen políticas de seguridad escritas en la mayoría de las Universidades investigadas, a las cuales deban acogerse los diferente administradores de la red y que sean comunes para enfrentar los problemas que pueden afectar a una subred, como a la red total.

En esta investigación se trata un tema de gran interés a nivel mundial en lo relacionado a las políticas y procedimientos de seguridad para las redes con un enfoque hacia las Universidades y Escuelas Politécnicas del Ecuador, buscando disminuir la incidencia de pérdidas, daños físicos de los medios de transmisión, equipos y dispositivos de las redes; así como ataques lógicos contra los servidores, dispositivos activos o el mal uso de las redes universitarias para el ataque a otras redes conectadas al Internet.

Las políticas y procedimientos de seguridad planteadas en la propuesta están redactadas para las Universidades y Escuelas Politécnicas en las cuales se realizó la investigación y que se pudo determinar a través del análisis que tienen situaciones de falta de seguridad comunes.

La redacción del documento está expuesta a través de cuatro capítulos. En el primer capítulo Seguridad en Internet se presenta un marco teórico que se utiliza de referencia para interpretar los resultados del estudio. El segundo capítulo contempla la metodología utilizada en el desarrollo de la tesis. El capítulo tres Análisis de las Seguridades Implementadas en las Universidades y Escuelas Politécnicas, presenta el análisis de los datos recopilados durante la investigación y la demostración de la validez de la hipótesis. En el capítulo cuatro está la Propuesta de Políticas y Procedimientos de Seguridad para las Redes de la Universidades Ecuatorianas.

JUSTIFICACION

La seguridad es crítica para el uso de Internet, sobretodo en el caso de las universidades que lo utilizan para exponer sus ofertas académicas, investigaciones, publicaciones de proyectos, ingreso mediante password y login a información académica, evaluaciones, administración de servidores y dispositivos de red o como forma de trabajo que ha convertidos a autoridades, estudiantes, profesores y personal administrativo dependientes de esta tecnología.

En Internet hay más de 30 mil sitios orientados a hackers con toda una variedad de herramientas para llevar a cabo ataques electrónicos a las redes de información conectadas al Internet entre las que se encuentran las redes de las Universidades y Escuelas Politécnicas del Ecuador. Las pérdidas por baja seguridad se reflejan en capital tangible e intangible y pueden llegar a ser multimillonarias.

Los virus se multiplican y fortalecen cada día más, se enfilan contra los datos e integridad de las Universidades públicas y privadas. Se transmiten principalmente vía Internet, siendo el correo electrónico su transporte preferido, pero con frecuencia llegan a través de disquetes infectados que traen los usuarios de las redes universitarias.

Los ataques internos son, según los expertos en seguridad, los de mayor frecuencia, los que generalmente se materializan en robos de información o daños a los datos de las Universidades y Escuelas Politécnicas. Las maneras pueden ser desde uso ilegal de claves para acceder a información confidencial hasta tentativas de borrar la información almacenada en los discos duros o servidores.

En lo referente a los ataques externos entran en juego los hackers, cuya mal ganada fama creó un nuevo verbo para el léxico informático: hackear. Estos se especializan en romper la seguridad electrónica de las redes universitarias o de cualquier otra red conectada al Internet, con propósitos

que incluyen desde robos de información, cambios de parámetros de los procesos, transacciones fraudulentas, etc.

Cada sitio tiene necesidades diferentes, la seguridad que requiere una empresa es diferente de la seguridad que requiere una Institución educativa como son las Universidades y Escuelas Politécnicas, por lo cual sus metas se vuelven particulares, por tanto los planes de seguridad deben estar acorde con las necesidades y cultura del lugar.

Muchos sistemas en las Universidades Ecuatorianas se encuentran en oficinas y laboratorios, a menudo manejados por su propio personal, que en la mayoría de los casos ponen poco interés en la seguridad, pues consideran que el mismo es proporcional a su percepción de lo que es el riesgo y amenazas.

Existen sistemas Universitarios que están conectados al Internet y a través de este alrededor del mundo, por lo que alguien podría conseguir ingresar desde cualquier red que sea parte del Internet y robar contraseñas en medio de la noche cuando los edificios universitarios están cerrados con llaves, y luego utilizar las mismas para provocar daños en archivos o en el sistema como un todo.

El Internet ha permitido el robo electrónico a través de ventanas o puertas abiertas en los sistemas y con mucho del software de monitoreo desarrollado en la actualidad una persona puede verificar cientos de máquinas en pocas horas y determinar su vulnerabilidad. Entre los sistemas más apetecidos para los ataques están los de las Universidades, porque no tienen altas seguridades y se convierten en medios de prueba para ataques posteriores a sistemas más seguros.

En realidad la complejidad de las soluciones para tener redes seguras universitarias está directamente relacionada con los niveles de riesgo, por lo que estas deben basarse en sistemas de protección contra ataques externos e internos. Además se debe identificar los puntos débiles de la red y a partir de un informe de vulnerabilidad crear políticas y procedimientos de seguridad.

PROBLEMA

¿La falta de utilización de políticas y procedimientos de seguridad afecta la operatividad de los sistemas de redes universitarias que se encuentran conectadas al Internet?.

OBJETIVOS

OBJETIVO GENERAL

Crear políticas y procedimientos de seguridad para la universidad ecuatoriana.

OBJETIVOS ESPECIFICOS

- Determinar niveles de protección y por tanto de soluciones de seguridad
- Analizar los servicios de Internet que presta la universidad y cuales deben prestar en función de los condicionantes de seguridad y economía
- Planificar estrategias de seguridad
- Definir las políticas y procedimientos de seguridad
- Analizar las tendencias de amenazas y ataques

FORMULACION DE HIPOTESIS

La operatividad no óptima de los sistemas de redes universitarias conectadas al Internet es debido a la falta de políticas y procedimientos de seguridad.

OPERACIONALIZACION DE LAS VARIABLES

HIPOTESIS	**VARIABLES**	***DIMENSION***	**INDICADORES**	SUBINDICES	ITEMS
La operatividad no óptima de los sistemas de redes universitarias conectadas al Internet es debido a la falta de políticas y procedimientos de seguridad.	**Variable independiente** Políticas y procedimientos de seguridad	Seguridad Física	Control de acceso	Servicio de vigilancia Formularios de datos personales Credenciales de identificación Mediante algo que saben (password) Sistema biométrico Verificación automática de firmas Control de ingreso de vehículos	¿Cómo realiza el control de acceso de personas? ¿Se realiza control de acceso de vehículos?
			Ergometría	Pantallas antirreflejo Iluminación	**¿Utiliza pantallas antireflejo?** ¿La iluminación es la adecuada?
			Tipos de desastres	Temperatura ambiental Extinguidores Rociadores automáticos de agua Material de las paredes Tipo de piso instalado Protección contra inundaciones Instalaciones eléctricas Calefacción Ventilación Aire acondicionado	**Ambiente físico del centro de cómputo** ¿Utiliza alguno (s) de los sistemas?

			Acciones Hostiles	Barreras infrarrojas Microondas Ultrasonido Detectores de aberturas Detectores de roturas de vidrios Detectores de vibraciones Circuito cerrado de televisión	¿Qué tipo de protección electrónica utiliza?
				CPU Cableado Impresoras Cintas Diskettes CD-ROM HUB Switch Routers	¿Cuál es la protección que ofrece a sus dispositivos?
		Seguridades Lógicas	Controles de acceso	Sistema operativo Aplicaciones Utilitarios	**La protección que ofrece al software**
			Niveles de seguridad informática	Bases de datos Documentos Archivos Virus	**¿Protección que ofrece a los datos?** ¿Medidas que tiene implementadas para proteger el software? ¿Emplea algún estándar de seguridad informática? ¿Para evitar el ingreso de virus desde el Internet a su red utiliza algunas políticas?
		Delitos informáticos	La información y el delito Delincuente y víctima	Ataques del exterior Ataques del interior	¿De donde considera que puede venir un ataque? ¿Ha experimentado algún tipo de ataque?

		Amenazas humanas	Personal interno y externo a la red	Recuperación de recursos	¿En caso de emergencia que posibilidad existe de recuperar los recursos perdidos o dañados? ¿Tiene algunos pasos que se deben seguir para defenderse de ataques?
		Administración	Monitoreo Normas Tecnologías de sistemas de seguridad Soporte técnico	Detección de extraños	¿Realiza monitoreo para detectar a extraños que buscan obtener información que está siendo transmitida?
				Análisis de las bitácoras Monitorización de las conexiones Sistemas de análisis Sistemas de criptografía Suma de verificación	¿Métodos que utiliza para la protección de la red de intrusos?
				Test de penetración Trampas de red Pruebas	¿Cómo disuade el uso no autorizado de sus sistemas y servicios de red? ¿Realiza ataques simulados en los sistemas de producción real?
				Personal Técnico	¿Tiene un equipo de respuesta a incidentes?
				Plan de contingencia	¿Posee un plan de recuperación de desastres?
			Recursos	Inversión en seguridad	¿Gasto de la universidad en seguridad informática?
			Fungibles	Materiales fungibles	¿Control y protección de materiales fungibles?
			Usuarios	Permisos de acceso a: Internet Servicios (ftp, telnet)	¿Se ha definido la lista de los usuarios que tienen permisos de acceso?
	Variable dependiente	Hardware	Medios de transmisión	Normas de cableado	¿Está hecho el cableado bajo alguna norma?

	La operatividad no óptima de los sistemas de redes universitarias conectadas al Internet		Topologías de red Tipo de conectividad	Enlace al internet Ancho de banda	¿Qué tecnología usa para el enlace al Internet? ¿Cuánto es el ancho de banda del enlace al Internet? ¿Qué tecnología utiliza en su red interna? ¿Cuál es la velocidad a la que trabaja su red interna?
		Software	Protocolos de comunicación	Net Bios TCP/IP IPX-SPX	¿Qué protocolos utiliza?
			Seguridad y protección	Software de seguridad Medidas de protección	¿Utilización de software de seguridad? ¿Medidas para proteger el software?
			Sistemas operativos	Windows Linux Unix Novell	¿Qué sistemas operativos utiliza?
			Respaldos	Sistemas operativos Información de los usuarios	¿Realiza respaldos? ¿Cada que tiempo verifica su integridad? ¿Lugar físico donde realiza el almacenamiento?
			Firewall	Producto comercial Producto gratuito	¿Emplea firewall?

		Servicios de red	Servicios de acceso remoto Servicios de Internet	Gopher Wais News Archie WWW e-mail Telnet FTP IRC USENET Finger Whois	¿Que servicios de Internet ofrece su universidad? ¿La identificación que posee el usuario le permite acceder a todas las aplicaciones y datos a los que su perfil le permite?

CAPITULO I

SEGURIDAD EN INTERNET

1. SEGURIDAD EN INTERNET

1.1 SEGURIDAD INFORMATICA

Los conceptos iniciales de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). La Biblia, los relatos de Homero, Ciserón, son libros en los que aparecen rasgos referentes a la seguridad en la guerra y el gobierno. La arqueología nos muestra pruebas de seguridad en la antigüedad al observar los descubrimientos hechos en la pirámides egipcias, el templo de Karnak en el valle del Nilo.

Los incas utilizaban los quipus para llevar el correo de forma segura de un lugar a otro, transportado por los chasquis y el cual a su llegada era interpretado por los quipucamayos.

Al definir el objetivo de la seguridad se habla de salvaguardar las propiedades y personas contra el robo, las inundaciones, el fuego, poder contrarrestar los disturbios sociales que puedan poner en peligro el progreso de un país, en definitiva buscar la paz y tranquilidad de la gente.

En la actualidad la seguridad está en manos del poder legislativo quienes promulgan las leyes en la que deciden la valoración de los delitos y el correspondiente castigo.

Si se dirige hacia el ámbito técnico la seguridad está a cargo de los administradores de las redes y de los usuarios de las computadoras .

La llegada de las redes informáticas incrementó los riesgos de robo, de modificaciones no autorizadas y daños flagrantes a los datos. La computadora personal cambió todo lo existente en los grandes sistemas y minicomputadoras las que podían abrirse o cerrarse completamente y eran por

tanto muy seguras. Una computadora hoy en día conectada a una red es una vía potencial de conflictos.

Como va el desarrollo en la actualidad en el campo de la informática y de las comunicaciones cada día más computadoras estarán formando parte de la red, sea esta privada o pública como en el caso del Internet. Al tener acceso a Internet desde una red privada o el acceso de personas mediante una extranet se está añadiendo una gran cantidad de puertas a través de las cuales pueden entrar datos espurios y salir datos confidenciales.

Todo el mundo tiene en la actualidad un profundo respeto con los riesgos asociados con Internet, que algunos denominan el paraíso de los hackers, pero las redes internas son vulnerables también por quienes trabajan con ellas de forma autorizada.

La seguridad de un red interna se relaciona con la verificación de los usuarios, de la restricción del acceso a datos siempre que sea necesario y el cifrado de comunicaciones confidenciales para impedir su interceptación.

1.1.1 Clases de seguridad informática

La información siendo intangible puede clasificarse en pública la cual esta al alcance de todas las personas y privada aquella que debe ser visualizada por quien la generó o un grupo de personas que trabaja con ella.

La seguridad informática involucra datos, hardware y usuarios; en ella se deben tener en cuenta ciertos parámetros, como los indicados en la tabla 1.1.

Tabla 1.1 Parámetros de la seguridad informática

PARAMETROS	CARACTERISTICAS
Confidencialidad	Proteger la información para que nadie pueda leerla o copiarla, sin la respectiva autorización de su dueño
Integridad	Proteger la información para evitar se borre o altere sin el permiso del propietario de la misma.
Disponibilidad	Proteger los servicios para que no se degraden o dejen de estar disponibles sin la respectiva autorización
Consistencia	Asegurar que el hardware y software se comporte como lo espera el usuario autorizado.
Control	Reglamentar la forma de acceder al sistema
Auditoría	Determinar qué se hizo, quién lo hizo y que fue afectado

1.2 POLITICAS DE SEGURIDAD

Mediante las políticas se define que se considera valioso y se especifica las medidas a tomar para proteger esos activos (figura 1.1), deben ser generales y no variar mucho a lo largo del tiempo.

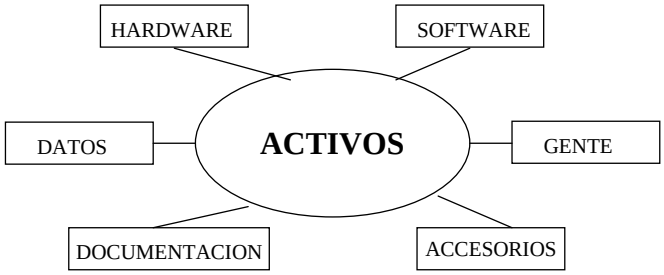


Figura 1.1 Activos a proteger

Las políticas pueden escribirse de algunas maneras :

- Políticas sencillas y generales que en unas cuantas páginas cubran gran cantidad de posibilidades.
- Políticas para diversos activos
- Políticas pequeñas y sencillas, complementadas por estándares y recomendaciones sobre el comportamiento.

Las políticas juegan tres papeles principales:

1) Aclarar que se está protegiendo y por qué
2) Establecer la responsabilidad de la protección
3) Poner las bases para resolver e interpretar conflictos posteriores

Mediante los estándares se codifican las prácticas exitosas de seguridad en una organización, son redactados generalmente en términos de "*es obligatorio*", implican una métrica que permite determinar si se han cumplido; son un apoyo para las políticas y cambian lentamente en el tiempo.

Las recomendaciones son redactadas en términos de "*debería*" , busca interpretar los estándares en el contexto de un cierto entorno sea éste de programas o físico. Estas se pueden violar si resulta necesario pues solo constituyen guías para el comportamiento.

1.3 SEGURIDAD FISICA

La seguridad física en muchas de las universidades es olvidada, dando importancia casi siempre a la parte lógica de los equipos informáticos.

1.3.1 Desastres

Las computadoras y dispositivos activos requieren que las conexiones físicas y el entorno tengan un balance para evitar fallas de manera inesperada y nada deseables por lo que es necesario tener presente las consideraciones de la tabla 1.2.

Tabla 1.2 Entorno que puede afectar a las computadoras

ASPECTOS A CONSIDERAR	DESCRIPCION
Incendio	Las computadoras no resisten el fuego, así éste no las alcance, porque el excesivo calor se encargará de derretir el disco duro y las soldaduras, o el agua utilizada para sofocarlo las destruirá. En la actualidad se esta utilizando el bióxido de carbono comúnmente, pero en lugares donde existen computadoras que pueden salir ilesas cuando son expuestas el agua se sugiere rociadores de agua.
Agua	El peligro principal con el agua es que provoca cortocircuitos, generalmente ésta proviene en los centros de cómputo; de la lluvia, inundaciones, bebidas (refrescos, café, etc.)

Humo	El humo actúa como abrasivo y se adhiere a las cabezas de los discos magnéticos, discos ópticos, unidades de cinta, causan fallas en los teclados.
Polvo	El polvo es abrasivo y destruye lentamente las cabezas de los discos magnéticos, las unidades ópticas y las unidades de cinta, puede provocar cortocircuito en los elementos activos.
Terremotos	En los últimos años en el Ecuador no se han dado fuertes movimientos sísmicos, por lo cual las construcciones no respetan severas normas de seguridad respecto a la resistencia contra terremotos, sin embargo se debe estar preparado para ellos ya que nos encontramos en zona de alto riesgo.
Temperatura	Las computadoras funcionan dentro de márgenes de temperaturas que son consideradas por los fabricantes como las adecuadas para evitar daños
Explosiones	Pueden ser causadas por el mal uso de sustancias químicas inflamables almacenadas en el edificio
Bichos	Estos animales a veces se introducen en las computadoras provocando daños en sus componentes
Rayos	Estas descargas eléctricas de la naturaleza provocan altas variaciones de voltaje que dañan los equipos incluso cuando están protegidos
Humedad	Las computadoras requieren de pequeñas cantidades de humedad para su buen funcionamiento, pues evita el almacenamiento de cargas estáticas; pero si ésta se encuentra en demasía puede provocar condensaciones en los circuitos de las computadoras causando cortocircuito.

1.3.2 ERGOMETRIA

La interacción del ser humano con la computadora ha hecho que se le de importancia a las condiciones de trabajo (tabla 1.3), tomando en cuenta aspectos como la anatomía, fisiología y psicología del operador; buscando evitar problemas tales como el agotamiento, sobrecargas y envejecimiento prematuro.

Tabla 1.3 Aspectos Ergonómicos

ASPECTOS A CONSIDERAR	DESCRIPCION
Trastornos óseos y o musculares	La operación del teclado constituye un movimiento repetitivo y continuo que puede provocar lesiones en los músculos, nervios y huesos de manos y brazos
Trastornos visuales	La pantalla constituye una fuente de luz que incide directamente sobre los ojos del operador. Esto provoca en exposiciones prolongadas cansancio visual, irritación, lagrimeo, visión borrosa y cefalea
Salud mental	La forma monótona de trabajar con las computadoras sobre todo en tarea de ingreso de datos provoca en las personas sensaciones de hastío y estrés informático que pueden llevar en el aspecto fisiológico al incremento de la presión arterial, al aumento de la frecuencia cardíaca; en el aspecto psicológico a la tensión, irritabilidad, agresividad; y de forma general a sensaciones de insatisfacción ante la vida, pérdida de la autoestima.
Ambiente luminoso	La iluminación deficiente causa dolores de cabeza y pérdida de la visión, además de una baja en la productividad
Ambiente climático	El ambiente donde el ser humano trabaja debe ser el adecuado evitando el exceso de calor o las bajas temperaturas.

1.3.3 Control de acceso

Los sistemas de control de acceso de los lugares permiten mantener protegidos los sistemas importantes. En la tabla 1.4 se indican los aspectos a considerar.

Tabla 1.4 Control de acceso

Aspectos a considerar	DESCRIPCION
Personas	El servicio de vigilancia está encargado de controlar el acceso de personas a los edificios, comúnmente mediante la colocación de guardias en lugares estratégicos.
Vehículos	Se debe realizar el control del ingreso y egreso de vehículos e identificación de sus ocupantes.
Sistemas biométricos	Mediante esta tecnología se realizan mediciones en forma electrónica que permiten comparar características únicas de cada persona (manos, ojos y voz)
Termograma	Basado en la emisión de calor corporal mediante el cual se trazan mapas de valores sobre la forma de cada persona
Verificación automática de firmas	Usando emisiones acústicas se toma datos del proceso dinámico de firmar o escribir que constituye un patrón único en cada individuo, pues contiene información de la manera en que la escritura es ejecutada
Animales	Los perros son utilizados para cuidar grandes extensiones de terreno por poseer órganos mucho más sensibles que cualquier dispositivo.
Barreras infrarrojas	Son codificadas por medio de pulsos con el fin de evitar intentos de sabotaje; al ser el haz interrumpido se activa el sistema de alarma no puede ser afectado por la luz ambiental, calefacción, vibraciones.
Microondas	Son ondas de radio de frecuencia muy elevada, permitiendo que se opere con señales de bajo nivel para que no sean afectadas por otras emisiones de radio, no son afectadas por turbulencias de aire o sonidos muy fuertes

Detector ultrasónico	Crea un campo de ondas; ante cualquier movimiento que realiza un cuerpo dentro del espacio protegido, genera una perturbación que acciona la alarma
Circuito cerrado de televisión	Se emplean cámaras colocadas estratégicamente, que permiten controlar todo lo que sucede en el área en la que puede captar imágenes la cámara

1.4 SEGURIDAD LOGICA

1.4.1 Contraseñas

Cada usuario que emplee una computadora debe tener una cuenta, la cual se identifique mediante el *nombre de usuario* y *una contraseña*, siendo esta última el sistema de autenticación más simple y el primer nivel de defensa que poseen los sistemas operativos contra los extraños. Las contraseñas son importantes en computadoras que se comparten entre varios usuarios o en computadoras que están conectadas a redes en las que varias tienen una relación de confianza entre ellas.

Muchas de las computadoras personales no utilizan contraseñas facilitando su uso tanto al usuario primario como a cualquiera que esté cerca, y la seguridad de estas esta basado tan solo en medios físicos.

Cuando las computadoras están conectadas a un módem y se puede acceder desde casi cualquier parte del mundo en donde exista teléfonos, o cuando estas se conectan a una red que utiliza gente fuera del círculo inmediato al dueño entonces las contraseñas son muy necesarias.

Los intrusos con una computadora casera y un buen programa para probar contraseñas pueden probar miles en menos de un día. Se dice que una mala contraseña es aquella que se puede adivinar, entre estas están el nombre del usuario, nombres de familiares, nombres escritos al revés o seguidos de un solo dígito, contraseñas cortas, números telefónicos, personajes de películas, nombres de científicos, etc.

Las mejores contraseñas deben ser aquellas que no se pueden adivinar y que poseen las características indicadas en la figura 1.2.

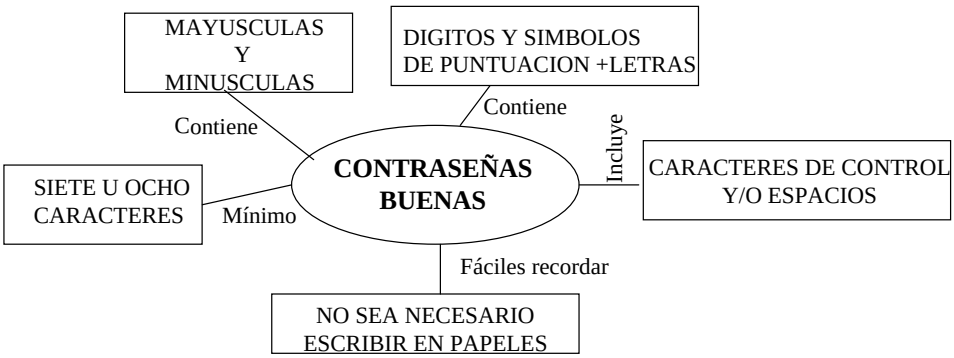


Figura 1.2 Contraseñas buenas

1.4.2 Criptografía

Criptografía constituye el arte y la ciencia de escribir en clave, permitiendo de esta manera mantener la información en secreto. En las computadoras y las comunicaciones actuales se utiliza una forma de criptografía denominada cifrado (es un proceso por el cual un mensaje se transforma en otro mensaje utilizando una función matemática y una contraseña de cifrado especial, llamada clave) el cual desempeña un papel muy importante; pues protege la información almacenada en la computadora contra accesos no autorizados, o cuando ésta es transmitida de un sistema de cómputo a otro evitando alteraciones accidentales o intencionales.

Las limitaciones del cifrado constituyen el no poder prevenir que un agresor borre intencionalmente todos los datos, que una persona modifique el programa de cifrado mismo, o construya un decodificador, por lo que el cifrado constituye solo una parte de la estrategia de seguridad.

Todos los sistemas de cifrado tienen ciertos elementos en común como se indica en la tabla 1.5

Tabla 1.2 Elementos de cifrado

ELEMENTOS	**SIGNIFICADO**
Algoritmo de cifrado	Mediante fundamentos matemáticos desempeña la función de cifrar y descifrar sus datos
Claves de cifrado	Son utilizadas por el algoritmo de cifrado para determinar como cifrar o descifrar datos. El programa de cifrado usa su clave para transformar el texto cifrado en texto claro.
Longitud de clave	La clave tiene una longitud predeterminada, el usar claves largas hace más difícil adivinar usando la fuerza bruta.
Texto en claro	Información que se va ha cifrar
Texto cifrado	Información producto de cifrar

1.4.2.1 Tipos principales de algoritmos de encriptado

En la actualidad están en uso dos tipos de algoritmos (figura 1.3) de clave privada y clave pública

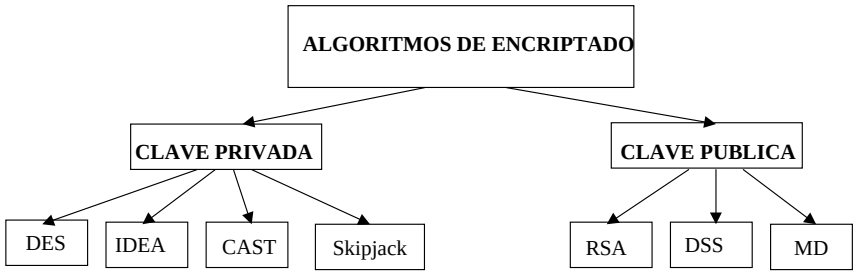


Figura 1.3 Algoritmos de encriptado

a) Clave privada

Utiliza la misma clave para cifrar y descifrar el mensaje. Se le conoce también como criptografía simétrica, los algoritmos más conocidas son los siguientes:

- **Data Encryption Standard (DES)**

  Es uno de los más comúnmente empleados, desarrollado por IBM, es un algoritmo muy conocido, con una gran base de implementaciones en aplicaciones comerciales y gubernamentales. Es la norma gubernamental de encriptado de los EE. UU desde 1976, pero solo para material no ultra secreto.

  Kerberos[1] utiliza el algoritmo DES para encriptar mensajes y para crear las llaves privadas que se emplean en las distintas transacciones. La llave puede ser cualquier número de 64 bits, pero debido a la forma que trabaja el algoritmo, su extensión efectiva es 56 bits.

  Para romperlo se necesitaría 2.000 años si se prueba 1.000.000 de llaves cada segundo por medio de una búsqueda exhaustiva del espacio de llave, pues el algoritmo proporciona 2^{56} llaves posibles. En 1997 el algoritmo fue abierto por DES Challenge .

- ***International Encryption Algorithm (IDEA)***

  Es uno de los algoritmos más seguros y mejor estructurados, utiliza una operación de retroalimentación de encriptado que refuerza el algoritmo; de esta forma el texto de encriptado se emplea como entrada del algoritmo de encriptado. IDEA es ideal para FTP, donde se transmite gran cantidad de datos, pero funciona deficientemente con Telnet.

  Este algoritmo utiliza un tamaño de bloque de 64 bits, lo suficientemente sólido contra el criptoanálisis, no tiene problema cuando encripta grandes cantidades de datos.

- **Cast**

  Utiliza un tamaño de bloque de 64 bits y una llave de 64 bits. El algoritmo emplea seis S-boxes

[1] http://www.process.com

con una entrada de 8 bits y una salida de 32 bits.[2]

- **Skipjack**

  Es un algoritmo sobre el cual no se conoce mucho porque esta clasificado como un secreto por el gobierno de Estados Unidos. Se conoce que utiliza una llave de 80 bits y tiene 32 vueltas de procedimiento por cada operación de encriptado o descencriptado. Es muy seguro pues si se emplea 100.000 computadoras RISC y cada computadora tuviera la capacidad de manejar cerca de 100.000 encriptados por segundo necesitaría 4 millones de años para abrir el código.[3]

b) Clave pública

En este modelo de criptosistemas se utiliza dos llaves que se usan juntas. Una de las llaves siempre permanece en secreto mientras que la otra es pública; puede utilizarse cada llave tanto para encriptado como descencriptado. Este sistema ayuda a resolver problemas de distribución de llaves a los usuarios, se utiliza para certificados[4], firmas digitales y texto simple.

- **Rivest Shamir Adleman (RSA)**

  Fue desarrollado en 1977, se ha convertido en una especie de norma, pues es el más utilizado. Para trabajar RSA toma 2 números primos, p y q y encuentra su producto n=pq. Elige un número e, menor que n y relativamente primo a (p-1)(q-1), y determina su inverso, d, mod(p-1)(q-1), lo que significa que ed = 1 mod(p-1)(q-1); e y d son los llamados exponentes público y privado, respectivamente. La llave pública es el par (n,e); la llave privada es d. Los factores p y q deben guardarse en secreto o destruirse. La seguridad de RSA dependerá del tamaño de la llave empleada.

- **Digital Signature Standard (DSS)**

  Es una norma gubernamental estadounidense para firmas digitales, le permite claves entre 512 y

[2] http://www.cs.wm.edu/~hallyn/des/sbox.html
[3] http://www.austinlinks.com/Crypto/non-tech.html
[4] http://home.netscape.com/comprod/server_central/support/faq/certificate_faq.html#1

1024 bits. Tiene algunos problemas, la fuga de datos secretos es una de ellos, si utiliza 2 veces el mismo número aleatorio cuando genera la firma, se revelará la llave secreta.

- **Message Digest (MD)**

  Los algoritmos de sintetización de mensajes se crearon para tomar cualquier mensaje como entrada y producir como salida una síntesis del mensaje. Existen 3 versiones disponibles que son: MD2, MD4 y MD5.

  MD5 es la versión más reciente, se puede utilizar para trasladar una cadena de bytes de longitud arbitraria en un valor de 128 bits. MD5 procesa el texto de entrada en bloques de 512 bits, divididos en 16 bloques secundarios de 32 bits. La salida es un conjunto de cuatro bloques de 32 bits, que están conectados en un solo valor de dispersión de 128 bits.

1.4.3 Cuentas a proteger

Cada cuenta en la computadora es una puerta hacia el exterior, que puede ser usada por usuarios autorizados y no autorizados. En la figura 1.4 se observan los tipos de cuentas.

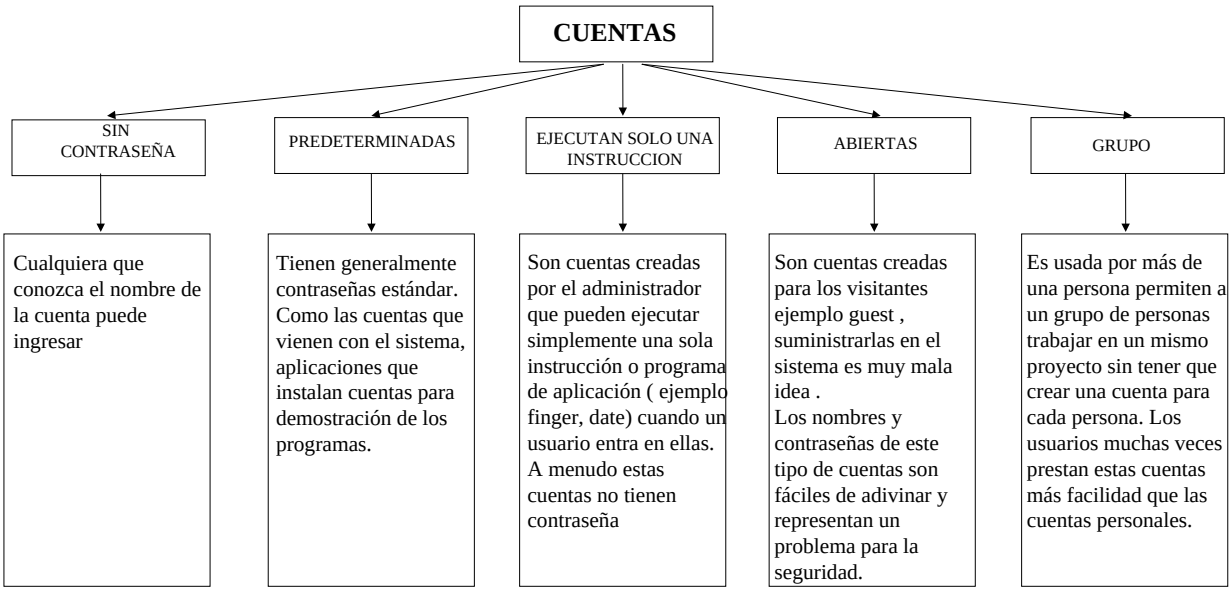


Figura 1.4 Clases de cuentas

1.4.4 Formas de detectar cambios en archivos

Existen tres formas de detectar cambios en archivos:

a) Usar copias para comparar datos a vigilar

Se mantiene una copia de datos no alterados y se realiza una comparación byte a byte cuando se necesita; al existir un cambio se podrá detectar él mismo. Al descubrirse un cambio no autorizado se podrá realizar la restauración del sistema a la normalidad. Este método es considerado demasiado costoso, pues se requiere espacio sustancial de disco para almacenar las copias.

b) Listas de control y metadatos

Es un método más eficiente mediante el cual se guarda un resumen de cada archivo y directorio, al ser necesario hacer una comparación las características serán regeneradas y comparadas con la información almacenada. Esto permite detectar cambios en los metadatos tales como en los propietarios de los archivos o los modos de protección. Este método tiene un problema debido a que pueden los archivos ser modificados de tal forma que la información que se vigila no muestre el cambio.

c) Listas de control y firmas

Consiste en crear una firma digital para los contenidos de los archivos para determinar si se efectúo un cambio. El sistema de firmas digitales de uso más común es la combinación de mensajes MD5 y el mecanismo de cifrado con clave pública RSA.

1.4.5 Respaldos

Para la protección de los datos lo más importante es realizar respaldos y verificarlos, pues ante un desastre se puede comparar el sistema actual con el sistema respaldado y se puede restaurar el sistema a un estado estable, esto se puede hacer aun cuando se haya perdido el equipo físicamente. Los respaldos son importantes por razones como las que se indican en la tabla 1.3.

Tabla 1.3 Razones para realizar respaldos

RAZONES PARA HACER RESPALDOS	DESCRIPCION
Errores de usuario	Los usuarios novatos casi siempre borran o sobre escriben archivos, destruyen directorios completos al cometer un error tecleando un carácter especial
Errores del personal de sistemas	Los encargados del sistema pueden cometer errores, con respecto al servicio que se esta proporcionando a los usuarios.
Fallas de software	Los programas de aplicación pueden venir con defectos ocultos que destruyen de pronto los datos
Fallas de hardware	Las famosas caídas del sistema que frecuentemente destruyen datos
Vandalismo	Los intrusos que con malicia alteran o borran datos. El robo del equipo y perdida consigo de la información
Desastres	Pérdidas causadas por desastres naturales como lluvia, terremotos, incendios. Fugas de agua

Existen tres tipos básicos de respaldos:

- **Respaldo día – cero**

  Se realiza una copia del sistema original.

- **Respaldo completo**

  Se hace una copia de cada archivo de la computadora en el dispositivo de respaldo.

- **Respaldo incremental**

  Se efectúa una copia en el dispositivo de respaldo solo de aquellos elementos en el sistema de archivo que se hayan modificado.

1.4.6 Vigilar el comportamiento del sistema

La vigilancia de los mecanismos de protección permitirán ver que estos realmente funcionen. Las bitácoras son la forma de poder detectar problemas (causas de errores), o localizar ataques (fuente de intromisión) y avalizar el daño causado, pues revelan problemas en el equipo, con la configuración de la red y con la seguridad

Los programas de noticias de Usenet, los servidores gopher, las aplicaciones de bases de datos, la World Wide Web, y muchas otras aplicaciones generan bitácoras en las cuales se van registrando el uso e indican potenciales problemas.

El proceso de auditar puede ayudar a decidir sobre necesidades de la red y resolver ciertos problemas que puede sufrir el entorno.

Durante la auditoría de la red comúnmente se decide que equipos de red se desea auditar y la información que sobre los mismos se desea obtener. Lo mejor es auditar sucesos relacionados con información privilegiada y seguridad.

Los archivos de registro de seguridad nos permiten conocer sobre sucesos tales como:

- Intentos de inicio de sesión completados con éxito y/o fallidos; cambios, creaciones o eliminaciones de cuentas de usuario o de grupo.

- Registro de cuando una cuenta cambia de nombre, se desactiva, se activa o se vuelve a establecer su contraseña.
- Inicios o cierres de sesión de usuario.
- Acceso a un archivo carpeta o impresora por parte de un usuario.
- Cambios realizados en las opciones de seguridad de un usuario, derechos de usuario y planes de auditoría.
- Acción desarrollada por un usuario en el sistema local.
- Acción realizada por un programa.
- Sucesos que afectan a la seguridad del sistema operativo o la seguridad en general.

1.5 AMENAZAS LOGICAS

Los errores de programación son la causa más común del comportamiento inesperado de un programa, pero si en cambio la fuente de instrucciones que hacen que el programa se comporte de forma anormal es debido a un individuo malicioso, entonces se está hablando de amenazas lógicas.

Existen programas maliciosos que son usados para ataques lógicos como los que se muestra en la tabla 1.7.

Tabla 1.7 Programas usados en las amenazas lógicas

PROGRAMAS	DEFINICIONES
Herramientas de seguridad	Diseñadas para que los administradores las utilicen en seguridad para encontrar problemas en sus sitios, además pueden ser utilizadas por alguien que busque fallas a explotar. También existen programas y juegos de herramientas que su única función es atacar a las computadoras
Puertas traseras	Es código escrito dentro de aplicaciones o sistemas operativos que permiten a los programadores el acceso a programas sin que sea necesario que paseen a

	través de autenticación de acceso, por lo tanto permiten el acceso no autorizado al sistema.
Bombas lógicas	Son características ocultas en programas que permanecen en ese estado hasta que se disparan, ejecutando una función que no es propia del programa en la cual están contenidas. Una vez que se dispara puede destruir o alterar datos, interrumpir el funcionamiento de la computadora o dañar el sistema.
Caballos de troya	Son similares a los programas que un usuario le gustaría usar (juegos, editores, hojas de cálculo, páginas Web, correo codificado en MIME), pero mientras el programa parece estar realizando lo que se le ordena, esta haciendo algo más sin el conocimiento del usuario.
Gusanos	Son programas que se propagan de computadora en computadora en una red, sin necesariamente hacer modificaciones en otros programas de la máquina en la que se encuentran, a no ser que contengan otro código que si lo haga (virus)
Bacterias	Son programas que no dañan ningún archivo, lo que hacen es copias de si mismos con el fin de saturar los recursos de un sistema (capacidad de procesador, la memoria, espacio en disco), reproduciéndose de forma exponencial.
Virus	Es código que se inserta en otro código ejecutable, para que en el momento que se ejecute el programa que requiere el usuario, el programa virus también se ejecute. Los virus se encuentran de forma general en computadoras personales.

Estos ataques se realizan por las razones siguientes:

La mayoría de las puertas traseras, bombas lógicas, caballos de troya y bacterias aparecen en el sistema porque se escribieron allí, por lo que la más grande amenaza al sistema es su propio grupo

de usuarios que entienden el sistema, conocen sus debilidades y saben sobre los sistemas de control y auditoría existentes.

Los usuarios también pueden ser agentes involuntarios de transmisión de virus, gusanos y otros tipos de amenazas, al instalar programas obtenidos de fuentes de dominio público, por ejemplo mediante un proceso simple se bajan de la WWW.

Si una máquina es conectada a una red o a otro medio de comunicación computadora a computadora, los programas como gusanos que pueden contener bombas lógicas o virus tendrán una forma de ingresar.
La mayoría de los sistemas se configura confiando en los usuarios , las máquinas y los servicios en el ambiente local.

1.5.1 TIPOS DE ATAQUES

Los ataques se llevan a cabo sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos. Existe una gran cantidad y variabilidad de los mismos, y estos se llevan a cabo remotamente.

a) Ingeniería Social

Se basa en convencer a las personas de que realicen acciones que normalmente no lo hacen para que revele lo necesario con la finalidad de superar las barreras de seguridad, es muy utilizada para averiguar nombres de usuarios y passwords.

b) Trashing

Los usuarios anotan su login y password en papelitos que luego cuando se lo graban en la mente proceden a votar en la basura.

c) Shoulder Surfing

Explota el error de los usuarios de dejar su login y password anotados cerca de la computadora o ver al usuario por encima del hombro en el momento en que teclea su nombre y password.

d) Decoy

Son programas que se diseñan con la misma interfaz que el original que conoce el usuario, en el cual se imita la solicitud del login y el usuario desprevenido lo hace; el programa guardará esta información y dará paso a las actividades normales del sistema.

Otra técnica semejante es mediante un programa que permite guardar todas las teclas presionadas en una sesión.

e) TCP Connect Scanning

Es el scanneo de puertos TCP; si el puerto está habilitado devolverá una respuesta de éxito. Para usar esta técnica no se necesita de privilegios especiales.

f) TCP SYN Scanning

En esta técnica se envía un paquete SYN como si se deseara abrir una conexión y se espera por la respuesta ACK; e inmediatamente recibida esta se envía un RST para terminar la conexión y se registra el puerto como abierto

g) TCP FIN Scanning – Stealth Port Scannig

Debido a que en la actualidad los Firewalls y Routers monitorean la red en busca de paquetes SYN a puertos restringidos, el TCP SYN Scanning no es lo suficientemente clandestino para ser utilizado por los atacantes.

El tipo de scanneo TCP FIN se basa en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente; mientras que los puertos abiertos suelen ignorarlo.

h) Eavesdropping – Packet Sniffing

Este ataque se realiza utilizando programas sniffers, los cuales monitorean los paquetes que circulan por la red; pueden ser ubicados en una estación de trabajo conectada a la red, en un router o gateway de Internet; para lo cual el usuario que lo realiza debe tener acceso legítimo a estos dispositivos.

Se emplea comúnmente para robar password de un recurso compartido o de acceso a una cuenta que viajen sin encriptar; capturar números de tarjetas de crédito y direcciones de e-mails; para lo cual se analizan las tramas de un segmento de red.

i) Snooping Downloading

A diferencia del anterior además de interceptar el tráfico de red, el atacante ingresa los documentos, mensajes de correo electrónico y otra información guardada, para a continuación, en la mayoría de los casos realizar copias de estos a su propia computadora, para luego proceder a un análisis exhaustivo.

j) Spoofing – Looping

El objetivo de esta técnica es actuar en nombre de otros usuarios; para lo cual el intruso utiliza un sistema para obtener información y utilizar en otro sistema, y luego utiliza esta información para ingresar en otro y así sucesivamente, lo que hace casi imposible la ubicación del atacante.

El envío de falsos e-mail es otra forma de Spoofing, en el cual el atacante envía un e-mail a nombre de otra persona.

k) IP Spoofing

El atacante genera paquetes de Internet con una dirección de red falsa en el campo fuente, que es aceptado por el destinatario del paquete. Si la víctima descubre el ataque verá a otra máquina como su atacante y no al verdadero origen.

l) Web Spoofing

Se crea un sitio Web completo similar al que la víctima desea ingresar; permitiéndole monitorear al atacante todas las acciones de la víctima.

m) IP Splicing-Hijacking

El atacante consigue interceptar una sesión ya establecida; esperando primeramente que el usuario legítimo se identifique ante el sistema y tras ello le suplanta como usuario autorizado. Para este ataque son utilizados los Sniffer que permiten ver todo el proceso Handshake; desarrollado éste el atacante calcula el número de secuencia siguiente, luego del cual él envía el paquete. El servidor no notará el cambio de origen

n) Jamming

Se utiliza para desactivar o saturar los recursos del sistema, para lo cual el atacante utiliza falsas direcciones IP, el servidor al responder al mensaje y no recibir respuesta acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas. Otra forma es enviando miles de e-mails sin sentido a todos los usuarios posibles en forma contínua, saturando los sistemas destino.

o) SYN Flood

El proceso handshake se lleva a cabo en tres pasos, si el paso final no llega a establecerse, la conexión permanece en un estado denominado “semiabierto”, Si se crean muchas peticiones

incompletas de conexión el servidor estará inactivo mucho tiempo esperando respuesta ocasionando lentitud en los demás servicios .

p) Connection Flood

Los ISP tienen un límite máximo en el número de conexiones simultaneas, una vez alcanzado el mismo no se admitirán conexiones nuevas; mientras van caducando las conexiones el atacante intenta nuevas conexiones para mantener fuera de servicio al servidor

q) Land Attack

Este ataque es común a las plataformas Windows en el cual se envía a un puerto abierto de un servidor un paquete que contiene la dirección y puerto fuente igual a la del destino; luego de una cierta cantidad de este tipo de mensajes provoca la caída del sistema.

r) Uso de diccionarios

Son archivos con millones de palabras, las cuales pueden ser posibles password de los usuarios, esta forma de obtener información del usuario legítimo se conoce como fuerza bruta.

s) Broadcast Storm

Se basa en la recolección de una serie de direcciones broadcast, para a continuación enviar una petición ICMP (ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. La petición maliciosa hecha, será repetida en broadcast por cientos o miles de host enviando una respuesta de eco a la víctima cuya dirección IP figuraba en el paquete ICMP como que realizaba el ping.

t) Out of Band, Supernuke

El ataque OOB consiste en configurar el bit URG del TCP como válido, lo que provoca que a estos paquetes trate de darles prioridad el sistema operativo de la máquina atacada.

El Nuke es una ataque que se realiza contra los equipos con windows, que escuchan por el puerto NetBios (137-139) mediante el envío de paquetes UDP manipulados

u) E-mail bombing, spamming

El bombing consiste en enviar gran cantidad de veces el mismo mensaje a una misma dirección, saturando así el buzón del destinatario. El spamming es enviar e-mails a miles de usuarios hayan estos solicitado el mensaje o no.

v) Ataques con Java Applets

Los applets son código ejecutable y por lo cual susceptibles de ser manipulados por intrusos, existe gente especializada en descubrir fallas de seguridad en las implementaciones de Java.

w) Ataques con JavaScript y Vbscript

Son programas que son interpretados por el navegador por lo cual los atacantes los utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo.

x) Ataques con ActiveX

ActiveX aparentemente soluciona los problemas de seguridad mediante certificados y firmas digitales, pero esta característica se ha convertido en su mayor punto débil, debido a que la mayoría de los usuarios aceptan el certificado sin siquiera leer, pudiendo ser esta la fuente de un ataque con un control dañino.

1.5.2 Proceso de ataque a las redes informáticas

Quienes atacan las redes lo hacen mediante procedimientos estructurados que les permite ir conociendo a su víctima, utilizando herramientas gratuitas o comerciales. El proceso es el siguiente:

1) Búsqueda de Información

Lo primero que hará un atacante, es examinar la página Web de la víctima, buscando información que le pueda ser útil, para lo cual puede emplear herramientas de copiado de sitios web enteros:

Tabla 1.8 Herramientas de copiado de sitios Web

Herramienta	Sistema Operativo	Página web
Wget	UNIX	http://www.gnu.org/software/wget/wget.html
Teleport Pro	Windows	http://www.tenmax.com/teleport/home.htm

Después se buscará páginas Web relacionadas con la víctima empleando herramientas como FerretPRO (http://www.ferretsoft.com) que le permite utilizar varios buscadores simultáneamente, o mediante un buscador múltiple como dogpile (http://www.dogpile.com), o realizando búsquedas avanzadas en su buscador favorito.

Además de las fuentes anteriores de información procederá a recolectar más información como son:

- Notas de prensa
- Números de teléfono
- Nombres de contactos y direcciones de correo electrónico
- Directivas de seguridad o privacidad que indiquen los tipos de mecanismos de seguridad instalados en la red.
- Visión del código fuente HTML de la páginas Web de la víctima buscando comentarios que le sean beneficiosos.

2) Fallas en la configuración del DNS

Identificado el nombre de dominio procederá a consultar el servidor DNS, para comprobar si está configurado de forma insegura para poder obtener información muy importante sobre la Institución víctima.

Dos fallas de configuración muy extendidas en los servidores DNS son:

- Permitir que se realice una transferencia de zona de DNS a usuarios de Internet no autorizados.
- Cuando no se utiliza un mecanismo de DNS público - privado para separar la información de DNS externa que es pública de la interna que es información DNS privada; pues en este caso el atacante puede ver los nombres de Hosts internos y las direcciones IP.

Al encontrar estos problemas en el servidor DNS procederá a transferir la zona desde una máquina con sistemas operativos Unix, NT o W2000 Server, utilizando la herramienta cliente **nslookup.**

Existen otras herramientas que se pueden utilizar para transferencia de zona como *axfr 1*(http://cr.yp.to/djbdns/axfr-get.html *)*, que transfiere de forma recursiva información de zona y crea una base de datos comprimida de la zona y de los archivos huésped para cada uno de los dominios consultados.

3) Identificación de la topología

Para identificar la topología de una red y sus posibles rutas de acceso potenciales puede utilizar el programa *traceroute* para el caso de Unix o *tracert* para Windows. Estas herramientas le permiten ver la ruta que sigue un paquete IP desde un host al siguiente.

Para explorar sistemas que estén situados detrás de un dispositivo de control de acceso (se da cuenta de esto porque al realizar un traceroute normal en la indicación de los saltos empiezan a salir tres asteriscos * * *) se envían paquetes con el puerto UDP 53 fijo.

$ traceroute – s –p53 *Ipmáquina atacada*

Existen herramientas que tienen un sistema gráfico para identificar la topología que realizan el mismo trabajo que traceroute o tracert.

Tabla 1.9 Herramientas gráficas para identificar la topología de la red

Herramienta	**Dirección de Internet**
Visual Route	http://www.visualroute.com
Neo Trace	http://www.neotrace.com/

4) Determinación de la actividad de un sistema

Para verificar que un sistema esta activo se realiza un barrido *ping* automatizado en un rango de direcciones IP y bloques de red, previo al ataque real. La técnica más simple es enviar paquetes ICMP Echo (tipo 8) para obtener paquetes ICMP Repley (tipo 0).

Para realizar barridos ping se emplea herramientas como las indicadas en la tabla 1.10 que envían gran cantidad de solicitudes (direcciones IP).

Tabla 1.10 Herramientas para barridos ping

Herramientas	Sistema Operativo	Dirección de Internet
Fping	Unix	http://www.fping.com
Nmap	Unix	www.insecure.org/nmap
Pingar	Windows	http://www.kilievich.com
WS_Ping ProPack	Windows	www.ipswitch.com
NetScan	Windows	www.nwpsw.com

Para solicitar la hora del sistema (timestamp) o la máscara de red (address mask request), con la finalidad de determinar todas las subredes que se están utilizando y poder de esta forma dirigir un ataque a una subred específica, se puede utilizar las herramientas Unix:

Icmpquery (http://www.pestpatrol.com/PestInfo/i/icmpquery_c.asp) o

icmpush (http://packages.qa.debian.org/i/icmpush.html)

5) Exploración de los puertos

Cuando el tráfico ICMP se encuentra bloqueado, se realiza una exploración de puertos de cada una de las direcciones IP que se desee para determinar que hosts están activos en función de los puertos que están abiertos o a la espera.

Al determinar los servicios que se están ejecutando o están en estado listening mediante la exploración de los puertos UDP y TCP, se puede establecer el tipo de sistema operativo y aplicaciones que se están empleando.

Existen muchas herramientas para la exploración de los puertos que corren en Unix (tabla 1.11) o en Windows (tabla 1.12).

Tabla 1.11 Herramientas para la exploración de puertos en Unix

HERRAMIENTA	DIRECCIÓN	CARACTERÍSTICAS
Udp_scan	http://wwdsilx.wwdsi.com/saint/	Desarrollado inicialmente por SATAN es uno de los exploradores UDP más fiables de los que existe actualmente. Las búsquedas se realizan por debajo del puerto 1024, y determinados puertos de alto riesgo por encima de 1024.
Nmap	http://www.insecure.org/nmap	Es una herramienta que ofrece muchas características como las siguientes: Escaneo de los puertos TCP, puertos UDP, determinación de host activos detrás del firewall enviando paquetes TCP ACK a la red objetivo y esperando un paquete RST.
Ping	http://www.kyuzz.org/antirez	Es mejor que nmap, al permitir controlar opciones específicas del paquete TCP, que permiten pasar a través de ciertos dispositivos de control de acceso.

Tabla 1.12 Herramientas para la exploración de puertos en Windows

HERRAMIENTA	DIRECCIÓN	CARACTERÍSTICAS
SuperScan	Http://www.foundstone.com/rdlabs/termsofuse.php?filename=superscan.exe	Permite especificar las direcciones IP y listas de puerto del sistema destino
WinScan	Http://www.prosolve.com	Tiene una versión gráfica y también de línea de comandos.
IpEye	http://ntsecurity.nu	Realiza exploración de puertos y exploraciones SYN, FIN, solo se puede ejecutar en Windows 2000 y solo puede analizar un host de forma simultánea.
WUPS	http://ntsecurity.nu	Es un analizador de puertos UDP gráfico y relativamente rápido.

6) Detección del sistema operativo

Para los atacantes detectar el Sistema Operativo es importante porque existen vulnerabilidades que son específicas de cada uno de ellos. Esto se debe a que cada fabricante cuando escribe sus pilas TCP/IP las interpreta a su manera de lo que viene escrito en el normativo del RFC correspondiente y con estas diferencias es que se detecta el sistema operativo que se esta utilizando.

Los sondeos que se envían y que permiten distinguir un sistema operativo se indican en la tabla 1.13.

Tabla 1.13 Herramientas para identificar un sistema operativo

TIPO DE SONDEO	CARACTERÍSTICAS
Sondeo FIN	Se envía un paquete fin a un puerto abierto. Según el RFC 793 la forma correcta es no responder a este paquete, sin embargo existen sistemas operativos que responden con FIN/ACK, como los de Windows
Sondeo Bogus Flag	Se coloca una bandera indefinida en la cabecera TCP de un paquete SYN. Algunos Sistemas Operativos como linux responden con esta bandera en su paquete de respuesta
Tamaño de ventana inicial TCP	En algunos desarrollos de pilas el tamaño de la ventana inicial es único
Valor ACK	Cuando responden con el ACK algunos sistemas operativos lo hacen con el mismo número de secuencia recibido y otros lo hacen con el número de secuencia + 1.
Muestreo del número de secuencia inicial	Se busca un patrón en la secuencia inicial elegida por la implementación TCP cuando responde a una petición de conexión
Supervisión del bit de no fragmentar	Algunos sistemas operativos activa el bit de no fragmentar para mejorar su rendimiento
Cita de mensajes ICMP	Entre los sistemas operativos difieren en la cantidad de información que entregan cuando envían mensajes de error ICMP.
Integridad de los mensajes de error ICMP	Algunos desarrollos de pilas TCP/IP pueden alterar las cabeceras IP cuando devuelven mensajes de error ICMP.
Tipo de servicio	En los mensajes ICMP de puerto inaccesible, la mayoría de los desarrollos de pilas utilizan un 0, pero existen otras posibilidades
Gestión de fragmentación	Cada pila maneja de forma diferente los fragmentos que se

	superponga. Algunas pilas cuando recomponen los fragmentos escriben los datos nuevos sobre los viejos, y viceversa. Analizando como se recompone los paquetes de sondeo, se puede realizar suposiciones sobre cual es el sistema operativo objetivo
Opciones TCP	Estas opciones son definidas en el RFC 793 y de forma mas reciente en el RFC 1323; donde se pueden encontrar las opciones mas avanzadas, que suelen a su vez estar en los desarrollos de pila más modernos. Enviando un paquete para el que se han definido una serie de acciones, es posible realizar algunas hipótesis sobre cual es el sistema operativo objetivo

Para la detección del sistema operativo se utiliza herramientas que poseen funciones de rastreo de pilas que emplean las técnicas antes mencionadas, que permiten averiguar rápidamente y con una alta probabilidad cual es el sistema operativo instalado en el host, una de estas herramientas es Nmap.

Otra forma que utilizan los atacantes para determinar el sistema operativo es la observación pasiva del tráfico que circula por la red (http://project.honeynet.org) que se basa en el tiempo de vida (TTL), tamaño de ventana, bit de no fragmentación, que es comparado con una base de datos que contiene los atributos indicados para diferentes sistemas operativos. Existe una herramienta denominada siphon (http://siphon.datanerds.net/) para realizar esta actividad.

Se puede emplear también Cheops (http://www.marko.net/cheops/) que es una herramienta de exploración de red pero gráfica.

7) Enumeración de cuentas de usuario, recursos compartidos

Los atacantes lo siguiente que hacen es tratar de identificar cuentas de usuario válidas o recursos compartidos mal protegidos. Conocido por un atacante una cuenta, un recurso compartido o un nombre de usuario de un sistema, solo será cuestión de tiempo para que llegue a adivinar la contraseña correspondiente o que identifique algún punto débil asociado al protocolo de compartición de recursos.

Para esto utiliza herramientas como:

DumpSec (http://www.somarsoft.com) que permite enumerar recursos desde los permisos del sistema de archivos hasta los servicios disponibles en sistemas remotos.

Winfo (http://www.ntsecurity.un) que extrae cuentas de usuario, recursos compartidos, cuentas interdominios de servidores y de estaciones de trabajo, mediante el modificador –n puede crear automáticamente una sesión nula.

lsadump2 (http://razor.bindview.com/tools/desc/lsadump2_readme.html), para revelar los últimos usuarios que han iniciado una sesión en el sistema y las contraseñas asignadas a las cuentas del servicio.

Brututs (http://www.hoobie.net/brutus/) que es una herramienta de fuerza bruta, para descubrir contraseñas.

Se utiliza también sniffers como snort (http://www.snort.org) que trabajan en conjunto con la interfaz de la red para capturar y analizar cualquier tráfico que pase por red.

1.6 SEGURIDAD DE LA RED INTERNA Y LA CONEXIÓN AL INTERNET

La información funciona en ambos sentidos, se debe poder enviar y recibir; tanto cuando se encuentra físicamente utilizando una computadora en su propia red, como cuando se encuentra fuera de ella y por necesidades de obtención o envío de datos debe comunicarse con los servidores de su

red de forma segura, evitando que vándalos puedan manipular la misma, por lo que es importante saber utilizar la tecnología actual.

1.6.1 Acceso a través del teléfono

Los modems son utilizados para permitir a las computadoras transmitir datos a través de las líneas telefónicas; en la actualidad estos permiten ser configurados para realizar y recibir llamadas, esta configuración puede ser remota y ser verificada de la misma manera.

En la actual era del Internet y las redes Locales aun el módem sigue constituyendo la forma más común de tener acceso remoto a las computadoras.

Las instituciones vigilan muchas veces más las conexiones de red que las conexiones de módems, que pudieran existir y que permitan acceso remoto a algún usuario desde dentro de la red constituyendo una puerta trasera.

Existen varias formas de realizar espionaje utilizando los módems entre los más populares se tiene:

- **En el propio local**

  Mediante la colocación de un segundo teléfono o grabadora en paralelo, la instalación de un micrófono para escuchar, el cual no altera el cableado como en los casos anteriores.

- **Entre el local y la oficina central**

  Se empalma un equipo de monitoreo al cable del servicio telefónico

- **En la central telefónica**

  Los empleados de la compañía telefónica pueden intervenir la línea, o un vándalo puede irrumpir en los conmutadores e instalar un micrófono.

- **Sobre un enlace inalámbrico**

  Las llamadas a través del satélite o microondas pueden ser intervenidas y decodificadas .

Para tratar de evitar los ataques mencionados a las redes utilizando módems , se diseñan estos bajo características específicas

- **Módem de contraseña**

  Requieren que el usuario que realiza la llamada se identifique mediante una contraseña antes de que el módem acepte conectarlo con la computadora.

- **Módem de llamada de verificación**

  Es necesario que el usuario que llama ingrese una clave de acceso, e inmediatamente cuelgue el teléfono, el módem inmediatamente realizará una llamada a un número predeterminado.

- **Módem de cifrado**

  Realizan el cifrado de toda la información transmitida y recibida a través de las líneas telefónicas, tiene una seguridad elevada frente a individuos que intentan obtener acceso no autorizado o intervienen las líneas telefónicas.

- **Módem con identificador de llamadas**

  La información proporcionada en este caso por la compañía telefónica es usada para registrar o controlar el acceso.

1.6.2 Protocolos de capa de aplicación de Internet

Los servicios de Internet conllevan riesgos de seguridad que pueden ser conocidos o desconocidos, pequeños o sustanciales y junto a cada uno ellos, en el futuro pueden encontrarse fallas en el protocolo o en el servidor.

a) Telnet

Es uno de los protocolos de aplicación más usados para conectarse a host con el propósito de obtener o intercambiar información. La seguridad es uno de los aspectos que deben ser analizados en el uso de Telnet, debido a que las claves de acceso vienen en formato de texto y sin encriptar por lo que son visibles por tanto requiere para su uso implementar mecanismos de seguridad a niveles inferiores, es decir a nivel de transporte o de red.

El protocolo de seguridad a nivel de capa de transporte (TLSP), permite solucionar la falta de seguridad de las conexiones telnet, al proveer cifrado criptográfico de extremo a extremo directamente sobre el nivel de red. Sin embargo lo mejor sería considerar la seguridad de las conexiones telnet a nivel de la capa de aplicación pues lo anterior implicaría la introducción del software en el núcleo del sistema operativo.

b) FTP

Es la principal forma de transferencia de archivos en Internet. FTP soporta dos modos de operación, el activo (modo predeterminado) y el pasivo los cuales determinan cuando el servidor o el cliente inician conexiones TCP que se emplean para enviar información desde el servidor al anfitrión. El servicio FTP anónimo al ser instalado debe tenerse cuidado, porque es similar a tener a alguien conectado con una cuenta guest en el servidor de la red; pues una vez que un hacker esté dentro de su servidor FTP, puede aprovechar de él y poner en peligro la seguridad del sitio.

c) SNMP

Es un protocolo que permite la administración remota de los dispositivos en la red, mediante el cual se puede monitorear el estado actual de la red o realizar cambios del estado de algunos de los

dispositivos de la red. Por tanto SNMP puede ser útil para un hacker porque este puede conocer la estructura interna de la red, modificarla, hacer cambios en la configuración o detener totalmente las operaciones.

d) DNS

Es un servicio de consulta de datos distribuido usado en Internet para traducir nombres de host.

DNS trabaja sobre el protocolo UDP para el proceso real de resolución de nombres de anfitrión, mientras TCP utiliza para transferencias de zona, las cuales pueden representar un riesgo de seguridad debido a que proporciona a extraños una lista completa de todas las computadoras conectadas a la red interna de la institución.

e) HTTP

Es el protocolo usado para solicitar y recibir documentos de servidores en la World Wide Web. HTTP puede usarse genéricamente para comunicación entre agentes de usuario y proxy o gateway para otros protocolos de Internet como SMTP, NNTP, FTP, Gopher y Wais; la flexibilidad ofrecida dificulta de sobremanera asegurar los servicios Web y los clientes.

HTTP tiene algunos agujeros de seguridad como el de permitir a los usuarios remotos solicitar comunicación a una máquina de servidor remoto y ejecutar comandos de forma remota lo cual compromete el servidor Web y al cliente en la autenticación de las solicitudes remotas, y de los servidores Web, violación de la privacidad de solicitud y respuesta, abuso de características de servidor y recursos, explotación de errores y agujeros de seguridad en los servidores, extracción de direcciones IP, nombres de dominio, nombres de archivo, etc. Por lo que podemos decir que los servidores Web son muy vulnerables a los comportamientos de los clientes en Internet .

Otro agujero existente proviene de las bitácoras del servidor las cuales contiene gran cantidad de datos personales sobre la información solicitada a diferentes usuarios; el problema de HTTP es que permite que se recupere dicha información sin ningún esquema de permisos de acceso .

Las tecnologías y esquemas de HTTP seguros son un serio intento por resolver los problemas de seguridad mencionados anteriormente a continuación se hace referencia a las más conocidas:

f) S-HTTP

Es el protocolo seguro de transferencia de hipertexto, desarrollado para solucionar el vacío de seguridad en la protección de información delicada durante su transmisión por Internet. Mediante S-HTTP un servidor seguro puede responder a una solicitud con un mensaje encriptado y firmado y mediante el mismo método un cliente seguro puede verificar una firma de un mensaje y autenticarla; la autenticación se lleva a cabo a través de la llave pública del servidor.

g) SSL

Es el protocolo de capa de sockets seguro, fue realizado con el propósito de desarrollar la seguridad de los datos de protocolos de la capa de aplicación HTTP, Telnet, NNTP, FTP.

SSL se basa en el encriptado de datos, autenticación de servidor, integridad de mensajes y autenticación opcional del cliente para una conexión TCP/IP.

1.6.3 Cortafuegos

Cada vez más personas pertenecientes a las Universidades tienen interés en poseer su correo electrónico, buscar en la Web, obtener archivos y estas Instituciones Educativas como tales desean ser conocidas a través del Internet publicando información propia, pero al tener que mantener un

cierto nivel de aislamiento y por tanto un grado de seguridad del exterior las Universidades utilizan los Firewalls.

En la política del cortafuegos se debe definir los datos que deben pasar y cuales serán bloqueados, o impedir que ciertos usuarios o máquinas accedan a ciertos servidores o servicios.

El cortafuegos puede ser utilizado para vigilar las comunicaciones entre la red interna y red externa, obtener registros para realizar un seguimiento de las penetraciones a la red o detectar una subversión interna .

Para formar las redes privadas virtuales cuando las instituciones tienen localidades físicas en distintos lugares mediante la programación del cortafuegos se puede hacer que automáticamente cifre paquetes que son enviados entre redes de la institución y de esta forma se utiliza el Internet como la red WAN

El uso de firewalls internos en una institución permite aislar las fallas físicas en la red a un número de máquinas menor, limita los daños producidos por el espionaje y las afectadas con ataques de desbordamiento y saturación y además crea barreras contra agresores internos y externos los cuales siempre buscan atacar máquinas específicas.

CAPITULO II

METODOLOGIA

2. METODOLOGIA

2.1 METODOLOGIA UTILIZADA

El presente estudio se realiza con el método científico debido a que la razón de la investigación está sujeta a una realidad en la que están inmersos los administradores de las redes Universitarias del País.

Esta investigación científica se efectúa de forma rigurosa y cuidadosa tratando de que sea sistemática, controlada y a su vez crítica de las proposiciones hipotéticas sobre las presumidas relaciones existentes en las políticas y procedimientos de seguridad en las Universidades y el Internet.

La presente investigación es aplicada pues busca resolver problemas existentes durante la utilización del Internet.

En la metodología se toma muy en cuenta los siguientes elementos:

- Se concibe inicialmente la idea a investigar, planteándose los problemas de investigación.
- Se plantean objetivos de investigación que buscan contribuir a resolver el problema de la seguridad de las redes Universitarias.
- En la justificación se exponen las razones por las cuales es necesario investigar el tema , su factibilidad y viabilidad.
- El marco teórico permite orientar la forma en que se realiza el estudio, evitando desviaciones del planteamiento original. Al final del trabajo el marco teórico se convierte en el marco de referencia para interpretar los resultados del estudio.
- La hipótesis planteada involucra dos variables que surge de los objetivos de la investigación y tiene una estrecha relación con el planteamiento del problema.

- La hipótesis se somete a prueba en un universo y contexto bien definidos que son las Universidades del Ecuador y sus actores principales los Administradores de las redes.
- Se define operacionalmente las variables contenidas en la hipótesis
- La presente investigación es ex post-facto en la cual no se manipularán las variables, pues se observarán situaciones ya existentes.
- Definida la unidad de análisis, se procede a delimitar la población que va hacer estudiada y sobre la cual se busca generalizar los resultados.
- Se recolecta los datos pertinentes sobre las variables involucradas en la investigación, mediante el instrumento de medición (cuestionario) que se construye utilizando una técnica apropiada para ello.
- Además se realiza entrevistas, encuestas, sesiones de trabajo. Se utiliza herramientas estadísticas descriptivas e inferenciales y se indaga las relaciones causales existentes.
- Con los datos recogidos, evaluados y los resultados obtenidos del mismo se diseña una propuesta para la políticas y procedimientos de seguridad con el fin optimizar la operatividad de los sistemas de redes universitarias ecuatorianas conectadas al Internet.
- Se elabora las conclusiones fruto de las investigaciones realizadas y es el antecedente de la valía de la propuesta.

2.2 UNIVERSO Y MUESTRA

El universo esta constituido por las Universidades y Escuelas Politécnicas que están conectadas al Internet (fuente: CONESUP[6]), sean estas públicas o privadas, que se encuentran en las Provincias de Bolívar, Chimborazo, Cotopaxi, Guayas, Pichincha, y Tungurahua.

[6] http://www.conesup.net

2.2.1 Población y fracción muestral

Universidades y Escuelas Politécnicas:

Bolívar	1
Chimborazo	2
Cotopaxi	1
Guayas	8
Pichincha	12
Tungurahua	2
Total	**26**

Determinación del tamaño de la muestra

$$n = \frac{PQ\ N}{(N-1)\frac{E^2}{K^2} + PQ}$$

n = Tamaño de la muestra

PQ = Constante de la variación poblacional 0.25

N = Universo o población

E = Error máximo admisible 0.05

K = Coeficiente de corrección del error 2

$$n = \frac{0.25 * 26}{(26-1)\ (0.05^2/2^2) + 0.25}$$

$$n = 6.5 / 0.2656$$

$$n = 24.47 \approx 25$$

Determinación de la fracción muestral

$$f = \frac{n}{N}$$

n = Tamaño de la muestra

N = Tamaño de la población

f = 25/ 26

f = 0.961

Se distribuye el tamaño de la muestra proporcionalmente al tamaño de los diferentes Universidades y Escuelas Politécnicas.

Universidades y Politécnicas	**Cálculo**	**Muestra Parcial**
Bolívar	1 * 0.961= 0.961	1
Chimborazo	2 * 0.961 = 1.922	2
Cotopaxi	1 * 0.961 = 0.961	1
Guayas	8 * 0.961 = 7.688	8
Pichincha	12 * 0.961 = 11.532	11
Tungurahua	2 * 0.961 = 1.922	2
Muestra		25

En el Anexo A se encuentran las encuestas realizadas a los Administradores de las Redes de Universidades y Escuelas Politécnicas.

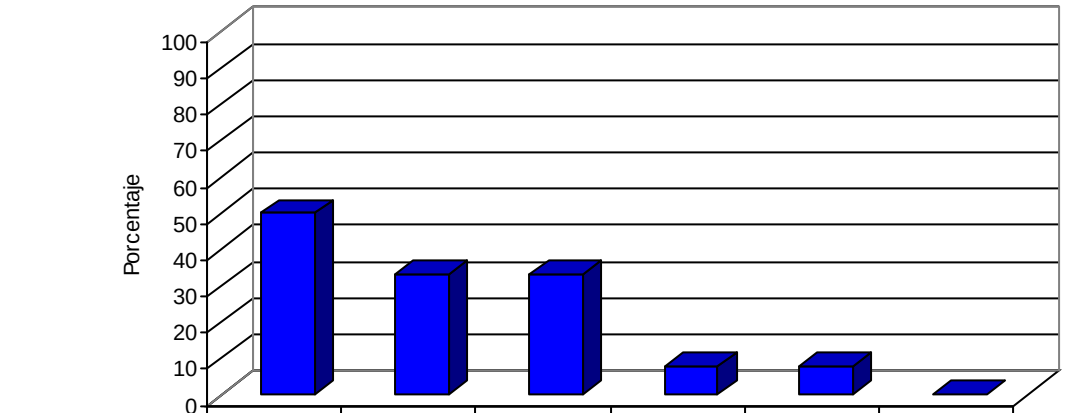
CAPITULO III

ANALISIS DE LAS SEGURIDADES IMPLEMENTADAS EN LAS UNIVERSIDADES Y ESCUELAS POLITECNICAS

3. ANALISIS DE LAS SEGURIDADES IMPLEMENTADAS EN LAS UNIVERSIDADES Y ESCUELAS POLITECNICAS

3.1 SEGURIDAD FISICA

3.1.1 Control de acceso



	Servicio de vigilancia	Formularios de datos personales	Credenciales de identificación	Algo que saben (password)	Sistema biométrico	Verificación automática de firmas
Control acceso en %	50	33	33	8	8	0

Figura 3.1 Control del acceso de personas

La mitad de las Universidades (el término Universidades se empleará para referirse a las Universidades Estatales y Particulares, y Escuelas Politécnicas del país) poseen servicios de vigilancia los cual están encargados del control de acceso de personas a los predios universitarios, mediante ubicación de guardias en lugares estratégicos. El otro 50% no posee un sistema de vigilancia mediante guardias; y encargan a sus conserjes el cuidado de los bienes Universitarios, en su totalidad, por lo que la probabilidad de perdidas se incrementa, en los momentos que no permanecen en su lugar por tener que realizar la entregar de documentación en otras dependencias Universitarias o ausentarse del lugar de trabajo luego de haber cumplido su jornada laboral.

La tercera parte de las Universidades utilizan formularios de datos personales para el ingreso a los Centros de Cómputo de todas las personas. Al producirse un suceso extraño de robo o daño se puede identificar a las personas que estuvieron en las instalaciones durante el tiempo que se produjo.

Un 33% de Universidades solicitan una credencial de identificación, comúnmente la cédula que es canjeada por una credencial durante el tiempo que dura la visita. Otras Universidades poseen credenciales para el personal permanente de planta, para el recién ingresado, para personas ajenas a la Institución que por algún motivo deben ingresar a dar algún tipo de servicio. La desventaja del uso de estas credenciales es que pueden ser copiadas o robadas permitiendo el acceso a cualquier persona que la posea.

El 8% de las Universidades emplean para el personal que trabaja en sus instalaciones de Cómputo una clave de acceso que es única para esa persona, la cual se solicita a su ingreso. La clave es constatada con una base de datos que almacena información de las personas autorizadas a ingresar. Este sistema puede no ser tan seguro en vista de que las personas eligen identificaciones sencillas o las olvidan.

Las Universidades están empezando a utilizar lectores biométricos (8%) que mediante mediciones en forma electrónica permiten identificar a la persona a través de las huellas digitales, el iris del ojo y la voz. Con estos sistemas los costos de administración disminuyen, pues se requiere solamente de una persona que realice el mantenimiento de la base de datos con la información biométrica.

Ninguna Universidad emplea verificación automática de firmas, que permitiría identificar a las personas mediante la secuencia sonora de emisión acústica que es generada durante el proceso de escribir, éste patrón es único en cada individuo. En la actualidad los equipos utilizados para esta forma de verificación son de bajo costo y robustos, que constan de una placa de metal sensible al proceso de firmar y una computadora que registra el mismo.

3.1.2 Ambiente de los centros de cómputo

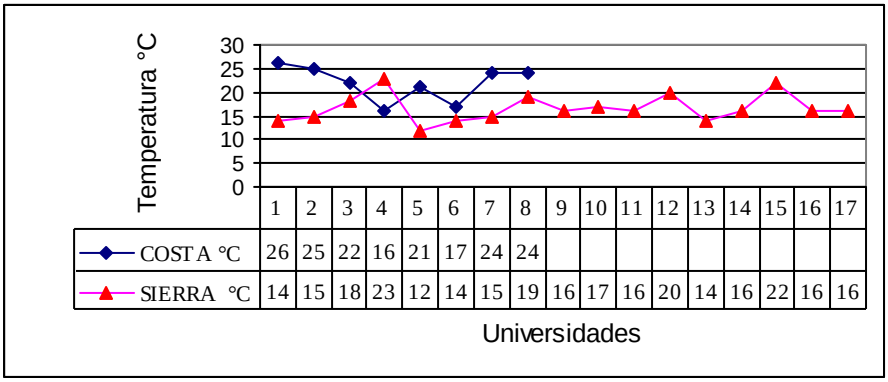


Figura 3.2 Temperatura media en los Centros de Cómputo

La temperatura ambiental media de los Centros de Cómputo de las Universidades, oscilan alrededor de 16.6°C en la sierra y 21.9°C en la costa. La temperatura es importante considerar debido a que si ésta es demasiado alta (sobre los 30 °C) las computadoras no se pueden emplear de forma adecuada , por falta de enfriamiento y sus componentes pueden dañarse. En el caso de las Universidades que trabajan con temperaturas menores a los 18 °C no existe problemas en la conservación de los equipos, pero si la temperatura del ambiente es menor a los 7.5 °C, se debe tener sistemas de alerta porque el equipo con la presencia de demasiado frío puede sufrir un choque térmico al ser encendido, lo cual provocaría que las tarjetas o circuitos integrados se quiebren.

Como se observa en la figura 3.3, el 75 % de los administradores consideran que las instalaciones donde se encuentran los equipos de cómputo no tienen una ventilación adecuada, al no existir una renovación de forma natural o artificial del aire.

Menos de la mitad (42%) de los centros de cómputo cuentan con aire acondicionado en los lugares dedicados para equipos de proceso de datos, firewalls, switch y routers, que tiene la finalidad de mantener en buen estado a los mismos, debido a su importancia y costos.

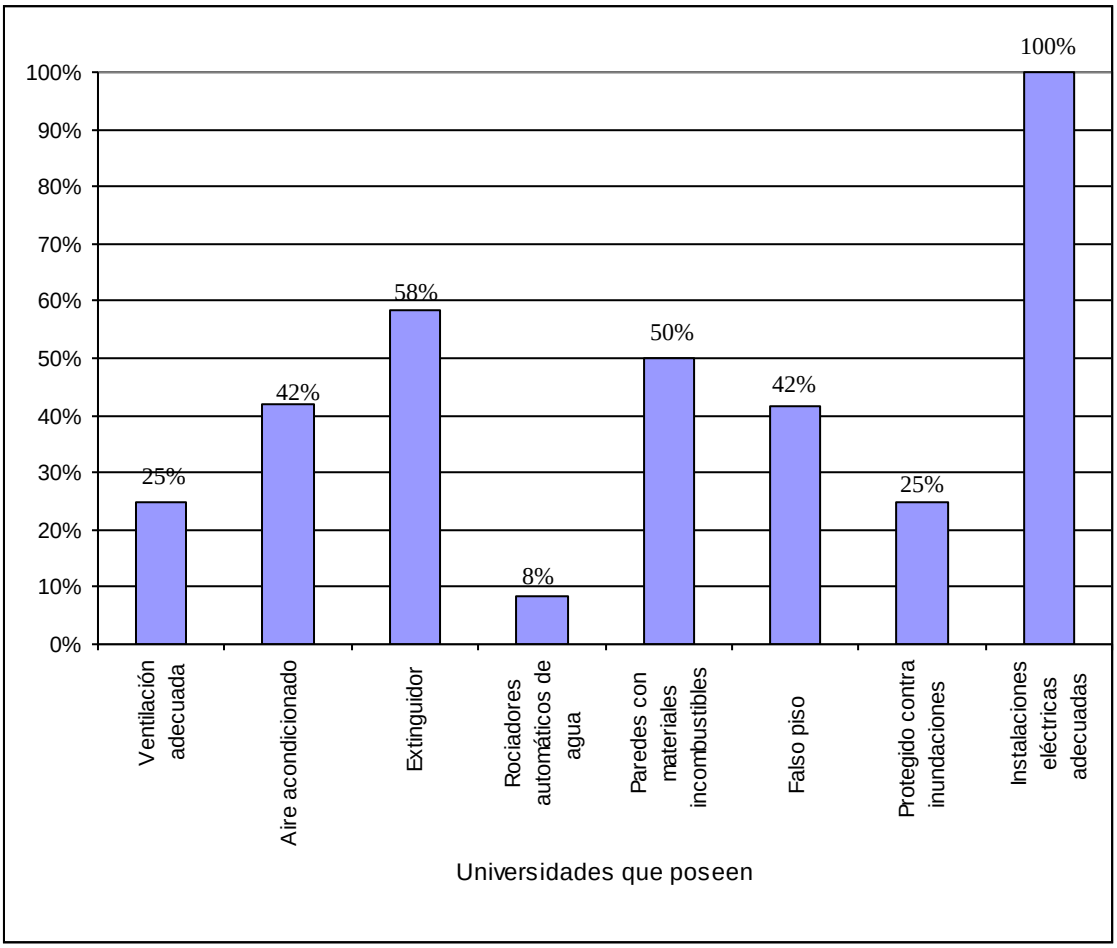


Figura 3.3 Ambiente del Centro de Cómputo

Los incendios son una de las principales amenazas contra la seguridad de los equipos de computación porque destruye fácilmente los archivos de información y programas, razón esta que ha llevado a la mitad de las Universidades ha construir las paredes de los centros de cómputo con materiales no inflamables y al 42% de ellas a construir pisos falsos con materiales resistentes al fuego.

El 58% de las Universidades han ubicado extinguidores de fuego en los lugares donde se encuentran los servidores, switches, routers, pero están a su vez descuidando la ubicación de estos en los laboratorios de computación; además el personal que labora en los mismos requiere un

entrenamiento adecuado para que sepan usar; pues en un momento de desastre el no atender a tiempo la emergencia provocaría daños mayores a los esperados.

La protección contra inundaciones ha sido considerada apenas por la cuarta parte de las Universidades, siendo ésta una de las causas mayores de desastres en los centros de cómputo. En ocasiones debido a que se intenta apagar un incendio en los pisos superiores utilizando agua, entonces se provoca inundación por la falta de drenajes adecuados en los pisos inferiores.

El 8.3% de las Universidades utilizan rociadores automáticos de agua, para defenderse de los incendios, estos sistemas deben estar muy bien controlados para que no actúen de forma inesperada y causen daño a los equipos.

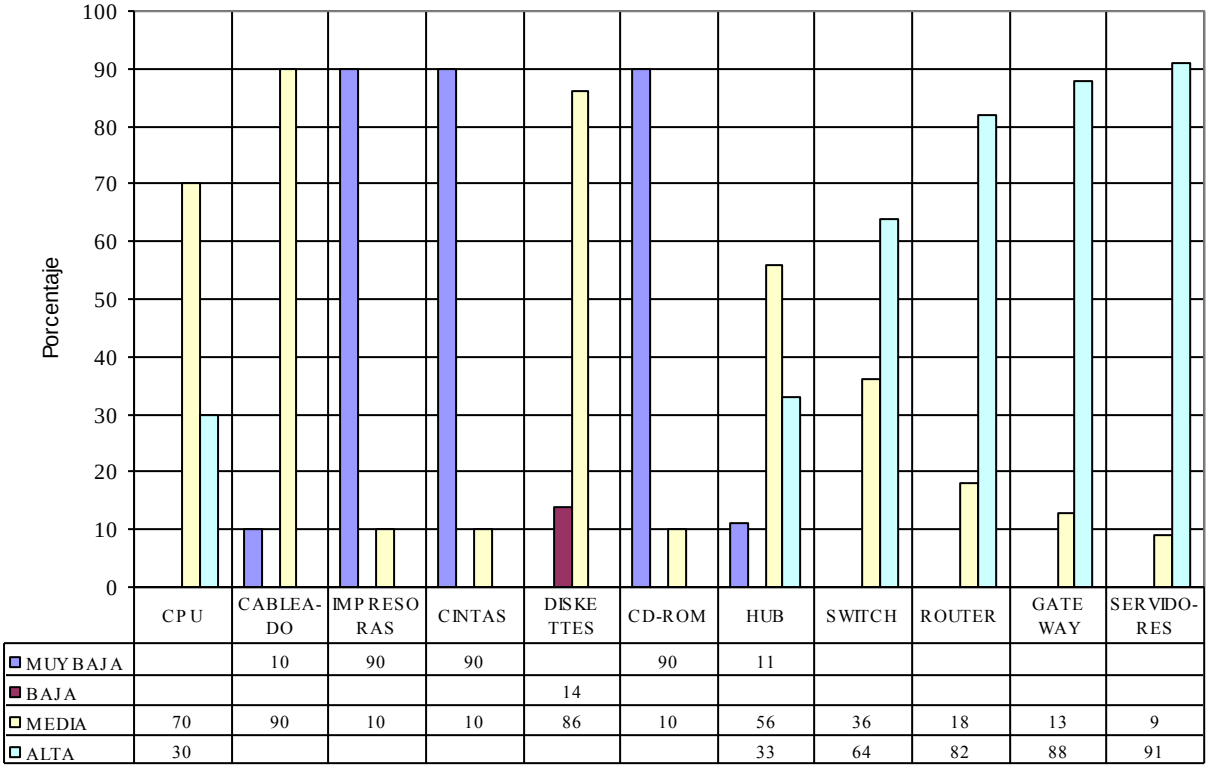
El 100% de las Universidades consideran que las instalaciones eléctricas son las adecuadas, para evitar cortocircuitos, pero a su vez se pudo notar que muchas de ellas no tenían instalaciones de tierra adecuada para contrarrestar sobrevoltajes.

3.1.3 Protección visual

La vista es una de las más afectadas cuando se trabaja en las computadoras por tiempo prolongado, es notorio el cansancio visual, la visión borrosa, la irritación y lagrimeo. El uso de pantallas antirreflejo puede ayudar a resolver en parte los problemas antes mencionados, pero se observa que en el 41% de las Universidades no se las utiliza y de las Universidades que lo utilizan apenas un 8% tiene instalado estas pantallas en la totalidad de sus computadoras.

El 67% de los administradores consideran que la iluminación es la adecuada en sus puestos de trabajo, este aspecto debe ser considerado para evitar la caída de la productividad de las personas al tener dolores de cabeza, molestias con los ojos.

3.1.4 Protección de los dispositivos



	CPU	CABLEA-DO	IMPRESORAS	CINTAS	DISKETTES	CD-ROM	HUB	SWITCH	ROUTER	GATEWAY	SERVIDO-RES
MUY BAJA		10	90	90		90	11				
BAJA					14						
MEDIA	70	90	10	10	86	10	56	36	18	13	9
ALTA	30						33	64	82	88	91

Figura 3.4 Protección de dispositivos

La protección física de los recursos de hardware y su valoración por parte de los administradores de los centros de cómputo universitarios permite identificar la alta importancia que se da al cuidado de servidores (91%), gateways (88%) y routers (82%), dejando en una protección media a los CPUs (70%) y switches (64%). Todo esto está relacionado con las amenazas a las que pudieran estar expuestos estos equipos, el costo operativo que representa su pérdida, los tiempos perdidos y costos de reparación o reemplazo.

La protección que se da a las cintas, CD-ROM, diskettes que contienen archivos y/o contraseñas, no es suficientemente efectiva en las Universidades, para evitar su daño o destrucción total, por la presencia de agua, un incendio, derrumbes de edificios o el robo en el cual muchas veces se utiliza el soborno que constituye un medio fácil y barato si se compara con el tratar de pasar a través del firewall o robar una contraseña cuando el usuario esta en línea y no ser detectado.

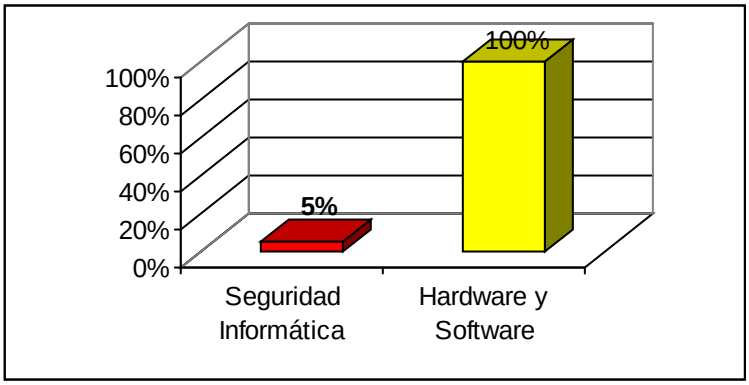


Figura 3.5 Gasto promedio en Seguridad Informática

El estígrafo de posición que representa el valor más típico en cuanto respecta a lo que gastan las Universidades en seguridad informática en relación al gasto total que realizan en equipos y software está por el orden del 5%. Por lo que sería importante que se hagan análisis de riesgos y un estudio de costo-beneficio, para justificar la necesidad de invertir en seguridad, debido a que en la actualidad es muy bajo el presupuesto asignado a la seguridad informática.

3.2 SEGURIDAD LOGICA

3.2.1 Protección del software

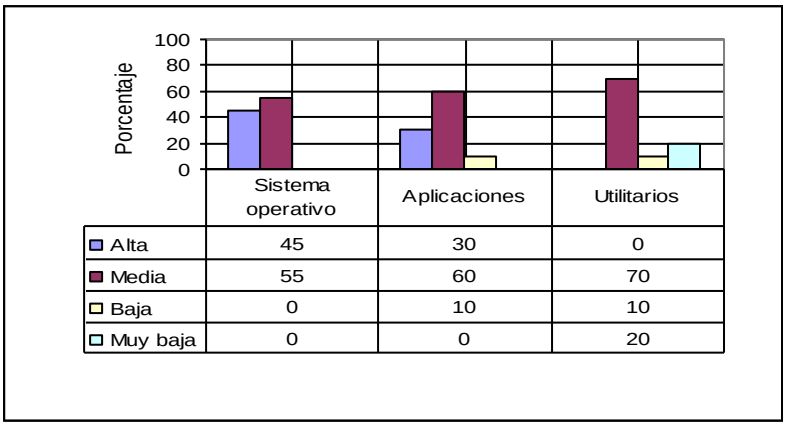


Figura 3.6 Protección del software

El sistema operativo es un conjunto de programas que constituyen la parte central del computador los cuales controlan los sistemas de entrada y salida del mismo, en él están los mecanismos y políticas que ayudan a controlar la manera en que se comparten los recursos del sistema pero se observa que menos de la mitad de las Universidades (45%) dan una protección alta al mismo, y el 55% de las Universidades realizan una protección media quizá basándose en que poseen respaldos del mismo para cuando se produzcan daños.

Una política de seguridad es importante para el manejo del computador con respecto a los usuarios y a la administración del sistema, pues si éste se utiliza sin pensar en la seguridad no puede ser confiable así se le equipe con los programas (aplicaciones) más sofisticados, a los cuales los administradores, no dan la protección requerida pues, el 30% manifiesta dar una protección alta a las aplicaciones y el 60% una protección media.

Por lo que se observa en la figura 3.6, la protección de los utilitarios (editores, filtros, programas de comunicaciones, operaciones con archivos y administración de programas) es media baja, por lo que pueden estar propensas a ser borradas o alteradas sin el permiso correspondiente.

3.2.2 Protección de los datos

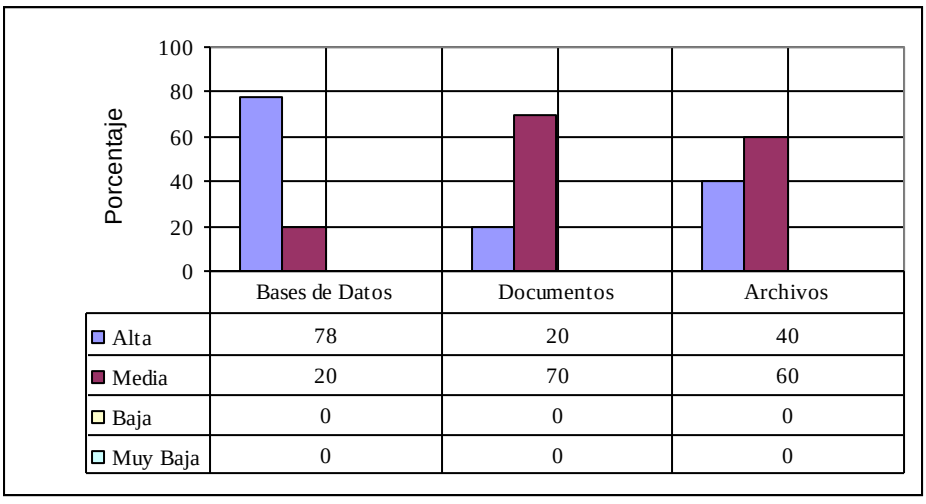


Figura 3.7 Protección a los dato

Al ser intangible el valor de la información tiene sentido en función de cómo y quien procese los datos, por esto la integridad, consistencia, confidencialidad de los mismos es importante para los usuarios. La protección de la información contenida en las bases de datos (78%) tiene alta prioridad en las Universidades aunque no se queda atrás el cuidado que se da a los documentos y archivos que esta entre alta y media, por lo que la realización de auditorias que permitan determinar las acciones o procesos que se están llevando a cabo en el sistema, así como quién y cuando las realizan es fundamental para la seguridad.

La seguridad de los datos en su almacenamiento, utilización, transmisión a través de las redes está siempre relacionado con el correcto funcionamiento del hardware, software, control de virus informáticos y modificaciones que pudiera sufrir por personas infiltradas en el sistema, por lo que los administradores deben tomar en cuenta estos aspectos al buscar seguridad en el manejo de bases de datos, archivos, documentos .

3.2.3 Protección de virus procedentes del Internet

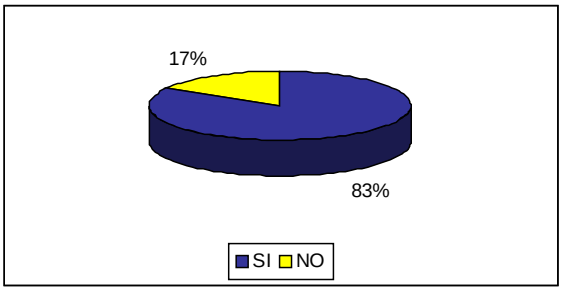


Figura 3.8 Protección contra virus del Internet

Los virus informáticos que en realidad son programas pequeños no detectables por parte del sistema operativo, llevan información suficiente y necesaria para que utilizando mecanismos de ejecución

que le ofrecen otros programas a través del microprocesador puedan lograr reproducirse formando réplicas de sí mismo, son susceptibles de mutar; y dando como resultado de su acción la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados en forma lógica, es por eso que más del 80 % de las Universidades tratan de proteger a sus Intranets del ingreso de virus procedentes del Internet mediante programas antivirus que a través de scanneo buscan eliminar los mismos o mediante procesos heurísticos detectarlos.

Los administradores de las redes universitarias han detectado que los medios de propagación de virus más comunes es el correo electrónico, las páginas web y archivos transferidos vía FTP, por lo que las políticas de seguridad deben ir encaminados a disminuir en lo posible este aspecto, mediante la concienciación de los usuarios.

Hay un mínimo de Universidades que constituyen un 17% que no dan a sus redes, ni usuarios protección contra el ataque de virus, quizá esto se debe a que consideran que existe un tiempo perdido durante la búsqueda de virus en los diferentes archivos que manipulan los usuarios.

3.3 DELITOS INFORMATICOS

3.3.1 Amenazas de personas

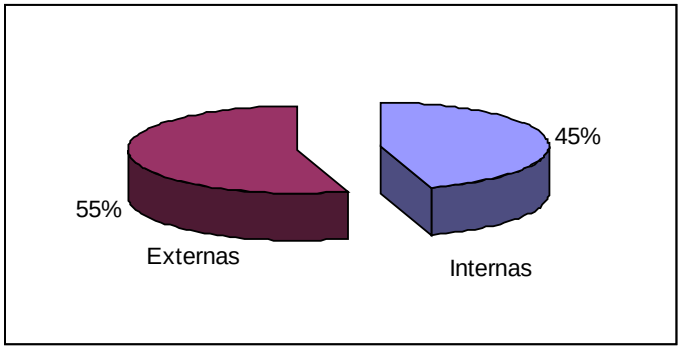


Figura 3.9 Amenazas Externas e Internas

En las Universidades los ataques de personas se considera que pueden venir un 54% procedentes del exterior y el resto desde el personal propio que utiliza su red interna. Se puede observar una tendencia a considerar que se debe tener una mayor protección ante ataques remotos lógicos y tener una seguridad física para evitar sufrir daños.

En la realidad hay que tomar más en cuenta los ataques que proceden del propio personal, debido muchas veces a la deshonestidad, descuidos y errores, que causan daños a los sistemas. Esto se debe a que las personas que trabajan con el administrador, programador o encargado de las máquinas tienen conocimientos del sistema, de sus puntos débiles y fortalezas, un ataque de estas personas puede ser más directo, difícil de detectar y más efectivo que el proveniente de un atacante externo, en esto también se incluye al personal que es despedido de su puesto de trabajo.

Constantemente se pudo observar en las entrevistas al personal que trabaja en los laboratorios, centros de cómputo; quejarse por los daños que son ocasionados por los usuarios de las computadoras (estudiantes) siendo estos ataques en la mayoría de ocasiones accidentales por desconocimiento o inexistencia de normas básicas de seguridad, pero también están los daños hechos intencionalmente.

En las Universidades existen estudiantes que tienen interés en las nuevas tecnologías pero que aun no tienen los conocimientos o experiencia de los hackers que intentan penetrar en los servidores de su Facultad o de otras Facultades de su Universidad, estos ataques muy pocas veces intenta dañar pero afectan la fiabilidad, confiabilidad del sistema.

Las Universidades en un 67%, como se puede observar en la figura 3.9 han experimentado algunos tipos de ataques como la toma del control de un Servidor Unix, daños al servidor DNS y al Web-Sever, daño del servidor principal con la anulación de los protocolos TCP/IP, intento de robo de información del correo electrónico y de direcciones IP, alteración del sistema operativo, denegación de servicio al servidor Web, ataque activo interno, denegación del servicio SQL.

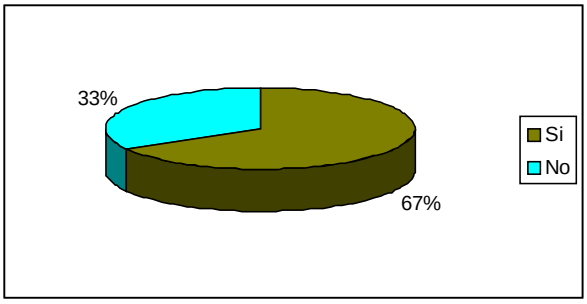


Figura 3.10 Ataques experimentados

3.3.2 Posibilidad de recuperar los recursos perdidos o dañados

Menos de la quinta parte de las Universidades tienen los recursos para comprar un nuevo hardware ante su perdida, realizar cambio de piezas y adquisición de software ante daños, estas Universidades que pueden hacer está inversión son Particulares y se les podría catalogar de elite en lo referente a recursos económicos.

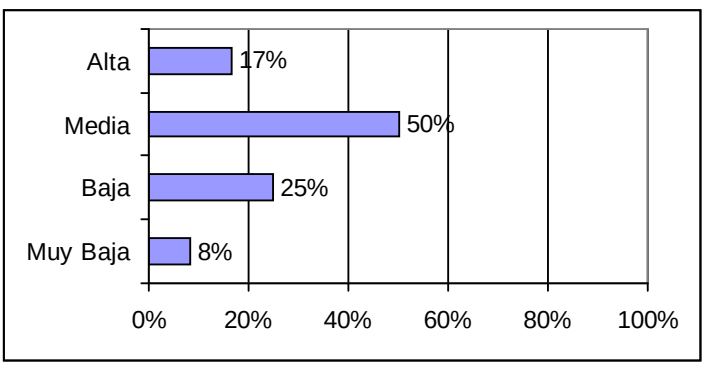


Figura 3.11 Recuperación de recursos perdidos o dañados

El 75% de las Universidades ante las circunstancias señaladas anteriormente tienen que improvisar, buscar de alguna forma trabajar tratando de mantener en lo posible los servicios disponibles para sus usuarios, hasta realizar los tramites de adquisición que demoran un buen tiempo debido a la falta de recursos y a los trámites burocráticos. En ocasiones para un grupo de Universidades sobre todo Estatales que no cuentan con recursos económicos que les permita solucionar estos problemas, se vuelve casi imposible enfrentarlos, pues no cuenta ni siquiera con el dinero para renovar los equipos obsoletos y comprar software legítimo.

3.4 ADMINISTRACION DE LA RED

3.4.1 Monitoreo

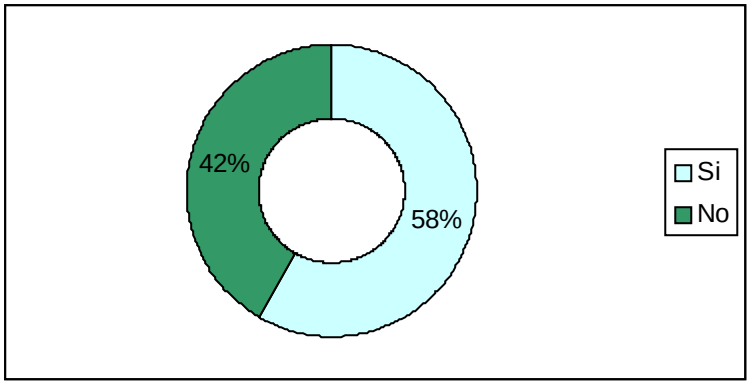


Figura 3.12 Realización de monitoreo de la Red

El 58% de las Universidades realizan monitoreo a nivel de su firewall para determinar si existen personas desde el exterior de su red que desean ingresar y manipular los recursos de su sistema. El monitoreo a este nivel es necesario debido a que los protocolos de comunicación utilizados que

comúnmente son TCP/IP carecen en su gran mayoría de seguridad, existen agujeros de seguridad en los sistemas operativos y en las aplicaciones, se comenten errores durante la configuración de los sistemas que hacen vulnerable al mismo.

El monitoreo es también necesario porque al producirse un ataque la información que no tenía defectos pasa a tenerlo, servicios que deben estar disponibles no lo están, los datos se pierden y no llegan a su destino.

Los atacantes utilizan diferentes técnicas contra las redes Universitarias entre ellas las más frecuentes son: ingeniería social, trashing, monitorización, autenticación , denegación de servicio y modificación este último utilizando lenguajes de programación como java, javaScript, VBScript, ActiveX.

3.4.2 Permisos de acceso al Internet

El 83% de los administradores han definido los usuarios o grupos que tienen permisos de acceso al uso de las diferentes aplicaciones que están activadas entre los servicios que se prestan a través del Internet, utilizando los derechos de acceso que le ofrecen los sistemas operativos.

Esto se debe a que al existir protocolos a nivel de la capa de aplicación que son inseguros como FTP, Telnet etc.; se deben determinar estrategias que hagan seguro el uso de estos protocolos, y evitar el ingreso de usuarios ilegítimos mediante la falsificación.

3.4.3 Métodos empleados para la protección

Las tres cuartas parte de las Universidades realizan análisis de las bitácoras que permiten la búsqueda de patrones de comportamiento o eventos que puedan considerarse sospechosos, partiendo de la información con la que han sido previamente alimentados estos archivos.

El 75% de las Universidades utilizan monitorización de las conexiones que se intentan establecer en sus redes o equipos particulares; esto permite establecer el origen y destino de las conexiones, los servicios que son solicitados, y si las conexiones cuentan con los permisos necesarios para en función de esto tomar acciones que van desde el rechazo de la conexión hasta poner en alerta a los administradores.

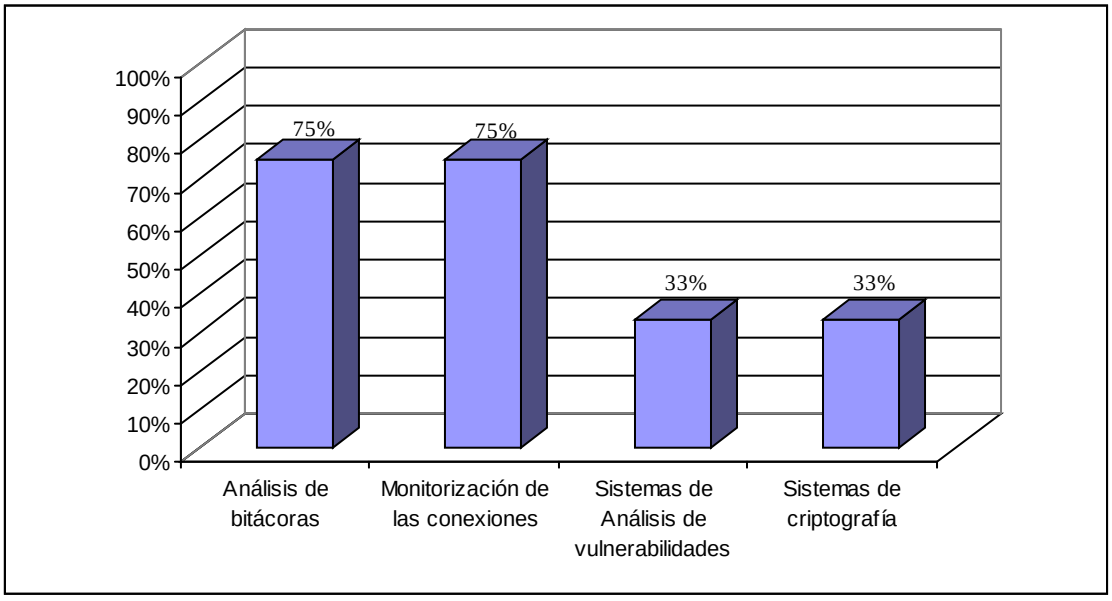


Figura 3.13 Métodos para la protección de la red

El 67% de las Universidades no realizan análisis de vulnerabilidad que permitiría encontrar agujeros en el sistema anticipadamente; éstos análisis se deberían efectuar debido a que son utilizados por personas que buscan acceso no autorizado al sistema

El 33% de las Universidades utilizan criptografía para impedir las alteraciones indeseadas en la información y asegurar que la misma sea visible por quien tiene autorización. En la actualidad existen varias herramientas que utilizan criptografía y se emplean en las en estas Instituciones de educación superior como: Pretty Good Privacity (PGP), Secure Sockets Layer (SSL), IpSec. Algo que aun no se utiliza en las Universidades son los certificados digitales.

3.4.4 Equipo de respuesta a incidentes

El 75% de las Universidades poseen personas encargadas de prestar su ayuda ante eventos que se puedan dar a nivel de la red y de los sistemas. Estos grupos de trabajo son importantes para el buen desempeño de las redes en la parte física y lógica pues acuden ante problemas que se suscitan, y dan solución de forma rápida, permitiendo de esta manera que se pueda seguir trabajando de forma eficiente.

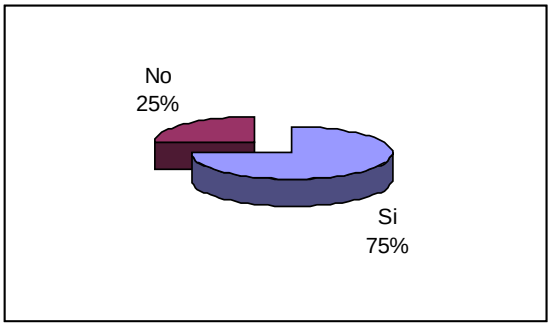
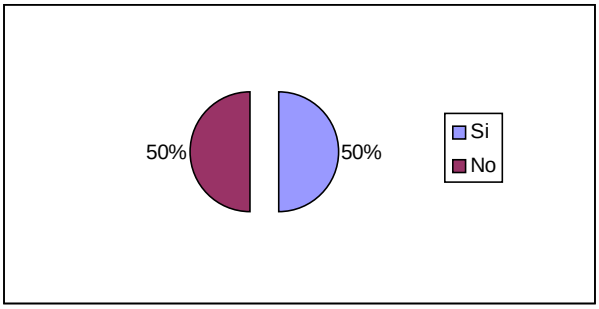


Figura 3.14 Conformación de un equipo de respuesta a incidentes

Estos grupos deben tener un plan de trabajo para problemas que siempre se están produciendo en la red y que afectan su desempeño o para cuando se producen desastres. Se pudo observar que la mitad de las Universidades poseen un plan que les permite recuperarse de desastres para cuando falle el sistema, con el objetivo de restaurar el servicio de computo de manera rápida, y con el menor costo y pérdidas posibles.

Pero también se observó la falta o la no utilización de medios de comunicación entre los administradores de la redes Universitarias tales como: mensajes de correo que aparezcan en la



pantalla de los administradores, telefonía IP o telefonía pública, que les permita mantener un contacto permanente entre ellos, para solucionar problemas que se van presentando en las redes.

Figura 3.15 Existencia de un plan de contingencia

3.5 HARDWARE

3.5.1 Normas de cableado

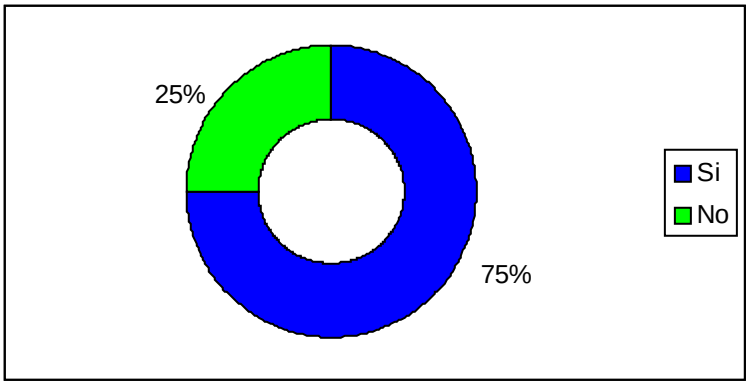


Figura 3.16 Utilización de normas para el cableado

Cada vez más Universidades tratan de emplear las Normas de Cableado Estructurado, que permitan cubrir las necesidades y requisitos de todos los posibles usuarios, así como también poder realizar

las modificaciones y ampliaciones necesarias que den soporte a cualquier servicio de transmisión actual o futura; de tal manera que se pueda incorporar novedades tecnológicas durante un período mínimo de 10 años, sin necesidad de volver a cablear. El utilizar normas de cableado estructurado ha permitido además que sea más sencilla la administración y el mantenimiento de la red.

El tratar de implantar las recomendaciones y estándares internacionales (ANSI/EIA/TIA-569 Norma para rutas y espacios de telecomunicaciones, ANSI/EIA/TIA-606 Norma de administración de la infraestructura de telecomunicaciones, ANSI/EIA/TIA TSB-67 Especificaciones de rendimiento de transmisión para pruebas de campo de sistemas de cableado UTP) en su totalidad se ha constituido en una gran dificultad, debido a que estas son muy exigentes, por lo que se han realizado adaptaciones de acuerdo a las posibilidades del medio o se han obviado.

El cable utilizado en la actualidad en las Universidades es UTP categoría 5 con al norma ANSI/EIA/TIA-568-A (Norma para cableado de telecomunicaciones), siendo la configuración más empleada la T568B de las dos que existen.

3.5.2 Enlace al Internet

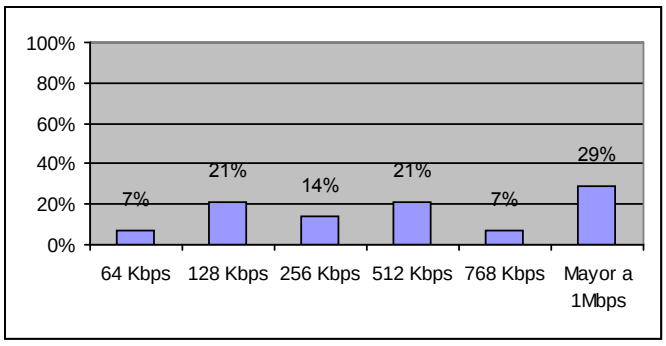


Figura 3.17 Ancho de banda

Se puede clasificar en 3 grupos de Universidades en función del ancho de banda que están utilizando para sus enlaces al Internet como lo muestra la Tabla 3.1

Tabla 3.1 Porcentaje de Universidades en función del ancho de banda

Enlace	Porcentaje
64 Kbps - 256 Kbps	43%
512 Kbps - 768 Kps	28%
> = 1 Mbps	29%

De esta clasificación se deduce que existe un 57% de Universidades que poseen enlaces que van desde los 512 Kbps hasta 1.4 Mbps. Estos enlaces se pueden considerar de muy buena calidad para trabajar en Internet, pero no se pudo determinar en los procesos de entrevista la forma como fue calculado en función de las necesidades de las Universidades.

Estas Universidades a su vez han considerado que la mejor opción para poder acceder a los servicios del Internet es una conexión satelital, que les permita llegar directamente a un conmutador ubicado en los Estados Unidos. Así mismo estas Instituciones de educación superior tienen gran cantidad de usuarios (sobre los 3000 estudiantes, más los profesores) por lo que las necesidades son cada vez mayores.

Las otras Universidades que tienen enlaces inferiores a los 512 Kbps son pequeñas en función del número de usuarios del Internet por lo que no requieren grandes anchos de banda, para dar servicio a profesores, estudiantes y empleados.

A las Universidades en la actualidad se les puede considerar como consumidores de lo que ofrece el Internet más no expositores de sus trabajos científicos. Por lo que estos no son conocidos en el ámbito mundial, esto es muy notorio al revisar sus páginas Web y al observar que muchas de ellas

tienen un ancho de banda inferior para enviar su información hacia el Internet, del ancho de banda que utilizan para bajar la información.

3.5.3 Redes internas universitarias

La tecnología más utilizada en las redes internas Universitarias es Ethernet (93%), esto se debe a los costos de inversión requeridos frente a tecnologías como ATM, y por la facilidad de poder ir emigrando a las versiones más actualizadas que ofrecen mejor ancho de banda y calidad de servicio.

Tabla 3.2 Tecnologías empleadas

ANCHO DE BANDA	TECNOLOGIA	PORCENTAJE
10 Mbps	Ethernet	23%
10 -100 Mbps	Fast Ethernet	62%
100 - 1000Mbps	Giga Ethernet	8%
155 Mbps	ATM	7%

Como se observa en la tabla 3.2 el 83% de las Universidades utilizan en la actualidad 10 Mbps como su ancho de banda para transmitir o recibir información a través de su red interna, por lo que aplicaciones desarrollas por estas Universidades son mínimas o no existen.

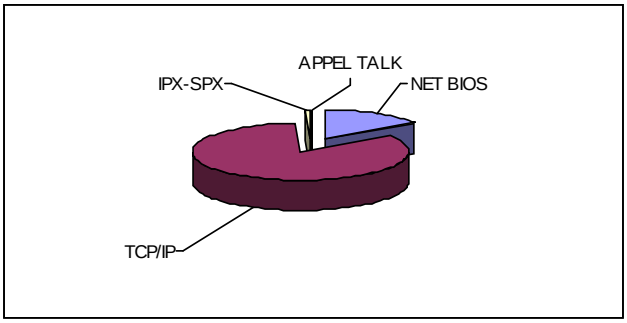
Más del 60% de las Universidades ha ubicado switch Fast Ethernet a nivel del backbone para mejorar el manejo de información procedente de cada una de sus subredes de Facultad.

Gigabit Ethernet esta empezando a ser empleada a nivel de backbone, por su alta perfomance comparada con ATM, porque permite aumentar el tráfico de múltiples switch de más baja velocidad hacia el router.

La tecnología ATM se podría decir que ha sido casi totalmente desplazada por la tecnología Ethernet y solo está siendo empleada a nivel de switch principal en backbones de configuración colapsada para mejorar las velocidades de manejo de la información y evitar en lo posible los cuellos de botella.

3.6 SOFTWARE

3.6.1 Protocolos utilizados



PROTOCOLO	PORCENTAJE
NET BIOS	15.41
TCP/IP	83.67
IPX-SPX	0.88
APPEL TALK	0.04

Figura 3.18 Protocolos utilizados

El protocolo más utilizado en la actualidad a nivel de redes Universitarias es TCP/IP (83.67%) debido a que posee un conjunto de protocolos que pueden especificarse en todas las redes y permiten simplificar los procesos. Mediante estos protocolos se puede integrar equipos de distintos fabricantes, proporcionando conexiones fiables y de alto rendimiento .

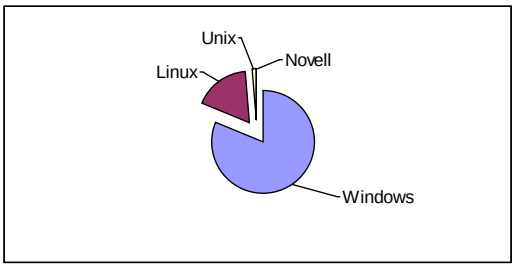
TCP/IP es muy utilizado porque es fácil configurar con él las redes y añadir o eliminar computadoras sin interrumpir las comunicaciones; además es el protocolo de Internet por lo que continuamente evoluciona en función de los avances que se van produciendo en Internet. Este conjunto de protocolos es el único disponible sin costo alguno y está definido en un entorno totalmente público.

El segundo protocolo en importancia es el protocolo de tramas NetBIOS (15.41%) utilizado por la mayoría de los programas para redes de Microsoft, pues constituye el API tradicional de los productos de red de Microsoft .

Estos protocolos deben ser tratados bajo la óptica de la seguridad debido a que muchos de los ataques se basan en las fallas que poseen y que convierten en inseguras a las redes Universitarias sino se toman las precauciones correspondientes.

3.6.2 Sistemas operativos

El sistema operativo más utilizado en las Universidades Ecuatorianas es Windows (81.44 %) en sus diferentes versiones (Windows: 95, 98, milenium, XP, NT, 2000), esto se debe a que su instalación, mantenimiento y ejecución es sencilla comparando con los otros sistemas operativos, y las personas que son parte de las Universidades están bastante familiarizados con su utilización. Pero las continuas fallas de seguridad que presenta a hecho que los administradores desconfíen, sobre todo cuando se lo debe utilizar para servidores.



SISTEMA OPERATIVO	PORCENTAJE
Windows	81.44
Linux	17.17
Unix	1.38
Novell	0.02

Fig. 3.19 Empleo de Sistemas Operativos

El uso de Unix tanto en su versión para PC, como en sus versiones propietarias que viene como un todo formado por hardware y software no llegan al 20%; esto se debe a que sus aplicaciones a nivel

de cliente no han sido muy difundidas y se observa una cierta resistencia a su utilización aun cuando cada vez tiene mejores interfaces gráficas, por lo que su empleo se lo ha dejado para el uso en servidores donde ha demostrado una alta perfomance.

Los sistemas operativos Unix se consideran más seguros y confiables que los sistemas operativos Windows pero también tienen sus problemas de seguridad que deben ser tomados muy en cuenta por los administradores de las redes Universitarias, para evitar sorpresas desagradables.

3.6.3 Realización de respaldos

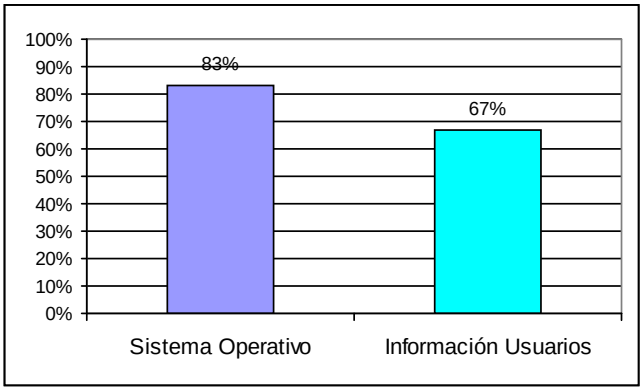


Figura 3.20 Información respaldada

Los respaldos permiten comparar el sistema actual con el sistema respaldado, para de ahí poder proceder a restaurar el sistema a un estado estable.

Se puede observar que el 83% de las Universidades le dan importancia a la protección de los Sistemas Operativos y poseen respaldos de los mismo para cualquier emergencia; pero así mismo se deducir de la figura 3.20 que no se le da similar importancia a los respaldos de la información de los usuarios, que si se hace un análisis profundo se puede llegar a determinar que más importante es tener respaldos de los datos de los usuarios

que de los Sistemas Operativos; pues ante la situación de pérdida o daño de estos últimos se podría comprar, lo que no podría hacerse con los datos de los usuarios.

Los respaldos son importantes porque se pueden producir errores por parte de los usuarios que accidentalmente borren sus archivos, también puede existir errores por parte del personal encargado del sistema que al borrar cuentas antiguas borre una cuenta activa; las debidas a fallas de hardware que a menudo destruyen datos; las que se producen porque los programas de aplicación debido a defectos de programación destruyen datos, y también es importante si se considera que se esta expuesto al vandalismo y desastres naturales; por lo que implementar un plan de respaldos permitirá determinar la forma y momentos en que se obtendrán los mismos y de esta manera mantener de forma segura la información.

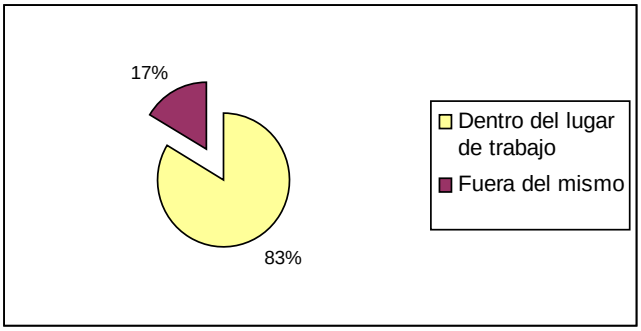


Figura 3.21 Lugar de almacenamiento de los respaldos

En el 83% de las Universidades los respaldos se ubican dentro del lugar de trabajo, esto podría ser causa de su destrucción si se produjese un desastre que afectase al sitio; pues además de destruirse el equipo que contiene la información se destruirían los respaldos. Idealmente los respaldos se debería mantener lejos del lugar donde se encuentra el sistema (centro de cómputo) para que un desastre en dicho lugar no afecte a ambos.

La seguridad física de los respaldos debe observarse ubicándose los mismos en lugares estratégicos con la protección adecuada que impida sean sustraídos o manipulados por personas sin autorización.

3.6.4 Integridad de los datos

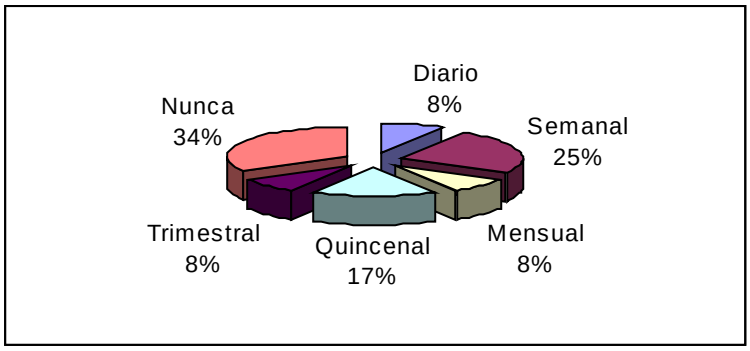


Figura 3.22 Verificación de la integridad de los datos

Existe un 34% de Universidades que jamás realizan una verificación de la integridad de los datos (registros contables, cintas de respaldo, la hora en que fueron creados los archivos y la documentación) por lo que no podrían determinar ni evitar el momento en que se borre o altere la información sin el permiso del dueño.

Un 8% realiza verificación de los datos trimestralmente y otro 8% mensualmente, que tampoco se podría considerar que se esta haciendo lo adecuado. Pues lo aconsejable sería hacerlo diariamente o máximo cada semana como lo realizan el 25% de las Universidades.

Para ayudar a mantener la integridad de los datos los administradores de las redes Universitarias en lo que más deberían poner énfasis, es en el establecimiento de los permisos apropiados de archivos y directorios, la restricción de acceso a la cuenta root, como el control de acceso a servicios remotos con los que cuentan algunas Universidades.

Se pudo observar que 8% de las Universidades realizan detección de cambios a través del monitoreo de la integridad de los datos, que les permite descubrir cambios maliciosos, violación de las políticas

establecidas, posibles fallas de los equipos, errores en los programas y presencia de virus en las computadoras.

3.7 FIREWALLS

De la manera como se ha organizado Internet cada sitio debe asumir la responsabilidad de su propia seguridad, es esta la razón por la que el 92% de las Universidades utilizan firewalls para mantener el tráfico no deseado y sin autorización procedente de Internet fuera de su red privada LAN, pero a su vez permiten que los usuarios de la red local Universitaria tengan acceso a los servicios de Internet.

Los Firewalls más sencillos en las Universidades han sido construidos basados en la configuración adecuada de los routers y estableciendo las listas de no acceso IP.

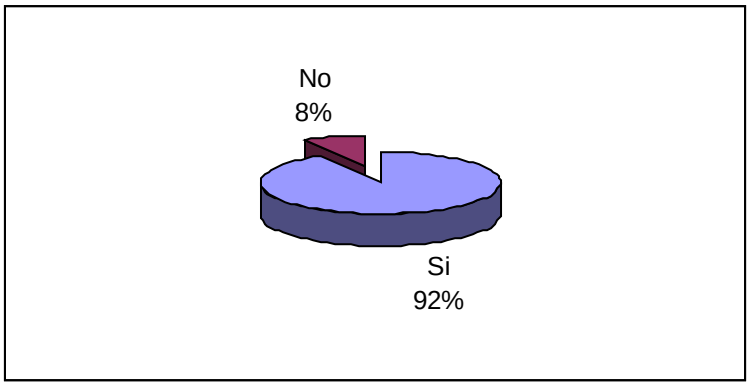


Figura 3.23 Utilización de Firewalls

Para la construcción de firewalls mediante un servidor proxy se está empleando en las Universidades el Sistema Operativo Unix, Linux donde se hace un control mediante IPTABLES , IPCHAINS , SQUID, también se emplean productos hardware como 3COM firewall, Winroute, Sun Screen, y además se configura listas de control de acceso (ACLs).

Algunas Universidades tienen instalado en el firewall herramientas de rastreo, las cuales permiten tener bitácoras para determinar el origen de las conexiones que entran, la cantidad de tráfico que tiene su servidor e incluso si existió algún intento de forzarlo.

Mediante los firewalls restringn los administradores de las redes Universitarias ciertos servicios que son considerados peligros por la falta de seguridades (telnet, ftp) o por que consumen demasiado ancho de banda (chat) o son sitios que se asume no deben ser visitados por los usuarios y se ubican restricciones; pero a su vez esto provoca el malestar en los usuarios quienes requieren estos servicios por lo que debería existir políticas de seguridad que permitan un adecuado uso de los mismos, sin perjudicar el aspecto de seguridad de la red.

3.8 SERVICIOS DE RED

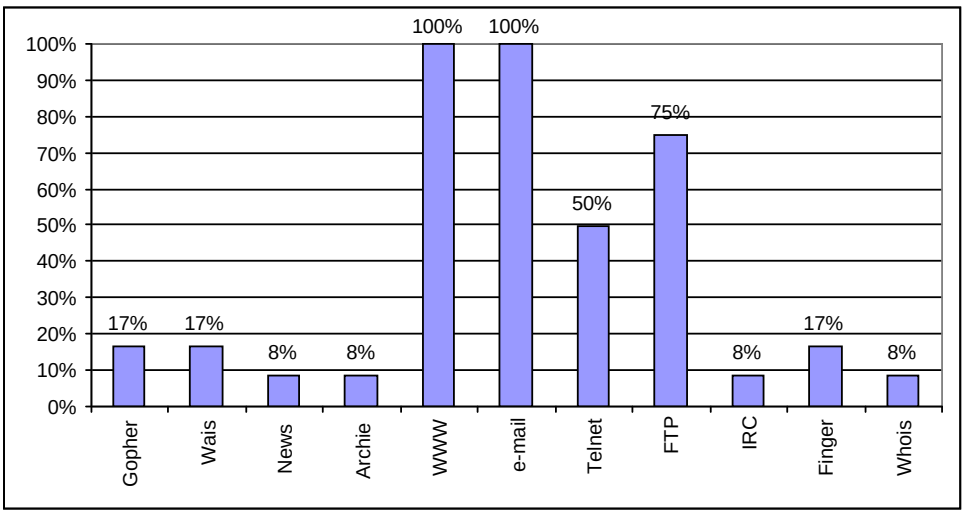


Figura 3.24 Servicios de Internet

Existen dos servicios que todas las Universidades en la actualidad ofrecen que son el acceso a la WWW y el servicio de correo electrónico, pero este último en la mayoría de Universidades esta destinado solo a los profesores y administradores de la red, casi a los estudiantes y empleados en general no se lo da.

El auge que en los últimos años viene teniendo la WWW ha hecho que otros servicios como Gopher, Archie , hayan caído casi en total desuso.

El servicio finger, whois, wais esta restringido en casi todas las Universidades y aquellas que lo tienen en su mayoría solo pueden ser utilizados por los administradores, pues se consideran que son peligros al ser softwares que entregar información referente a la red.

El servicio de news apenas el 8% de las Universidades lo ofrecen , lo que constituye un error pues, mediante este servicio los usuarios de las redes Universitarias, podrían tener información actualizada de los temas que les interesa conocer y que a su vez serían un aporte para la investigación, que debe ser parte de los centros de educación superior.

El servicio de Telnet es ofrecido por la mitad de Universidades y el servicio FTP por el 75% de éstas, en aquellas Instituciones que se ofrece estos servicios se restringe su utilización a la mayoría de usuarios, teniendo el privilegio de usarlos solo ciertos usuarios como por ejemplo los administradores o determinados profesores que requiere trabajar con estos servicios y que son de confianza; esto se debe a la falta de seguridad existente en su utilización, y porque se teme ataques de los hackers, e incluso que un intruso pueda intervenir las líneas de comunicación del sitio y hacer daño.

3.9 ANALISIS DE RESULTADOS

En los temas tratados anteriormente en este capítulo se ha podido ir determinando las falencias en seguridades que tienen las Universidades ecuatorianas y que constituyen fuertes razones para la utilización de políticas y procedimientos de seguridad.

Para la comprobación de la hipótesis de investigación se emplea la prueba estadística denominada chi cuadrado χ^2, que es una prueba no paramétrica que atiende a un ordenamiento de los datos independientes de los valores numéricos o de datos nominales u ordinales.

La ecuación para determinar el valor de χ^2 es la siguiente:

$$\chi^2 = \Sigma \frac{(f_o - f_e)^2}{f_e}$$

fo = frecuencia observada

fe = frecuencia esperada

3.9.1 Presentación de resultados

El grupo con el que se trabaja en la investigación esta conformado por los Administradores Principales de las redes Universitarias Ecuatorianas (Universidades públicas y privadas; y Escuelas Politécnicas) quienes conocen el funcionamiento del backbone. Este grupo esta conformado por 25 administradores y las preguntas del cuestionario fueron comunes para todos.

Tabla 3.3 Presentación de resultados de preguntas a los Administradores

PREGUNTAS A LOS ADMINISTRADORES	1	%	2	%	3	%	4	%
Evitar modificación del flujo de datos	19	75	0	0	0	0	6	25
Gasto en seguridad	0	0	2	8.33	17	66.67	6	25
Ataques desde el exterior	2	8.33	6	25	17	66.67	0	0
Ataques desde el interior	0	0	6	25	19	75	0	0
Experimentación de ataques	17	66.67	0	0	0	0	8	33.33
Uso de software de seguridad	19	75	0	0	0	0	6	25
Utiliza extinguidor	15	58.33	0	0	0	0	10	41.67
Rociador automático de agua	2	8.33	0	0	0	0	23	91.67
Material incombustible en paredes	12	48	0	0	0	0	13	52
Piso falso instalado	10	41.67	0	0	0	0	15	58.33
Protección contra inundaciones	6	25	0	0	0	0	19	75
Adecuadas instalaciones eléctricas	25	100	0	0	0	0	0	0
Cableado bajo estándar	19	75	0	0	0	0	6	25
Uso de ventilación	6	25	0	0	0	0	19	75
Uso de aire acondicionado	10	41.67	0	0	0	0	15	58.33

Uso de pantallas antireflejo	2	8.3	2	8.3	4	16.7	17	66.7
Iluminación adecuada	17	66.7	0	0	0	0	8	33.3
Control de acceso servicio vigilancia	12	48	0	0	0	0	13	52
Control con formularios de datos personales	8	33.3	0	0	0	0	17	66.7
Control con credenciales de identificación	8	33.3	0	0	0	0	17	66.7
Control mediante password	2	8.33	0	0	0	0	23	91.67
Control con sistema biométrico	2	8.33	0	0	0	0	23	91.67
Control de acceso de vehículos	15	58.33	0	0	0	0	10	41.67
Protección electrónica por ultrasonido	6	25	0	0	0	0	19	75
Detectores de roturas de vidrios	2	8.33	0	0	0	0	23	91.67
Detectores de vibraciones	8	33.3	0	0	0	0	17	66.7
Circuito cerrado de televisión	2	8.33	0	0	0	0	23	91.67
Sensores de movimiento	2	8.33	0	0	0	0	23	91.67
Posibilidad de recuperar recursos perdidos	4	16.67	12	48	7	27	2	8.33
Protección CPU	6	25	19	75	0	0	0	0
Protección cableado	0	0	23	91.67	0	0	2	8.33
Protección impresoras	0	0	19	75	0	0	6	25
Protección cintas	0	0	13	52	0	0	12	48
Protección diskettes	0	0	13	52	2	8.33	10	39.67
Protección CO-ROM	0	0	17	66.67	0	0	8	33.33
Protección HUB	8	33.33	14	55.56	0	0	3	11.11
Protección Switch	16	63.63	9	36.37	0	0	0	0
Protección Routers	20	80	5	20	0	0	0	0
Protección Gateway	22	88	3	12	0	0	0	0
Protección servidores	22	88	3	12	0	0	0	0
Protección Sistema Operativo	11	45	14	55	0	0	0	0
Protección Aplicaciones	7	30	15	60	3	10	0	0
Protección Utilidades	0	0	17	70	3	10	5	20
Protección Base de datos	19	77.78	6	22.22	0	0	0	0
Protección Documentos	8	33.33	17	66.66	0	0	0	0
Protección Archivos	10	40	15	60	0	0	0	0
Control de materiales fungibles	17	66.66	0	0	0	0	8	33.34
Monitoreo para detectar extraños	14	58.33	0	0	0	0	11	41.67
Definido permisos acceso Internet	21	83.33	0	0	0	0	4	16.67
Definido permisos acceso FTP	23	91.16	0	0	0	0	2	8.84
Definición del acceso a aplicaciones en función del Usuario	17	66.66	0	0	0	0	8	33.34
Emplea algún estándar de seguridad informática	0	0	0	0	0	0	25	100
Utilización de NetBIOS	0	0	10	41	15	59	0	0
Utilización de TCP/IP	21	83.33	4	16.67	0	0	0	0
Utilización de Windows	10	41.66	13	50	2	8.34	0	0
Utilización de Linux	0	0	2	8.33	15	58.33	8	33.34
Utilización de Unix	0	0	0	0	2	8.33	23	91.67
Servicio FTP ofrecido	19	75	0	0	0	0	6	25
Servicio WWW ofrecido	25	100	0	0	0	0	0	0
Servicio e-mail ofrecido	25	100	0	0	0	0	0	0
Servicio Telnet ofrecido	12	48	0	0	0	0	13	52
Servicio finger ofrecido	4	16.66	0	0	0	0	21	83.34
Servicio Gopher ofrecido	4	16.66	0	0	0	0	21	83.34
Servicio Wais ofrecido	4	16.66	0	0	0	0	21	83.34

Servicio Usenet ofrecido	2	8.33	0	0	0	0	23	91.67
Servicio de IRC ofrecido	2	8.33	0	0	0	0	23	91.67
Utilización de políticas para evitar el ingreso de virus desde el Internet	21	83.33	0	0	0	0	4	16.67
Análisis de bitácoras	19	75	0	0	0	0	6	25
Monitarización de conexiones que se tratan de establecer	19	75	0	0	0	0	6	25
Análisis de vulnerabilidades	8	33.33	0	0	0	0	17	66.67
Utilización de Sistemas de criptografía	8	33.33	0	0	0	0	17	66.67
Utilización de suma de verificación	0	0	0	0	0	0	25	100
Utilización de Test de penetración	4	16.66	0	0	0	0	21	83.34
Utilización de trampas de red	4	16.66	0	0	0	0	21	83.34
Equipo de respuesta a incidentes	19	75	0	0	0	0	6	25
Existe respaldos de los Sistemas Operativos	21	83.33	0	0	0	0	4	16.67
Existe respaldos de la Información de los Usuarios	15	58.33	0	0	0	0	10	41.67
Verificación de la integridad de los datos	2	8.33	8	33.33	7	25.01	8	33.33
Realiza el almacenamiento dentro del lugar de trabajo	21	83.33	0	0	0	0	4	16.67
Emplea firewalls	23	92	0	0	0	0	2	8
Posee plan de recuperación de desastres	12	48	0	0	0	0	13	52
TOTAL	**817**		**287**		**113**		**808**	

La interpretación de la simbología (1, 2, 3, 4) empleada en la tabla 3.3 esta en función del cuestionario utilizado en el proceso de investigación; los valores numéricos que aparecen en estas columnas, constituyen el número de administradores de redes universitarias que contestaron a las preguntas en relación al cuadro siguiente:

1	Si	Alta	Siempre
2		Mediana	Frecuentemente
3		Baja	A veces
4	No	Muy baja	Nunca

3.9.2 Prueba de la hipótesis

La hipótesis se prueba en función de los resultados obtenidos de las encuestas realizadas a los Administradores de las redes. Para la prueba estadística se establece la hipótesis nula H_o y la hipótesis de investigación H_1.

H_o = La operatividad óptima de los sistemas de redes universitarias conectadas al Internet es debido a la falta de políticas y procedimientos de seguridad.

H_1 = La operatividad no óptima de los sistemas de redes universitarias conectadas al Internet es debido a la falta de políticas y procedimientos de seguridad.

Lo que se busca mediante la prueba χ^2 es comprobar si las variables que conforman la hipótesis son independientes, esto constituye probar la hipótesis nula Ho.

Los valores numéricos totales obtenidos de las encuestas se anotan en una tabla de doble entrada, conocida como tabla de contingencia (tabla 3.4).

Tabla 3.4 Matriz de frecuencias observadas en los Administradores

ADMINISTRADORES	**POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD**		
OPERATIVIDAD	**FALTA**	**SI EXISTE**	**TOTAL**
La operatividad no óptima de los sistemas de redes Universitarias conectadas al Internet	817	287	1104
La operatividad óptima de los sistemas de redes Universitarias conectadas al Internet	113	808	921
TOTAL	930	1095	2025

La tabla de contingencia 3.5 , constituye las frecuencias esperadas y se obtiene de la matriz de frecuencias observadas al multiplicar el resultado total de una fila por el total de una columna y dividir para la suma total de las columnas o las filas.

Ejemplo para obtener el valor 507.02: (930 x 1104)/2025 = 507.02

Tabla 3.5 Matriz de frecuencias esperadas en los Administradores

ADMINISTRADORES	POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD		
OPERATIVIDAD	**FALTA**	**SI EXISTE**	**TOTAL**
La operatividad no óptima de los sistemas de redes Universitarias conectadas al Internet	507.02	596.98	1104
La operatividad óptima de los sistemas de redes Universitarias conectadas al Internet	422.98	498.02	921
TOTAL	930	1095	2025

En la tabla 3.6 se realiza el cálculo del valor del ¡ ^{2}

Tabla 3.6 Obtención del valor del ¡ ^{2} Administradores

Fo	fe	fo-fe	(fo – fe) ^{2}	(fo – fe)^2/fe
817	507.02	309.98	96087.60	189.51
287	596.98	-309.98	96087.60	227.17
113	422.98	-309.98	96087.60	160.96
808	498.02	309.98	96087.60	192.94
751	751.00			¡ ^{2} = **770.58**

Cálculo de los grados de libertad (gl) para determinar el ¡ ^{2} tabulado, a partir de la tabla de contingencia:

gl = (Número de filas –1)*(Número de columnas –1)

gl = (2 – 1)*(2 – 1)

gl = 1

De la tabla del χ^2 que se encuentra en el Anexo B, con

gl = grados de libertad 1
α = nivel de confianza 0,05
p = probabilidad del suceso 95%

se obtiene

$\chi^{2\ (1)}_{0.05}$ = 3.841 **chi tabulado**

$\chi^2_{calculado} > \chi^{2\ (1)}_{0.95}$

770.58 > 3.841 **El ¡² calculado es mayor que el ¡² tabulado por lo que se rechaza** Ho

se acepta H_1 **que constituye la hipótesis de investigación.**

CAPITULO IV

PROPUESTA DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD PARA LAS REDES DE LA UNIVERSIDAD ECUATORIANA

4. PROPUESTA DE POLITICAS Y PROCEDIMIENTOS

4.1 PRESENTACION

Las políticas y procedimientos de seguridad para las redes de la Universidad Ecuatoriana están relacionadas con los riesgos que se trata de eliminar. La eliminación de los riesgos es casi imposible en su totalidad, primero por el costo muy alto y segundo porque la mayoría de ocasiones no se justifica.

Por los avances tecnológicos y los conocimientos nuevos, que en la actualidad poseen los usuarios de las redes universitarias, es imposible mantener información oculta. Es solo cuestión de tiempo para que ésta sea conocida.

El administrador, más bien debe tomar otro camino. Utilizar un método organizado que le permita tener seguridad, en la parte física; y mediante el uso de herramientas apropiadas poder mantener la seguridad de su red en la parte lógica.

La presente propuesta de políticas y procedimientos de seguridad para la Universidad Ecuatoriana pretende dar solución a los problemas encontrados dentro del análisis de seguridades realizado en el capítulo III.

En las universidades la integridad y la disponibilidad son los requerimientos más importantes. La red universitaria debe estar a disposición de los estudiantes para que éstos puedan realizar sus trabajos académicos.

4.2 OBJETIVO

Presentar una propuesta de políticas y procedimientos de seguridad para las redes de datos de la Universidad Ecuatoriana, conectadas a la Internet.

4.3 FORMULACION DEL PROBLEMA

La Universidad Ecuatoriana, en un 50%, posee un servicio de vigilancia con personal de la propia institución o contratado en empresas de seguridad; pero, el 50% restante no lo posee; esto implica que el acceso físico a cualquier sitio de la universidad no es difícil, por la extensión del campus que tiene cada una de ellas.

Cuando los centros de cómputo y los laboratorios de las universidades están funcionando en sus horarios regulares de servicio, apenas el 33% de éstos anota en formularios los datos personales de quienes ingresan a sus instalaciones; o solicitan credenciales de identificación, por tanto, ante la pérdida de cualquier dispositivo que se encuentre en los centros de cómputo y laboratorios será difícil investigar y hacer un seguimiento al o a los culpables.

El 41.7% de las universidades carecen de extinguidores por lo que ante un inicio de incendio sería un problema sofocarlo. El 50% de las universidades no tienen paredes construidas con materiales incombustibles. Las instalaciones eléctricas, en el 58.3% están ubicadas en los pisos y sin la protección de un piso falso, por lo que ante la presencia de fuego fácilmente se destruirían.

Los administradores consideran que los equipos de más cuidado en las redes universitarias son los servidores, gateways, routers, switches; pero la inversión que realizan las universidades en seguridad informática en relación con el gasto total que hicieron en equipos y software, está en el orden del 5% que constituye un valor insuficiente.

La mayoría de universidades da una protección media a los sistemas operativos, aplicaciones y utilitarios; esto en un momento dado puede ser causa para ser borrados o alterados, sin la anuencia del administrador.

Aunque el 80% de las universidades ha ubicado sistemas de escaneo de virus es imposible realizar un control total de los mismos, por lo que es necesario tomar medidas que disminuyan su efecto.

Las redes universitarias están expuestas a los ataques provenientes del exterior y del interior. Esto se debe al grupo humano con el que se trabaja que está constituido por usuarios que conocen poco sobre el manejo de la información y las redes; y también expertos que están siempre buscando explorar nuevas opciones.

El 75% de las universidades carecen de recursos para comprar equipos, realizar cambios de piezas o adquirir software, por lo que la protección de lo que poseen es sumamente importante.

El 42% de las universidades no realizan ninguna clase de monitoreo, por lo que puede estar siendo cambiada la información sin el consentimiento, ni conocimiento de los administradores.

Los dos protocolos más utilizados en la Universidad Ecuatoriana son TCP/IP en un 83.67% y NetBios de Microsoft en un 15.41%; y los sistemas operativos de mayor empleo son Windows (81.44%) y Linux (17.17%), por lo que se requiere una especial atención en lo referente a sus problemas y soluciones de seguridad.

El 33% de las universidades no tienen respaldos de la información generada por los usuarios, por lo que su pérdida en un momento de desastre sería total. El 83% de aquellos que realizan respaldos de

la información de los usuarios también lo perderían, por ejemplo en un incendio, porque el almacenamiento se realiza en el mismo lugar donde son generados.

Los servicios que ofrece la Universidad Ecuatoriana son: WWW (100%), correo electrónico(100%), FTP(75%), Telnet (50%), por lo que es necesario establecer las seguridades correspondientes para estos servicios.

4.4 DESARROLLO DE LOS ASPECTOS TECNICOS OPERATIVOS

4.4.1 Políticas de seguridad

Las políticas de seguridad desarrolladas para las Universidades Ecuatorianas contemplan los problemas encontrados; que se buscan solucionar a nivel físico como lógico.

4.4.1.1 Seguridad Física

4.4.1.1.1 Control de acceso al sitio

- El personal de vigilancia ubicado en la puerta de ingreso de las universidades debe asentar en el formulario de datos personales, la información sobre las personas que ingresan con vehículo, para lo cual se solicitará licencia de conducir y matrícula del vehículo.
- Cuando ingresa la gente con equipos a la institución debe hacer un registro de los mismos en la entrada, para su verificación a su salida.
- La mayoría de las universidades tienen grandes extensiones de terreno. Para su vigilancia los guardias deben utilizar perros cuyo costo de cuidado y mantenimiento es muy bajo.
- Verificar que las paredes internas lleguen hasta el techo y el piso, con la finalidad de impedir que algún intruso pase burlando la pared.

- En los lugares que se requiere bastante ventilación los ductos de aire deben ser pequeños en lugar de uno grande, o, si es uno solo debe ser lo suficientemente pequeño para que no pueda pasar una persona a través de ellos.
- Utilizar cerraduras y candados de buena calidad en las puertas de acceso a los centros de computo y laboratorios.
- Proteger los cables de la red haciéndolos pasar por sitios seguros, para evitar su daño y deterioro.
- Para controlar el acceso a los lugares que contienen los equipos de cómputo se deben llenar formularios con los datos personales. Se solicitará a los estudiantes su carné estudiantil y a otras personas la cédula de identidad.
- El personal que trabaja en los centros de cómputo y laboratorios tendrán credenciales que les autorice la permanencia en estos lugares.
- Para el ingreso a lugares que contienen equipos (switches, routers, servidores, etc), que si dejan de funcionar provocarían el colapso de la red, se debe emplear sistemas biométricos para que solo pueda ingresar el personal autorizado.
- Impedir la entrada con alimentos y bebidas, hacia las salas de cómputo y laboratorios debido a que su derrame puede provocar corto circuitos.
- Tener cuidado de la sustracción de la memoria RAM de las computadoras o de otros elementos, para lo cual debe observarse que la caja del CPU esté físicamente con los seguros correspondientes, todos los días.
- Vigilar cuidadosamente las computadoras portátiles, pues son fáciles de sustraerse.
- Diseñar un plan para obtener equipo nuevo en caso de robo, incendio o fallas.

4.4.1.1.2 El lugar de trabajo y ubicación de equipos

- Ubicar un extinguidor de mano recargable en cada piso donde se encuentre un centro computo o laboratorios, esto permitirá combatir el fuego si se presenta.

- Enseñar la forma de utilización del extinguidor al personal que trabaja en los lugares donde sean ubicados.
- Revisar el extinguidor una vez al mes probando que esté funcionando.
- Tener un sistema de alarmas automático para en caso de existir humo o fuego, poder detectarlo.
- Ubicar alarmas en los pisos falsos y/o techos falsos para detectar la presencia de humo o fuego.
- Tener un teléfono en la sala de cómputo y laboratorios, para que se pueda dar aviso en caso de que se descubra un incendio
- Mantener la sala de cómputo y laboratorios lo más limpio posible, y desprovistos de polvo, para evitar daños en los equipos. Para esto se vigilará que los conserjes o el personal encargado de la limpieza efectúen de forma correcta su labor.
- Limpiar los equipos de forma periódica con una aspiradora diseñada especialmente para este fin.
- Colocar cobertores cuando no se está utilizando los equipos, pero esperar un lapso de tiempo hasta que estos se enfríen antes de taparlos.
- No colocar las computadoras en repisas altas por el peligro de que al caerse sufran daños irreparables.
- Ubicar los anaqueles en lo posible lejos de las computadoras, para que en una situación de temblor o terremoto no caigan encima de las mismas.
- Ubicar las computadoras alejadas de las ventanas, para que en caso de la rotura de un vidrio no se afecte al equipo y a la persona que lo está utilizando.
- No colocar las computadoras demasiado cerca de las paredes, pues esto evita el flujo adecuado de aire
- Comprar mesas hechas específicamente para colocar computadoras, pues éstas protegen el CPU.
- Sujetar las computadoras sobre la superficie en las cuales descansa, esto evitará robos y caída de éstas.
- Prohibir fumar en la sala de cómputo y laboratorios porque esto afecta a los equipos.
- Leer los manuales de los equipos para que se conozca los rangos de temperatura, bajo los cuales trabajan de forma óptima y no se expongan a daños.

- Observar que las ventanas tengan todos los vidrios para evitar el ingreso de insectos, que suelen ser atraídos por el sonido del CPU y el calor de los monitores y al ingresar dentro de éstos provoquen daños.
- Comprar supresores de variaciones de voltaje, para evitar se quemen los equipos.
- Apagar las computadoras y otros dispositivos si es factible cuando hay tormentas (descargas eléctricas) y desconectar el sistema de alimentación eléctrica, esto evitará una sobrecarga en el fluido que quemará los equipos.
- Ubicar los medios magnéticos lejos de estructuras metálicas del edificio para que no sufran daños.
- En los lugares de alta confiabilidad se puede instalar una alarma que dé aviso cuando la humedad relativa sea mayor al rango que se haya establecido. Debe leerse las especificaciones técnicas correspondientes en los manuales de los equipos respecto a estos requerimientos.
- Colocar sensores de agua en el piso, cerca del sistema de cómputo. Si además existe piso falso ubicar un sensor debajo de él. También otro sensor a una cierta altura para que desconecte el flujo de energía a los equipos automáticamente, en caso de inundación.
- No ubicar los centros de cómputo en los sótanos, o en zonas donde ocurre frecuentemente inundaciones.
- Colocar interruptores automáticos para que en el caso que se suceda una inundación fuera de horas de oficina, se diera la alerta correspondiente.
- Diseñar el lugar de trabajo de los operadores de manera que les permita colocarse en la posición más natural posible, debiendo ser el sillón ajustable para que se adapte a las medidas y posiciones naturales de cada operador.
- Elegir monitores y placas de video de buena calidad para las computadoras con la finalidad de evitar el cansancio visual.
- Colocar pantallas antirreflejo en los monitores
- Utilizar lentes antirreflejo apropiados para la actividad en computadoras con medida o sin medida.

- Revisar que los ambientes de trabajo tengan los lúmenes suficientes en función del área. Esta actividad solicite que lo realicen los electricistas propios de la institución o si la misma no tiene por personal externo de la rama.
- Tratar que la temperatura ambiente del centro de computo y laboratorios esté comprendida entre 18 °C y 21 °C.
- Ubicar sistemas que remuevan el aire periódicamente.
- Revisar el ambiente sonoro del centro de cómputo para que no supere los 55 decibeles, pues valores superiores provocan daños en el oído.

4.4.1.1.3 Protección de datos

- Inspeccionar de manera rutinaria los cables que llevan datos en búsqueda de daños físicos.
- No abandonar en las salas de cómputo los respaldos porque alguien podría llevárselos y acceder a archivos importantes del sistema.
- No entregar los respaldos a servicios de mensajería que no tengan garantía.
- Guardar los respaldos en un lugar distinto al del sistema de cómputo.
- Cualquier medio de almacenamiento antes de ser arrojado a la basura se debe verificar que los datos se hayan borrado completamente, o proceda a su destrucción física.
- Al utilizar impresoras semipúblicas se debe tener cuidado porque los documentos que se imprimen pueden ser robados antes de ser recogidos.
- Los encargados de los laboratorios deben sugerir a los usuarios que no abandonen sus máquinas mientras tienen una sesión abierta porque esta constituye una gran oportunidad para los vándalos.
- Configurar el sistema operativo de tal manera que se cierre automáticamente una sesión o que se borre la pantalla del usuario y congele su teclado si la terminal ha estado activa por más de cinco minutos.

- No almacene los CD ROM de respaldo en el mismo lugar donde está el sistema, pida a la universidad que invierta en una caja fuerte a prueba de fuego para proteger en ese lugar los dispositivos en que se realiza los respaldos y ubicar la caja fuerte fuera del centro de computo, además asegúrese que sea para guardar medios magnéticos.
- Si está utilizando diskets para realizar respaldos inmediatamente que retire de la unidad cambie el botón de protección de escritura.
- Para guardar diskets, CD ROM, y otros elementos de almacenaje tenga un armario que posea llaves.
- Guardar las copias de las claves en trozos de papel dentro de sobres, que deben entregarse a cada miembro de la junta directiva que exista en la universidad, o a los jefes superiores en jerarquía.

4.4.1.2 Seguridad lógica

4.4.1.2.1 Respaldos

- Respaldar todo lo que es único en el sistema, incluyendo todos los archivos, cualquier base de datos del sistema que se haya modificado y directorios importantes del sistema.
- Almacenar todo lo referente al sistema en medios magnéticos de respaldo a intervalos regulares y predefinidos.
- Cuando un sistema se ha instalado por primera vez, antes de que la gente haya comenzado a usarlo, respáldese cada archivo y programa del sistema.
- Debe hacer respaldos de cada archivo y programa en el sistema inmediatamente después de haberse recuperado de una invasión.
- Realizar respaldos cuando se apliquen parches.
- Realizar respaldos completos el primer día de cada semana de trabajo

- Hacer un respaldo incremental cada noche de todo lo que se haya modificado desde el último respaldo completo
- De los archivos de usuario realice respaldos incrementales. Cuando hace respaldos incrementales no use el cd-rom regrabable en la cual sacó el respaldo la noche anterior, debe tener uno para cada noche de la semana e ir rotando.
- Utilizando una computadora sin configurar y diferente, al menos una vez al año debe tratarse de restaurar el sistema completo de los respaldos para asegurarse que el sistema entero de respaldo está funcionando correctamente.
- También es bueno elegir un archivo aleatoriamente una vez a la semana y tratar de restaurarlo.
- Hacer respaldos anuales que se archiven indefinidamente en CD-ROM que servirá como histórico.
- Utilizar cifrado para hacer más segura cierta información pero en este caso más de una persona deberá conocer la clave y siempre utilice la misma clave .

4.4.1.2.2 Cuentas

- Rastrear cuentas sin contraseña y proceder a suspenderlas
- Cuando el sistema operativo solicite una contraseña para cuentas especiales hágalo.
- Haga una lista de todas las cuentas que vienen en el sistema, inhabilítelas o cambie de contraseña.
- Borre o inhabilite las cuentas que crean los programas para sus demostraciones después de instalar el programa.
- En lugar de crear cuentas de grupo, cree una cuenta para cada persona en el grupo.
- Se puede especificar horas y días de la semana para cada cuenta, con la finalidad de prohibir cualquier conexión al sistema desde ciertas terminales y fuera de esas horas.
- Para los visitantes se requiere tener cuentas abiertas por lo que se debe generar diariamente una cuenta nueva y aleatoria.

- Si un usuario va a ausentarse por un período extenso se debe considerar evitar accesos directos a su cuenta hasta su regreso, puede poner un tiempo limite para la conexión a éstas cuentas.
- Inhabilite las cuentas que se usan esporádicamente y habilítelas solo cuando se necesita.

4.4.1.2.3 Contraseñas

- Establezca la longitud mínima de contraseña en ocho caracteres.
- Aconcejar a los usuarios que si escriben en papel el login o el password procedan a destruir cuando no lo requieran o lo ubiquen en un lugar seguro.
- Utilice un programa que rastree el archivo donde se ubican las contraseñas para buscar usuarios con contraseñas fáciles de adivinar y en ocasiones asigne contraseñas directamente a sus usuarios.
- La vigencia mínima de las contraseñas puede ser semestral y la máxima anual.
- El tiempo en que se advertirá antes de que la contraseña expire puede ser de quince días.
- Establezca los permisos apropiados en los archivos y directorios.
- Restrinja el acceso a la cuenta de superusuario, y controle el acceso a servicios remotos.
- Si va a tener usuarios que accedan desde el Internet hacia los servidores, trabaje con contraseñas descartables, con la modalidad que más se acerque a su presupuesto mediante tarjeta inteligente, calculadora especial, código o entréguele un grupo de claves de acceso para que las vaya utilizando y tachando una tras otra.
- Si su sistema operativo lo permite utilice los archivos de contraseñas ocultos, en este caso evite copias de respaldo del archivo de contraseñas ocultas que estén públicamente disponibles en algún lugar del sistema.

4.4.1.2.4 Detección de cambios

- Para mantener la integridad de la información trate de colocar todas las instrucciones, bibliotecas del sistema, bases de datos del sistema y los directorios importantes en medios de solo lectura.
- Realice copias de comparación que pueda almacenarlas en un disco distinto con el que trabaja, de esta forma tendrá una buena versión del sistema, si éste ha sido comprometido por accidente o por un agresor. Otra forma de realizar copias de comparación es hacer copias en disco en algún lugar del sistema, comprimiendo o cifrando la copia para ayudar a reducir el uso del disco y mantenerlo a salvo de allanamientos.

4.4.1.2.5 Bitácoras

- Ubique bitácoras en PCs que en la actualidad son obsoletas, y de esta forma evite la vulnerabilidad que existe cuando las bitácoras se encuentran grabadas en el mismo sistema.
- Enseñe a los usuarios a verificar la última hora de acceso cada vez que se conecten al sistema, esto permitirá determinar si no existió un acceso no autorizado después de la última vez que el usuario dueño de la cuenta ingresó, si encuentra problema indíquele que debe cambiar la contraseña y notificar al administrador del sistema.
- Revise frecuentemente el archivo o archivos que el sistema tiene para registrar quién está conectado al mismo en un momento dado. Revise información relacionada al nombre de la terminal usada para el acceso al sistema, nombre del usuario, nombre del anfitrión del cual se originó la conexión si ésta se realizó a través de la red, hora en que el usuario se conectó, etc.
- Revise que su sistema cuando está trabajando con un servidor de HTTP registre en bitácora el nombre de la computadora remota que inició la transferencia, el nombre de acceso remoto si se proporcionó o no, nombre del usuario remoto, hora en que la transferencia fue iniciada, las instrucciones HTTP, código de estado regresado y número de bytes que fueron transferidos

- Ponga todas las bitácoras en el mismo directorio, esto le permitirá vigilar y seguir la pista a los archivos de bitácora presentes en el sistema de mejor manera.
- Se puede mantener archivos de bitácora por usuario que permitan hacer análisis cuando algo desfavorable ha sucedido, mediante la verificación de modificaciones de éste archivo, para asegurar que fue usado durante el tiempo en que la actividad sospechosa ocurrió (creación, modificación, las instrucciones que se ejecutaron, programas que se compilaron).
- Se puede hacer una bitácora que registre el correo enviado y recibido para que si en algún momento se dañara el disco duro y se destruyeran buzones, pueda pedir que las personas reenvíen su correo.
- Se puede asignar una impresora para consignación de mensajes del sistema, pues así los intrusos borren los archivos de bitácora, no podrán hacer con lo enviado a la impresora a no ser que allane físicamente el local.
- Si desea alta seguridad puede hacer registrar los eventos ocurridos en todas las máquinas en la bitácora de una (o más) máquinas que posean diferentes sistemas operativos, lo que incrementaría la seguridad del sistema total.
- En vista de que hoy en día los discos son baratos, se puede todo lo que es útil registrar en muchos lugares diferentes, esto dificulta en gran medida los intentos de los agresores por borrar cualquier evidencia de su presencia.
- Las bitácoras deben ser examinadas periódicamente y también recortadas para evitar que se clausure las computadoras por que se ha llenado el dispositivo de almacenamiento.
- Utilice bitácoras manuscritas (en papel) para registrar las actividades del día, éstas deben mantenerse en una localidad físicamente segura, cada página debe estar numerada y no se puede arrancar hojas de las bitácoras, deben ser escritas con tinta, estas tienen las ventajas de que pueden:
    - Registrar muchos tipos de información diferente.
    - Registra números de cuenta y números telefónicos importantes para servicio de campo, contactos de servicios y el personal clave.

- Ante un desastre con los discos, se puede recrear algo de la información vital
- Los jurados aceptan mejor las bitácoras manuscritas que las bitácoras en computadora en un juicio.

- Realice bitácoras por sitio, las cuales deben conservar información de uso para todas las máquinas, donde existan:

  Reportes de excepción y de actividad

  - Cortes de corriente eléctrica (hora, fecha, duración)
  - Servicio de mantenimiento y prueba de los sistemas de alarma
  - Accionamiento de los sistemas de alarma
  - Servicio de mantenimiento y prueba de los sistemas de extinción de fuego
  - Visitas de personal de servicio incluyendo la compañía telefónica
  - Fechas de contratación y terminación de empleados con acceso privilegiado

  Material informativo

  - Información para contactar personal importante: autoridades, servicio de campo
  - Copias de las notas de compra, recibos y licencias de todos los programas instalados en los sistemas
  - Números de serie de todo el equipo importante en el sitio
  - Todas las direcciones de máquina de nivel MAC con sus correspondiente números IP
  - La hora y circunstancia en que se hizo un reporte de error al proveedor de un programa
  - Números telefónicos conectados a las computadoras para llamadas de entrada y salida
  - Configuración de ruteadores, firewalls y otros dispositivos de red no asociados a una sola máquina

- Lista de configuraciones de disco, geometrías SCSI y tablas de información de las particiones
- Cada máquina debe tener una bitácora manuscrita que contenga:

Reportes de actividades

- Relacionado a interrupciones o caídas (hora y fecha)
- Información sobre las medidas importantes tomadas para la recuperación del sistema
- Sobre tiempo muerto (hora, fecha, propósito)
- Datos que impliquen ocurrencias inusuales
- Instancias de cambios de contraseñas para usuarios
- Tiempos y niveles de respaldos y recuperaciones junto con la cuenta de cuantas veces se ha usado cada respaldo
- Instalación o actualización de programas (tiempo empleado, fecha y circunstancias por las que se realiza)
- Actividad de mantenimiento (tiempo, fechas y circunstancias por las que se realiza)

Material Informativo

- Copia de los archivos de configuración vigentes, deben ser actualizados periódicamente o cuando se cambien los archivos
- Listado de correcciones aplicadas por el vendedor del programa, número de revisiones e identificación del programa
- Información de configuración sobre programas instalados en la máquina que no haya venido con ella

- Asegúrese que todas las bitácoras se copie a los medios de respaldo en forma regular de preferencia diariamente
- Las bitácoras deben revisarse diariamente o mejor varias veces al día
- Escriba un programa que filtre aquellos mensajes que se ven de forma común para reducirlos a una colección más manejable

4.4.1.3 Amenazas lógicas

- El administrador debe conocer los puntos vulnerables de los sistemas, mantenerlos protegidos y vigilados; por lo que es importante que conozca las herramientas de seguridad que están disponibles de forma gratuita; pero no debe usarlas a menos que esté seguro de que entiende lo que hacen y como podrían ayudarle a asegurar el propio sistema. (ver cd-rom incluido en la tesis).
- Para evitar la existencia de puertas traseras y virus verifique los archivos importantes del sistema; revise los permisos y los propietarios de archivos y directorios importantes; revise los programas nuevos, especialmente de fuentes desconocidas o no bien conocidas los cuales pueden contener puertas traseras.
- Los programas nuevos instálese en algún sistema no crítico para realizar pruebas y familiarizarce, de esta forma podrá aislar problemas, identificar incompatibilidades y notar peculiaridades, esto sirve para evitar tanto las puertas traseras como las bombas lógicas.
- Para evitar los caballos de troya nunca ejecute nada (un programa o entrada a un interprete) hasta que no se haya leído cuidadosamente todo el archivo. Sino se comprende lo que hace el archivo, no se debe ejecutar. Si se esta desempaquetando archivos o ejecutando guiones por primera vez, esto debe hacerse en una máquina secundaria.
- Para proteger a una máquina contra los gusanos se debe tener control sobre los accesos no autorizados.
- No tenga mucha confianza del código fuente obtenido mediante FTP, no transfiera nunca archivos binarios de grupos de noticias, por que puede contener virus.
- Los interpretes de archivos PostScript deben poseer interruptor de seguridad, pues normalmente se transfieren vía FTP o WWW y automáticamente son interpretados.
- Debe tener cuidado con las paginas de la WWW que poseen applets que son ejecutados en la máquina cliente, porque pueden abrir conexiones de red con otras máquinas para generar otros procesos y modificar archivos.

- El correo codificado en MIME puede contener archivos diseñados para sobrescribir archivos locales o contener aplicaciones codificadas, que al ejecutarse realicen actos maliciosos.
- Indique a los usuarios que no deben responder preguntas referentes a características del sistema a través del teléfono o el correo electrónico, que parecieran venir de parte del administrador de la red, sino se puede determinar quien dice ser.
- Tener cuidado de quienes publicitan sobre ayuda en el Internet que pueden brindar a los usuarios en caso de problemas, pues usualmente cuando se los llama se trata de intrusos que aprovechan esta oportunidad para obtener la información que requieren.
- Los administradores de red deben configurar adecuadamente sus routers para filtrar los paquetes ICMP de peticiones broadcast; o configurar sus computadoras para que no respondan a dichos paquetes, para que de esta manera sus máquinas no participen inocentemente en los ataques contestando a paquetes de eco (ping) hacia una máquina que es víctima de un ataque.
- Configure su router de salida para evitar spoofing; esto se hace filtrando todos los paquetes de salida que tuviesen una dirección de origen que no perteneciera a la red interna .
- Utilice filtros para garantizar la detección de inundación de bits urgentes.
- Para evitar los problemas que existe en algunos sistemas operativos como windows NT, que no pueden armar correctamente los fragmentos IP que se superponen provocando que el sistema se cuelgue, el administrador debe conseguir los parches que solucionen este problema.
- Para mantenerse informado sobre cada una de las vulnerabilidades encontradas y parches lanzados, se recomienda que los administradores se suscriban a listas que brindan estos servicios de información.

4.4.1.4 Seguridad en la red

4.4.1.4.1 Módems

- La administración central de la red universitaria debe controlar los módems existentes, ubicándoles en un lugar con acceso restringido, para evitar el acceso físico a personas no autorizadas.
- Los números telefónicos que se están utilizando para los módems, debe estar restringido solo a personas que realmente requieren conocerlos.
- Se debe especificar cuales módems han de realizar las llamadas al interior y cuales han de recibir las del exterior.
- En la actualidad en el país existe el servicio de identificación de llamadas que viene integrado en muchos módems, por lo que se debe desarrollar programas apropiados para limitar las llamadas que ingresan a una lista específica de números telefónicos.
- Los administradores que utilizan para el mantenimiento y administración remota módem desde sus casas deben asegurarse que la línea telefónica sea físicamente segura y que los tableros de empalme en la universidad estén con llaves.

4.4.1.4.2 Servicio de red

Tenga en cuenta lo siguiente referente a los servicios de red:

- Retire cada servicio para el cual no se haya demostrado una necesidad
- Realice una consideración de costo-beneficio, para determinar si inhabilita un servicio
- Realice una copia de cualquier archivo de configuración antes de que inicie cualquier modificación por si se comete un error y se desea regresar al modo anterior o hubiese la sospecha de la presencia de un intruso y poder comparar los archivos.

Las consideraciones que se debe tener referente a los servicios de red son:

a) Telnet

- Si utiliza telnet debe determinar la duración de las sesiones de sus usuarios, el cual debe estar basada en el tipo de usuario o el usuario individual.
- Configure una sesión telnet de tal manera que finalice cuando después de un tiempo no se haya realizado ninguna actividad
- Utilice protectores de pantalla activado por tiempo para que se dispare cuando no exista actividad en una sesión después de cierto período.
- Haga que se respete el uso de contraseñas de por lo menos ocho caracteres y exija a que sean cambiadas dentro de determinados lapsos de tiempo, máximo cada 6 meses.
- Restrinja las sesiones y el acceso mediante contraseñas y ubicación de terminales.
- Si la sesión se inicia desde fuera de la red se debe requerir una segunda contraseña o un procedimiento de llamada de verificación de origen.
- Debe encriptarse las contraseñas
- Registre una bitácora con todos los accesos con contraseña y las direcciones de red; además genere informes de uso con el nombre del usuario, la dirección de red y la fecha
- Desarrolle perfiles de usuario y supervise las desviaciones del perfil
- Los usuarios deberían firmar un acuerdo confidencial

b) FTP

- El servidor FTP siempre debe estar fuera del firewall o no debe tener conexiones a su servidor o a la estación de trabajo conectada al mismo.
- Se debe contar con el modo pasivo para simplificar la tarea de construcción del cortafuegos pues este simplemente permitirá pasar conexiones internas hacia el mundo exterior, pero no permitirá el paso de conexiones del exterior de forma directa.

c) SNMP

- Si usa SNMP debe cambiar el valor determinado (public) que viene en los equipos a algún otro, para evitar que esta puerta trasera sea utilizada para reconfigurar un equipo maliciosamente.

d) DNS

- Por seguridad del sitio permita paquetes DNS UDP a través del cortafuegos y enrutadores, pero bloquee la transferencia de zona DNS originadas desde el exterior, de tal forma que evite a extraños determinar la dirección IP de cada computadora interna.
- Puede a nivel del enrutador bloquear las conexiones de llegada TCP en el puerto 53.
- La mejor manera de proteger al DNS es colocando un servidor DNS que opere para la red interna el cual manejará los nombres y las direcciones IP de todos los anfitriones locales e impedirá que los nombres internos sean filtrados hacia el Internet; y otro DNS frente del cortafuegos, el cual contiene solo los nombres y las direcciones IP de la computadora gateway de manera estática.
- Si desea incrementar la protección contra los ataques al servidor DNS, emplee direcciones IP en las listas de control de acceso en vez de usar nombres de host.
- Verifique que el servidor DNS no contenga cuentas de usuario
- Si por condiciones económicas el servidor DNS debe estar ejecutándose en una computadora empleada para usuarios ordinarios, asegúrese de que los archivos del servidor DNS sean todos propiedad de la raíz y tengan los modos de protección

e) HTTP

- Cuando seleccione un firewall asegúrese de elegir uno que incluya un servidor proxy HTTP esto dará seguridad a su red interna.
- Emplee alguna tecnología HTTP que permita en cierto grado resolver los problemas de seguridad en los cuales podría estar implicada su red

- Al configurar su servidor HTTP nunca utilice direcciones numéricas para entrar en sus páginas Web; debido a que esto producirá un número excesivo de las mismas en su lista de acceso lo que dificultará su mantenimiento.

f) FIREWALL

- Utilice cortafuegos internos en la institución para tener redes internas independientes y de esta forma minimizar el daño que ocurriría si una de las redes internas se compromete; sea por un intruso o por personal interno.
- Debe habilitarse el nivel más alto en registro en bitácoras para los gateways y la seguridad más restrictiva posible, no permitiéndose que exista claves de usuario en las máquinas gateway.
- El gateway debe tener una versión muy reducida de algún sistema operativo y no debería tener compilador para evitar que los agresores compilen programas en él; tampoco deben tener claves de usuario regulares; limitando de esta manera los lugares donde un agresor puede ingresar
- El gateway o el router deben proporcionar el servicio DNS de Internet para el mundo exterior
- Configure el gateway para que todo el correo de salida parezca venir de esta máquina
- Si tiene el servicio de News configure el gateway de tal manera que sea la máquina principal quien dé este servicio en la institución.
- Use apoderados o envolventes para dar a los usuarios internos la capacidad de usar FTP para transferir archivos de sitios remotos
- Para que de soporte a FTP anónimo desde la red externa es necesario de que el directorio de FTP público resida en la máquina gateway
- Si va a tener activado el servicio Finger debe tratar de limitarlo porque este puede proporcionar mucha información acerca de la estructura interna del sistema de archivos
- Si desea dar el servicio de Telnet que es justamente lo que trata de evitar los firewalls que es las sesiones remotas, puede crear una clave de usuario temporal en el gateway con un nombre aleatorio y una contraseña aleatoria que no pueda ser cambiada por el usuario; para mayor

seguridad se debe hacer que se borre la clave después de unos días o usar un identificador de tarjeta inteligente para acceder al gateway.

- Habilite la capacidad de auditar si el sistema operativo del gateway lo permite.
- Active el registro de bitácoras completo en el gateway
- Habilite la contabilidad de procesos en la máquina gateway
- Recuerde inhabilite los servicios de red no requeridos

4.4.1.5 Personal que trabaja en el centro de cómputo y laboratorios

- Cuando es contratada una persona para trabajar en los diferentes centros de cómputo de las universidades se debe examinar de forma cuidadosa su currículum y comparar los documentos entregados en copia con los originales, además se debe tratar de determinar cual ha sido su trayectoria, esto incluye también al personal de mantenimiento y limpieza.
- Dar capacitación básica a todos los usuarios del sistema sobre las políticas de seguridad de una manera rutinaria en el cual debe incluirse material escrito y una copia de la política sobre el uso de las computadoras y las redes, sobre el uso personal del equipo, las políticas sobre la propiedad y el uso del correo electrónico, las políticas sobre la importación y exportación de programas e información sobre los castigos que merecen las violaciones a estas políticas
- Todos los usuarios deben firmar el recibido de esta información así como aceptar por escrito las restricciones.
- Se deben adquirir revistas técnicas, comprar libros de referencia, para que lea el personal del centro de cómputo, laboratorios y hacer que asistan a seminarios de actualización en seguridad.
- Cuando el personal se retira voluntaria o involuntariamente se debe proceder a cancelar sus cuentas, cambiar las contraseñas clave y evitar el acceso a los sistemas de las mismas.
- Cuando se enferma alguien del personal o tiene una partida inesperada debe haber personal que lo va a reemplazar.

4.4.2 Procedimientos de seguridad

Los procedimientos de seguridad, son formas de protección contra ataques relacionados con el Internet, sistema operativo que se emplea y los dispositivos. Los sistemas operativos que están usando en las Universidades Ecuatorianas son: Windows y Unix.

4.4.2.1 Evitar ataques a través de la Web

- Debe existir una persona que evalúe y clasifique el tipo de información que se va a ser pública en la Web, retirando cualquier información que no se considere necesaria y que pueda ayudar a un atacante.
- Debe tener en cuenta los números de teléfono y direcciones que están ubicados en la Web porque pueden ser utilizados para ataques telefónicos o con fines de ingeniería social.
- Asegúrese que la información existente en las bases de datos públicas (CONESUP, Fundacyt etc.) sea fiable.
- Puede utilizar un nombre de contacto administrativo ficticio esperando de esta manera localizar a alguien que esté intentando llevar a cabo una labor de ingeniería social.
- Tenga un método seguro para la modificación de la información del dominio como por ejemplo utilizando PGP (Pretty Good Privacy).
- Vigile los registros para localizar incrementos exagerados a peticiones GET
- Si utiliza IIS 4.0 para solucionar el flujo alterno de datos, limite los permisos de acceso a archivos correspondientes a todo el código fuente, eliminando el permiso de lectura del grupo everyone. Información al respecto puede encontrar en ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis4-datafix/
- Cuando emplee IIS (Internet Information Server) en cualquiera de sus versiones use los parches ubicados en ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/Viewcode-fix/

- Para evitar la vulnerabilidad webhits.dll deberá eliminar las aplicaciones para las extensiones .htw, para que el servidor no vuelva a llamar a webhits.dll.
- No almacene información sensible en archivos ejecutables (.asp, .asa), que pueden ser vistos por los usuarios del Internet. Utilice el parche incluido en el Service Pack 1 para Win2000 y proteger de esta manera la información sensible.
- Para evitar el ataque iishack utilice el parche que se encuentra en la dirección ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/.
- Elimine todas las DLL que no utilice de forma activa para evitar ataques de desbordamiento de búfer.
- Instale los parches que se encuentran en los boletines MS00-057, MS00-078 o MS00-086 para evitar la vulnerabilidad del uso de Unicode.
- Trabaje siempre con la última versión de PHP, para evitar problemas de validación de entrada.

4.4.2.2 Evitar transferencia de zonas DNS

Para restringir la transferencia de zona solo a los servidores autorizados haga lo siguiente:

- En Unix utilice la directiva xfernets en el archivo named.boot.
- En Microsoft utilice la opción notify; información referente a esta opción se encuentra en http://support.microsoft.com/support/kb/articles/q193/8/37.asp
- Configure el cortafuegos o el router de filtrado de paquetes para que rechacen todas las conexiones no autorizadas al puerto 53 de TCP, que se utiliza para la transferencia de zona.
- Puede utilizar firmas transaccionales criptográficas para permitir que únicamente los hosts válidos puedan transferir información de zona.
- Configure los servidores de nombres de dominio externos para que solo proporcionen información sobre los equipos directamente conectados al Internet.

4.4.2.3 Identificación de intrusos en la Red

- Utilice programas que permiten detectar intrusiones en la red como el software snort localizado en http://www.snort.org/ .
- También puede realizar un registro de solicitudes traceroute entrantes y generar respuestas falsas utilizando la herramienta RotoRouter ubicada en http://cert.uni-stuttgart.de/archive/bugtraq/1998/08/msg00112.html.

4.4.2.4 Limitación del tráfico ICMP

- Puede configurar sus routers frontera para limitar el tráfico ICMP y UDP a ciertos sistemas específicos, minimizando de esta forma las amenazas.
- Evalúe el tipo de tráfico ICMP que permite en sus redes o en determinados sistemas; pues la mayoría de los sistemas no necesitan los tipos de tráfico ICMP.
- Para detectar ataques mediante barrido ping en máquinas con sistema operativo Unix utilice el snort o scanlogd (http://www.openwall.com/scanlogd), y en Windows genius (http://www.indiesoft.com/).
- Si su cortafuegos debe por alguna razón dejar pasar algún tipo de tráfico ICMP, realice un análisis cuidadoso para determinar lo que realmente requiere dejar pasar. De esta forma evitará un ataque de negación de servicio o que se abran puertas traseras en su sistema operativo mediante un paquete ICMP ECHO
- Si tiene una zona desmilitarizada DMZ puede hacer que el único tráfico ICMP permitido sea: echo_ replay (0), Host unrechable (3) y time exceeded (11).
- Si es factible trate de limitar el tráfico ICMP a direcciones IP específicas de su ISP, mediante una lista de control de acceso.
- Para controlar el acceso a nivel de sistema para ping en Linux puede utilizar Pingd (http://www.cs.sandia.gov/cplant/doc/man/load/pingd.html)

- Bloquee los paquetes ICMP en su router frontera para evitar que traspasen paquetes timestamp (13) y address mask request (17)

4.4.2.5 Detección de exploración de puertos

- Para detectar una actividad de exploración de puertos en Unix utilice snort (http://www.snort.org/) o Psionic PortSentry (http://es.tldp.org/LinuxFocus/pub/mirror/Linux-Focus/Castellano/ September2001/article214.shtml) para que detecte y responda a un ataque activo, definiendo automáticamente reglas de filtrado de núcleo, para prohibir el acceso desde el sistema atacante.
- Desactive todos los servicios que sean innecesarios, si esta utilizando UNIX comente los servicios no necesarios en /etc/inetd.conf y en caso de Windows desactive los servicios que no sean necesarios desde la aplicación Servicios del Panel de Control.
- Si esta utilizando sistemas Windows puede utilizar los siguientes detectores de exploración de puertos Genius (http://www.indiesoft.com), BlackICE (http://www.networkice.com), Zone Alarm (http://www.zonelabs.com/).
- El cortafuegos debe estar configurado para detectar los intentos de exploración de puertos.
- Configure sus alertas para que le adviertan en tiempo real mediante correo electrónico.

4.4.2.6 Evitar ataques contra el Sistema Operativo Windows

- Para evitar ataques filtre los puertos TCP y UDP 139 para windows NT y además de los puertos anteriores el 445 para WIN2000 en todos los dispositivos de acceso perimetrales de la red.
- Evite el acceso desde el exterior a los puertos 135 a 139 TCP y UDP, para que no tengan éxitos las actividades de enumeración que opera sobre NetBIOS, y además de esto en el sistema operativo Windows 2000 debe bloquear el puerto TCP/UDP 445. Este proceso se lo debe hacer mediante el router, o el cortafuegos.

- Desactive por completo los servicios SMB. Para mayor información al respecto revise las direcciones Web http://search.support.microsoft.com.
- Para evitar ataques a través de SNMP puede eliminar este agente o desactivar el servicio SNMP sino lo esta utilizando, caso contrario asegúrese de cambiar la cadena común predeterminada "public" por una privada , o edite el registro para que solo permita el acceso autorizado para SNMP Community Name y para impedir que se envíe información de NetBIOS. Asegúrese de bloquear el puerto 161 (SNMP GET/SET) para TCP y UDP, en todos los dispositivos perimetrales de acceso a al red, si esta utilizando SNMP para administrar su red.
- En Windows 2000 es fácil restringir la transferencia de zona utilizando el programa complementario Microsoft Management Console denominado *administrración de equipos*, bajo servicios y aplicaciones. También puede desactivar completamente la transferencia de zona, eliminando la selección del cuadro Permitir Zona de Transferencia, siempre y cuando no tenga servidores secundarios DNS.
- Bloquee el acceso a los puertos TCP y UDP 135-139 y 445 para impedir la identificación de los nombres de usuario, o sino tendrá que desactivar los servicios SMB o configurar Restrict Anonymous para asegurarlos. Para evitar sesiones nulas en Windows 2000 se asigna a RestrictAnonymous = 2.
- Para que nadie pueda acceder al Active Directory de Windows 2000 desde el exterior, filtre el acceso a los puertos 389 y 3268 TCP en la frontera de la red y para evitar desde las redes internas, restrinja los permisos del Active Directory.
- Para impedir que los intrusos obtengan información de las aplicaciones y servicios que se están ejecutando en su red, realice un inventario de las aplicaciones críticas y determine una forma de evitar la presentación de información especialmente sensible (nombre del fabricante, número de versión del software). Realice una auditoría de su sistema utilizando netcat a los puertos activos para comprobar que no se está facilitando información importante a los atacantes
- Utilice DumpSec para realizar una auditoria de su sistema operativo y comprobar que no existan fisuras en su seguridad

4.4.2.7 Evitar ataques contra el Sistema Operativo Windows 2000

El sistema operativo Windows más utilizado en la actualidad en las Universidades es el Win2000 por lo que a continuación se dan procedimientos para evitar ataques contra éste.

- Denegar todos los protocolos a todos los hosts (para lo cual puede ejecutar services.msc), y luego en función de la necesidad vaya activando los servicios y host que se requieran.
- Configurar los dispositivos de control de acceso (switches, routers, cortafuegos) de redes perimetrales para denegar la conexión desde el exterior a todos los puertos que no puedan ser desactivados en Win2000.
- No utilice los controladores de dominio como la base de la mayoría de las aplicaciones y servicios de archivo y de impresión.
- Utilice los filtros IPSec para llevar a cabo un filtrado de puertos basados en host. Para crear filtros IPSec utilice desde la línea de comandos ipsecpol.msc, o de forma gráfica, pero menos completa que la forma anterior, utilizando la aplicación Herramientas Administrativas |Directiva de Seguridad Local.
- Para desabilitar NetBIOS (puerto 139) sobre TCP/IP utilice las Propiedades de Conexión de Red y Acceso Telefónico a Redes |Propiedades del Protocolo Internet (TCP/IP)| botón Avanzadas |ficha WINS| Desabilitar NetBIOS sobre TCP/IP.
- Las sesiones nulas se realizan utilizando los puertos 139 y 445 de SMB, para evitar esto debe utilizar la aplicación Conexiones de Red y de Acceso Telefónico y seleccionar la opción Avanzadas |Configuración avanzada y desactive la opción compartir impresoras y archivos para redes Microsoft. Es la mejor forma de mantener seguro un servidor Windows conectado al Internet.
- Puede también utilizar filtro IPSec para restringir el acceso a NetBIOS y SMB

- Configure Win 2000 para que efectúe comunicación cliente o servidor con firma digital, de tal manera que se firmen de forma criptográfica cada bloque de comunicaciones SMB. Esto se realiza localizando la opción Directiva de seguridad/Directivas locales/Opciones de seguridad.
- Configure el gateway de la red o el software del cortafuegos para disminuir al máximo los daños que pueda provocar DoS (Denny of Service).
- Configure cada host de manera individual para resistir los ataques, en el caso de que falle lo anterior.
- Para evitar la escalada de privilegios en Windows 2000 debe utilizar el parche que modifica el modo en que el administrador de control de servicios crea y asigna las canalizaciones con nombre; este parche se encuentra en http://www.microsoft.com/technet/security/bulletin/MS00-053.asp
- Si el atacante accede físicamente y sin restricciones a un sistema existen pocas medidas para hacer frente al ataque en el cual se ubican las contraseñas en SAM, quizá la única medida que queda es configurar Windows 2000 para que se inicie en modo SYSKEY con contraseña o con diskette. Otras medidas es mantener los servidores físicamente a salvo, eliminar o deshabilitar las unidades extraíbles desde las que se puede arrancar el sistema o configurar una contraseña en el BIOS que el usuario deberá introducir antes de que se pueda iniciar el sistema.
- Si está utilizando EFS cree el archivo dentro de una carpeta que haya sido cifrado de esta forma todo el contenido se cifrará desde un principio y no se creará ningún archivo de copia en texto claro.
- Para evitar las puertas traseras debe limitar al máximo los inicios de sesión interactivos en los servidores
- Asegúrese de que cierra las sesiones del terminal seleccionando cerrar el equipo en el submenú inicio |apagar o utilizando la combinación de teclas Ctrl-Alt-Fin.
- El GPO (Objetos de Directiva de Grupo) es el mejor modo de configurar de forma segura grandes dominios de Windows 2000. Para utilizar GPO ir a Ejecutar y en la ventana que asoma ubicar gpedit.msc.

- Los administradores pueden utilizar la herramienta configuración y análisis de la seguridad que viene incluido en Windows 2000 y que están relacionadas con la función directiva del grupo, para realizar la auditoría de configuraciones del sistema local para comprobar su cumplimiento respecto de una plantilla definida y para modificar el valor asignado a cualquier parámetro que no se ajuste a la misma. De esta forma se podrá determinar rápidamente si un sistema cumple los requisitos básicos de seguridad.
- Los administradores deben iniciar la sesión para trabajar en el sistema como un usuario normal con los menos privilegios posibles y acceder a la cuenta del administrador cuando lo requiera alguna tarea específica

4.4.2.8 Evitar ataques contra el Sistema Operativo Unix

Después de Windows el sistema operativo más utilizado en las Universidades Ecuatorianas es el Unix y su versión para PC el Linux, por lo que a continuación se dan procedimientos de seguridad para este sistema operativo.

- Si está usando NFS asegúrese de que sus sistemas de archivos exportados tienen los permisos adecuados y que NFS se encuentra bloqueado en el cortafuegos en el puerto 2049. También puede registrar las peticiones showmount para coger a los infractores.
- No ejecute finger y coméntelo en inetd.conf y ejecute killall –HUP inetd; además bloquee el puerto 79 en el cortafuegos. Si es necesario permitir el acceso a finger use TCPWrappers, para poder restringir y registrar el acceso al host.
- No ejecute TFTP y si lo está haciendo restrinja su acceso al directorio /tftpboot y asegúrese de que esté bloqueado en el cortafuegos externos (puerto 69 UDP)
- Si utiliza RPC emplee alguna forma de autenticación. Asegúrese de que el cortafuegos filtra los puertos 111 y 32771.

- Si no está utilizando SNMP desactívelo; caso contrario configúrelo adecuadamente, escogiendo los nombres de comunidad adecuados y no los “public” o “private”. Si SNMP utiliza para administrar su red bloquee el acceso al puerto 161 de TCP y UDP en todos los dispositivos de acceso perimetrales de la red.
- Registre los intentos fallidos múltiples de autenticación y desconecte al usuario después de que éste intente 2 sesiones sin éxito.
- Utilice herramientas de generación de contraseñas como cracklib (http://www.crypticide.org/users/alecm/security/cracklib,2.7.txt), para impedir que el usuario escoja una contraseña fácil de adivinar.
- La mejor forma de defenderse contra ataques de desbordamiento de bufers es utilizando buenas prácticas de programación para evitar comprometer la seguridad del sistema, por lo que debe diseñar programas teniendo en cuenta la seguridad, utilizar compiladores seguros, realizar una validación de los argumentos cuando se reciben de un usuario o de un programa; utilizar rutinas seguras tales como fget( ), strncat( ), strncpy( ), deduzca la cantidad de código que se ejecuta con privilegios de la cuenta root, aplique todos los parches del fabricante relacionados con la seguridad
- Emplee TCP Wrappers y xinetd (http://www.xinetd.org/), para aplicar una lista de control de acceso selectiva a cada uno de los servicios. Utilice una función de filtrado (ipchains o netfilter para Linux) de paquetes a nivel de kernel.
- Protegerse de un back channel es difícil, la forma parcial es desactivar los servidores innecesarios y aplicar los parches del distribuidor y los programas complementarios relacionados.
- Elimine X Windows de cualquier sistema que requiere un alto grado de seguridad que evitará ataques con xterm y que los usuarios locales puedan aumentar los privilegios hasta convertirse en un administrador
- Ajuste los permisos de sus archivos binarios tales como telnet (chmod 750) para que sean ejecutados solo por el propietario del binario o grupos específicos

- Si va a dar el servicio FTP anónimo asegúrese de que está aplicando los últimos parches de seguridad desarrollados y elimine y si no es posible reduzca el número de directorios de escritura universal disponible.
- Si requiere usar sendmail para recibir correo en una red utilice la última versión con todos los parches de seguridad. Elimine los alias decodificados del archivo alias, debido a que este es un agujero para la seguridad. Emplee utilidades de seguridad (http://www Tis.com/research/software/) como Smap que se emplea para recibir mensajes de una forma segura y ponerlos en cola en un directorio especial y smapd que explora periódicamente este directorio y entrega el correo al usuario correspondiente utilizando sendmail. Considere la utilización de otros servidores de correo como qmail (www.qmail.org) o postfix (http://www.postfix.com/).
- Si no esta usando sendmail debe desactivarlo.
- Para defenderse de los ataques RPC debe desactivar todos los servicios que no sean absolutamente necesarios. Utilice los parches asociados a las vulnerabilidades RPC si va ha tener activos este servicio y además emplee Secure RPC que proporciona un nivel de autenticación adicional utilizando criptografía basada en clave pública.
- Si no es necesario en su red utilizar NFS desactívelo conjuntamente con los servicios mountd, statd y lockd. Si lo va emplear utilice controles de acceso de aplicaciones clientes y usuarios para permitir únicamente el acceso a los archivos a quienes estén autorizados.
- Cuando emplee X Windows no permita que se ejecute el comando xhost +. Utilice mecanismos de autenticación como MIT-MAGIC-COOKIE-1, XDM-AUTHORIZATION-1 y MIT-KERBEROS-5. Si está empleando xterm active la opción secure Keyboard. Puede también pensar en instalar un cortafuegos en los puertos 6000-6663 para evitar que los usuarios no autorizados se conecten a sus puertos de servidor X. Utilice ssh para mejorar la seguridad mediante sus sesiones X.
- Desactive y elimine BIND en cualquier sistema que no utilice como servidor DNS.

- Asegúrese que la versión de BIND se encuentra actualizada y que se utilizan los parches adecuados para corregir los defectos de seguridad (http://www.isc.org/products/BIND/bind-security.html). Ejecute named como un usuario sin privilegios; es decir ejecute named con los privilegios del administrador para enlazar el puerto 53 y luego elimine estos privilegios durante la operación normal con la opción –u (named –u dns –g dns). Finalmente debe ejecutar named desde un entorno chrooted( ) con la opción –t, con lo que impedirá atravesar su sistema de archivos.
- Para evitar problemas de vulnerabilidad con SSH actualice su sistema a la versión 2.3.0 o posterior de OpenSSH (http://www.openssh.com)
- Si tiene un sistema que utilice exclusivamente para capturar tráfico de red o efectúe detección de intrusos, ponga la tarjeta de red en estado de modo silencioso que es cuando se encuentra en modo promiscuo pero no cuenta con una dirección IP.
- Elimine los bits SUID de cualquier programa en que no sean imprescindibles y aplique todos los parches desarrollados por los fabricantes que guarden relación con la seguridad. No debe crear nunca archivos de comando de shell SUID
- Los usuarios de Linux pueden emplear Bastille (http://www.bastille-linux.org/) para fortalecer el sistema frente a muchos de los ataques locales, especialmente para ayudar a eliminar el bit SUID de los distintos archivos.
- Las bibliotecas compartidas deben estar protegidas con el mismo nivel de seguridad que los archivos más delicados
- Si un archivo es de inicio del sistema, de configuración del sistema, inicio de usuario no debe ser de escritura universal.
- Para evitar los troyanos debe realizar una vigilancia y un inventario de todos los puertos de escucha, requerirá un programa de comprobación de sumas que realice una firma única de cada archivo binario y almacenar estas firmas de forma segura, puede utilizar el programa Tripwire (http://www.tripwire.com) como herramienta de comprobación de sumas. Para los sistemas

solaris puede obtener una base de datos completa de sumas MD5 de http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl

- Para limitar las actividades de los snifers puede hacer lo sifguiente:
- Pase de su red ethernet compartida a una red ethernet conmutada
- Utilice la herramienta L0pht (http://security.nnov.ru/search/source.asp?souname=L0PHT) para determinar si existe un sniffer funcionando en una máquina determinada de su red.
- Utilice cifrado SSH o IPSec punto a punto
- Para evitar que sea borrada la información del archivo de registro puede configurar con el atributo append-only para que solo pueda añadirse información a los archivos de registro y los atacantes no puedan modificarlos. Otro método es utilizando el comando syslog para enviar información crítica de un registro a un host seguro.

4.4.2.9 Seguridad en los dispositivos de red

- En los dispositivos de red para evitar ataques debe eliminar las contraseñas, y las cuentas que viene con el equipo en el momento en el que configure el dispositivo, las más comunes son las mostradas en la tabla 4.1, pero también revise los manuales de los dispositivos.

Tabla 4.1 Nombres de usuarios y contraseñas predeterminadas

Dispositivo	Nombre usuario	Contraseña	Nivel
Cisco	(telnet) (telnet) enable (telnet)	(Cisco 2600s) cisco cisco cisco routers	Usuario Usuario Administrativa
3Com	Admin Read Write	Null Null Null	Administrador Usuario Administrador

	Debug Teach Monitor Manager Security	Null Teach Monitor Manager Secutity	Administrador Usuario Administrador Administrador
Motorola	cable com	Router	Administrativa
Shiva	Root guest	Null Null	Administrativa Usuario
Bay router	Usuario Manager	Null Null	Usuario Administrador

- Ubique contraseñas difíciles de adivinar para TELNET, SNMP y los servicios FTP y TFTP
- La mejor medida para evitar que sean descubiertas las contraseñas es cifrarlas utilizando SSH .
- Para los sistema críticos (cortafuegos y routers frontera) configure entradas ARP estáticas.
- Para evitar que se vea comprometido el tráfico SNMP en la red debe cifrar la información mediante (DES) o realizando un túnel punto a punto sobre una red privada virtual VPN, empleando un cliente VPN de cifrado tal como Entrust (http://www.entrust.com).

4.4.2.10 Evitar ataques al cortafuegos

- Para evitar los ataques puede bloquear las formas de exploración de puertos en su router frontera o utilizar herramientas de detección de intrusos
- Si el ISP es quien administra su router tendrá que ponerse en contacto con él para realizar el bloqueo y si usted es quien lo administra deberá escribir en su dispositivo las listas de control de acceso.
- Restrinja la respuesta a paquetes caducados TTL de su cortafuegos y router cuando sea posible
- Limite la información que proporciona al exterior en forma de mensajes, recomendando no entrar de forma fraudulenta y advirtiendo que se registrará todos los intentos de conexión

- Para evitar que los atacantes enumeren las listas de control de acceso que manejan su router y cortafuego puede desactivar la capacidad que tiene el router para responder con el paquete ICMP de tipo 13 (solicitud de horario).
- Las reglas impuestas en el cortafuegos deben ser explícitas para indicar quienes pueden conectarse y dónde.
- En la lista de control de acceso impida el tráfico ICMP a través del cortafuegos
- Desactive el acceso proxy desde la interfaz externa al cortafuegos o restrinja el tráfico proxy entrante en su router frontera mediante una cláusula de control de acceso.

CONCLUSIONES

- Las Universidades no realizan un control riguroso del acceso físico a sus instalaciones, lo que puede provocar la sustracción de equipos de cómputo que posean información importante y exclusiva de la Institución.

- Los tipos de usuarios al ser diversos en las universidades, desde los quienes conocen las funciones mínimas del manejo de la computadora, hasta quienes saben programar, instalar y configurar software, conocen herramientas que si son bien usadas en una red son benéficas, pero a su vez también pueden ser empleadas para ataques a la red, hacen que la administración y seguridad de las redes universitarias se convierta en un tema que debe ser de alta prioridad.

- Los equipos de personas de respuesta a incidentes que poseen las Universidades tienen alta importancia en el mantenimiento, control y buen funcionamiento de las redes en la parte física y lógica, por lo que requiere una continua capacitación y actualización de sus conocimientos en el área de las seguridades; además deben conocer y aplicar las políticas de seguridad establecidas en la Institución.

- La necesidad de que los usuarios de las Universidades tengan acceso a la información existente en el Internet, ha hecho que estas Instituciones busquen mejorar el ancho de banda de su enlace, así como desarrollar e implementar aplicaciones que puedan ser utilizadas a través del Internet. Esto ha provocado que se produzcan ataques desde el exterior, o que sus redes sean utilizadas como medio para atacar otras redes, lo que ha demostrado que al momento de configurar los equipos no se consideró la seguridad.

- Los respaldos de la información es quizás el último recurso que en ocasiones le queda a los administradores de las redes para recuperar los datos perdidos, pero si la forma de protección de los respaldos no sigue políticas de seguridad adecuadas están expuestos a su pérdida definitiva.
- Con un 95% de confianza se puede afirmar que la operatividad no óptima de los sistemas de redes universitarias conectadas al Internet es debido a la falta de políticas y procedimientos de seguridad.

- Las políticas y procedimientos de seguridad de la propuesta están planteadas en función de los problemas de seguridad física y/o lógica encontrados en las 25 universidades en las cuales se realizó la investigación, que comprenden universidades grandes, medianas y pequeñas, públicas o privadas dentro de la nación ecuatoriana, que poseen acceso al Internet y como mínimo tienen una página Web.

RECOMENDACIONES

- Las políticas de seguridad a implementarse en las Universidades y Escuelas Politécnicas del país deben ser difundidas a través de la página Web de cada institución, de manera que los administradores de las redes puedan consultar y si es necesario imprimirlas.

- Los procedimientos de seguridad establecen las formas de defensa de las redes universitarias, de ataques internos como externos y constituyen el complemento a las políticas de seguridad, por lo que tienen que ser conocidos e implementados por los administradores.

BIBLIOGRAFIA

- BROWN, Steven. Implementación de Redes Privadas Virtuales (RPV).Ed. McGraw Hill, México. 2001.
- COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. Ed. Prentice Hall. México, 1996.
- COMER, Douglas. Redes de Computadoras Internet e Interredes. Ed. Prentice Hall. México, 1997.
- CHERRE, Rafael. Redes y Conectividad. Ed. Macro. Perú, 2001.
- GONCALVES Marcus. Manual de Firewalls. Ed. McGraw Hill, México, 2001.
- GORDON, Bennett. Introducción a las Intranets, Ed. Prentice Hall, España, 1997.
- HERNANDEZ, Roberto. Metodología de la Investigación, Ed. McGraw Hill, México 1998.
- JONES, Keith. JOHNSON Bradley. Super Utilidades Hacker. Ed. McGraw Hill. España 2003.
- PETERSEN, Richard. Linux Manual de Referencia, McGraw Hill, España, 1997.
- SCHIFFMAN, Mike. Hackers: 20 Desafíos Prácticos, Ed. McGraw Hill, España, 2002.
- SERVATI, Al. BREMNER, Lynn. LASI, Anthony. La Biblia de la Intranet. Ed. McGraw Hill. México, 1997.
- SIMMONS, Curt. Guía Avanzada Microsoft Windows 2000 Server Configuración. Ed. Prentice Hall, España, 2000.
- SIYAN karanjit,. Internet y Seguridad en Redes. Ed. Prentice Hall. México, 1995.
- STALLINGS, William. Comunicaciones y Redes de Computadoras. Ed. Prentice Hall. España 2000.