ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Tema:

Análisis de los recursos, servicios de red y diseño de un esquema de seguridades para una empresa XYZ S.A.

Integrantes:

Josefina María Egas Alprecht[1]
Christian César Zambrano Intriago[2]
Angel Edwin Gaona Salinas[3]
Ing. Albert Espinal Santana[4]

[1]Licenciado en Sistemas de información 2004.
[2]Licenciado en Sistemas de información 2004.
[3]Licenciado en Sistemas de información 2004.
[4]Director de Tópico, Título de Pregrado: Ingeniero en Computación, ESPOL, Diciembre 1996. Título de Postgrado: Maestría en Sistemas de Información Gerencial, ESPOL, Enero 2000. Profesor de la ESPOL desde: Julio 2000.

RESUMEN

La empresa XYZ S.A es una empresa líder en el Ecuador en la fabricación y montaje de cámaras para refrigeración, equipos y accesorios. Es una empresa pequeña con requisitos de nivel de seguridad informática medios. Actualmente la red informática tiene algunas vulnerabilidades importantes, como por ejemplo: no existe una cultura de seguridad por parte de los usuarios, en los servidores se ejecutan servicios de red inseguros como: Telnet, FTP anónimo, archivos compartidos, no se encripta el tráfico en la red, ciertos puertos están abiertos, no existe un Sistema de Detección de Intrusos en la red y no existe un log que audite el sistema.

Para contrarrestar por lo menos el 60% de las vulnerabilidades, se ha sugerido los siguientes cambios en red actual. Estos son: Segmentar la red por medio de la emulación de un router, función que la realizaría un PC que arranca desde un disquete el cual usa el kernel 2.4 de Linux utilizando el software Coyote Linux; se sugiere cerrar puertos innecesarios, desinstalar lo servicios que no se usan en la red, instalar y configurar un Sistema de Detección de Intrusos, función que se la haría con el Snort, se utilizaría IPTables como Firewall definiendo las reglas necesarias para su correcto funcionamiento, restringir el uso a ciertas paginas Web por medio ACLs configuradas en el web-cache del Squid. Además se sugieren políticas de seguridad informática como complemento a este proyecto. Y capacitación para el personal de la empresa concerniente al uso de los Recursos Informáticos y su seguridad.

SUMMARY

The company that we are analyzing in this project is leader in manufacturing and assembly cold storage room, equipment and accessories in Ecuador. This is small company with a media level security requirement. Currently the network in the company has some important vulnerabilities, such as the users has no security culture, servers run insecure services such as Telnet, anonymous FTP, sharing files, data traffic is not encrypted on the network, some ports are currently open, there is no Intrusion Detection System and there is no security log auditing the system of the company.

To balance at least around 60% of vulnerabilities, we have suggested some important changes on the topology of the currently network, those are: Network Subnetting using a PC as a router, the PC boot with Coyote Linux under Linux Operating System with Linux kernel 2.4. Unnecessary ports should be closed, unnecessary services should be uninstalled on the network, we suggest installing an Intrusion Detection System such as Snort, and we suggest using IPTables as a firewall, to deny some dangerous web sites using ACL's through Squid. Also we suggest security policies related to Information Technology Department and we recommend that the personal of the company take some courses about how to use Network security resources.

INTRODUCCIÓN

El auge del Internet, el avance en las telecomunicaciones y en el hardware de los computadores han sido importantes en los últimos años, lo que ha posibilitado a que un usuario pueda realizar transacciones en forma remota sin desplazarse a ningún sitio. La falta de medidas de seguridad en las redes de las empresas es un problema que está en crecimiento. Cada vez es mayor el número de atacantes, son mejores las herramientas que estos utilizan y cada vez están más organizados.

A lo largo de este trabajo se va a analizar la situación actual de la Empresa objeto de este proyecto, relacionado a los aspectos de seguridad computacional con requisitos de seguridad medios esto es: un Análisis de Vulnerabilidades, Análisis de Riesgos, y proponer soluciones para nuestra empresa estableciendo la importancia de la utilización de herramientas de seguridad como un Firewall y un Sistema de Detección de Intrusos entre otros, utilizando plataformas Linux y Windows y redes de computadoras, sin dejar de lado la importancia que tiene como complemento unas buenas Políticas de Seguridad.

El objetivo final de este proyecto será marcar unas pautas para conseguir un nivel de seguridad aceptable en los sistemas Linux y Windows conectados a la red de la empresa, entendiendo por “aceptable” un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los equipos de nuestra empresa fracasara ante un ataque contra los mismos.

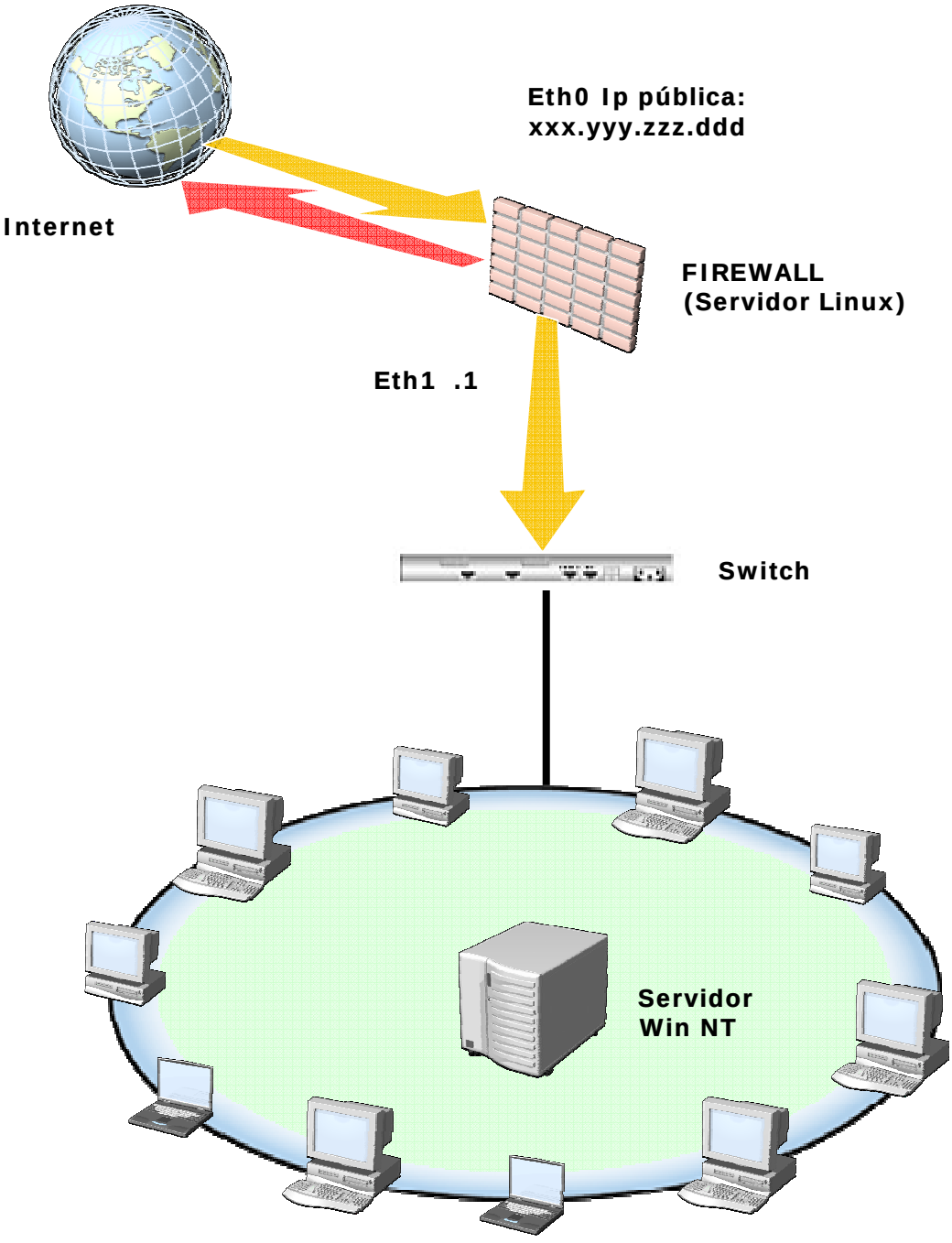
CONTENIDO

HISTORIA DE LA EMPRESA

XYZ es una Empresa que comenzó hace 36 años, comercializando repuestos y brindando servicio técnico para el área de refrigeración. Posteriormente se transformaron en fabricantes de última tecnología en Cámaras Frigoríficas y soluciones de aislamiento con poliuretano en general.

XYZ es una Empresa líder del Ecuador en la fabricación y montaje de cámaras para refrigeración, equipos y accesorios. Son los representantes y distribuidores exclusivos en el Ecuador de los productos METECNO de Colombia.

ESQUEMA ACTUAL DE LA RED DE LA EMPRESA



Red: 10.10.10.0/24

Figura 1. Esquema Actual de la Red XYZ S.A.

ESQUEMA DE RED PROPUESTO

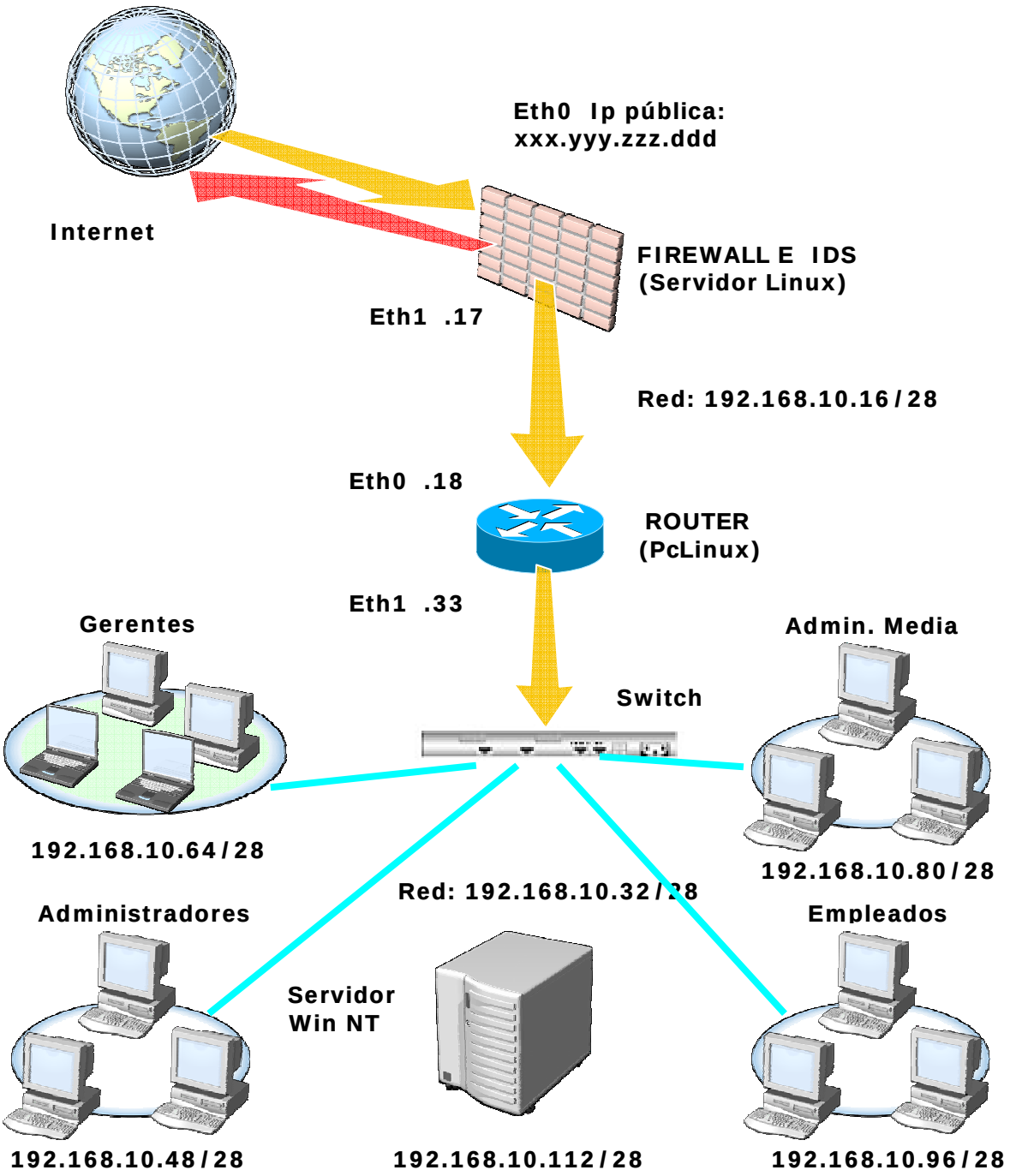


Figura 2. Esquema de Red Propuesto

PERMISOS DE CONTENIDO POR GRUPOS

GRUPO	CONTENIDO
Administradores	Todos los sitios.
Gerentes	Todos los sitios excluidos pornografía, música, videos, juegos.
Admin. Media.	Solo paginas del banco, IESS, SRI.
Empleados	Ningún sitio.

Tabla I. Permisos de Contenido por Grupos

ANALISIS DE VULNERABILIDADES

Vulnerabilidad	Efecto
No esta segmentada la red por dominios de broadcast, sólo existe un switch en toda la red. Las direcciones IP no están subneteadas, actualmente se lleva un esquema de direccionamiento IP estático con una sola dirección de red para toda la empresa.	♦ Posibles ataques DoS exitosos causados por tormenta de broadcast, debido al ingreso de gusanos o troyanos en la red. ♦ LA red no es administrable, debido a que todos pertenecen a la misma red. ♦ NO se puede controlar eficientemente el uso de recursos de red. ♦ Cualquier usuario de cualquier departamento puede acceder directamente a toda la red y a su vez analizar el trafico de toda la red, comprometiendo los datos confidenciales de la empresa. ♦ Se degrada el rendimiento de la red.
No están bien definidas las reglas de firewall en el servidor Linux, y además, no existe instalado un Firewall en el Servidor Windows NT.	♦ Los hackers pueden acceder remotamente al sistema a través de servicios inseguros que no están protegidos con reglas de filtrado. ♦ Los usuarios internos pueden utilizar los servicios a su antojo. ♦ Los usuarios pueden comprometer seriamente la confidencialidad de la empresa. ♦ Si un troyano es ingresado a la red, puede atacar fácilmente a este servidor, produciendo un robo fácil de información. ♦ Se pueden recibir paquetes deformados o fragmentos que pueden producir DoS, y pueden hachear el sistema. ♦ Se pueden producir ataques tipo Spoofing de IP y ARP. ♦ Acceso ilegal a la red.
Vieja versión de Open SSH 1.x. en el Servidor Linux.	♦ Con versiones anteriores a la 1, tiene varias vulnerabilidades, las personas pueden ejecutar ciertos comandos.
Telnet se esta ejecutando en el Servidor Linux.	♦ Un usuario remoto puede interceptar los datos con un Sniffer y puede robar los usuarios y passwords.
Algunos servicios como Pop 3, Telnet y SSH presentan Banners, con información: que sistema operativo se esta ejecutando, la	Esta información puede ser de mucha ayuda para el hacker, puesto que con esto el hacker puede encontrar en sitios de internet ciertas vulnerabilidades para el sistema operativo y versión

Vulnerabilidad	Efecto
versión del SO y la versión del Kernel o servicio que se esta ejecutando. Esto sucede en ambos servidores Win NT y Linux.	de Kernel en particular, produciendo ataques exitosos y eficaces.
No existe un IDS de red.	♦ El Jefe de Sistema no esta prevenido de los diversos tipos de ataques: DoS, virus, troyanos, Spoofing, sniffing. ♦ Baja rendimiento de la red, debido a la circulación de paquetes innecesarios que no son controlados en la red.
No hay control de acceso físico al centro de cómputo.	Cualquier persona que tenga acceso al área de administración y ante una distracción del personal, puede ingresar en él, con todo el riesgo que esto implica, debido a la sensibilidad crítica de los datos y activos que allí se encuentran.
No hay en los empleados de la empresa, plena conciencia con respecto a la importancia de la seguridad informática.	Al no existir una cultura de la seguridad implementada en la empresa, no se asegura el cumplimiento de normas y procedimientos.

Tabla II. Vulnerabilidades más importantes.

ANALISIS DE RIESGOS

Como conclusión general se puede decir que el porcentaje de riesgos descubiertos en la empresa es del 56,9 % (2220,33 puntos), considerando el nivel máximo de riesgos como el 100% (3900 puntos), y sabiendo que el porcentaje mínimo es de 33.3% (1300 puntos). Por esto podemos concluir que la empresa debería reducir en 23,6 el porcentaje de riesgos descubiertos, para así conseguir el nivel mínimo de riesgos posible y de esta forma llegar a obtener un nivel de seguridad aceptable.

Porcentaje de riesgos descubiertos	56,9
Porcentaje de riesgos mínimos	33,3
Desviación	23,6

Tabla III. Interpretación de Resultados.

INCIDENCIA DEL ÁREA DE TECNOLOGÍA INFORMÁTICA EN LA EMPRESA.

A continuación se muestra la tabla relacionada a los ingresos promedios que la empresa percibe relacionado a la incidencia del área de Tecnología Informática en la empresa, basada en un porcentaje aproximado, para este caso se estipuló en 10%.

Mes	Ventas Mensuales ($)	Incidencia Tecnología Informática 10%	Peso	Días Laborables	Costo de producción diaria ($)	Costo de producción por hora ($)	Costo de producción cada 5 min. ($)
Enero	200.058	20.005,80	5,36	22	909,35	113,67	9,47
Febrero	246.274	24.627,35	6,60	20	1.231,37	153,92	12,83
Marzo	237.337	23.733,72	6,36	23	1.031,90	128,99	10,75
Abril	241.953	24.195,31	6,48	22	1.099,79	137,47	11,46
Mayo	173.385	17.338,50	4,64	21	825,64	103,21	8,60
Junio	294.160	29.416,00	7,88	22	1.337,09	167,14	13,93
Julio	210.573	21.057,33	5,64	22	957,15	119,64	9,97
Agosto	801.203	80.120,29	21,46	22	3.641,83	455,23	37,94
Septiembre	483.755	48.375,49	12,96	22	2.198,89	274,86	22,91
Octubre	299.837	29.983,71	8,03	21	1.427,80	178,47	14,87
Noviembre	225.000	22.500,00	6,03	19	1.184,21	148,03	12,34
Diciembre	320.000	32.000,00	8,57	21	1.523,81	190,48	15,87
TOTAL	**3.733.535**	**373.353,51**	**100,00**	**257**	**17.368,83**	**2.171,10**	**180,93**

Tabla IV. Incidencia del Área de Tecnología Informática

COSTO PROMEDIO DE FACTORES DE RIESGOS EN LA EMPRESA.

En la siguiente tabla se muestra los costos promedios de cada factor de riesgo en la empresa, es decir lo que le costaría a la empresa tener inactivo alguno de estos recursos.

N#	Activos	Importancia (1 a 10) %	Promedio de Costo por día (un año) ($)	Ajustado ($)	Por hora ($)	Cada cinco minutos ($)
1	Datos de usuarios.	1,1	1452,74	15,56	1,94	0,16
2	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)	1,4	1452,74	20,74	2,59	0,22
3	Hardware (teclado, monitor, unidades de discos, medios removibles)	2,9	1452,74	41,49	5,19	0,43
4	Cableado, antenas, routers, switch, bridge.	6,9	1452,74	99,57	12,45	1,04
5	Usuarios.	8,0	1452,74	116,69	14,59	1,22
6	Red.	9,3	1452,74	134,84	16,85	1,40
7	Datos en tránsito, datos de configuración, datos en medios externos.	12,4	1452,74	179,78	22,47	1,87
8	Documentación de programas, hardware, sistemas, procedimientos	3,3	1452,74	47,87	5,98	0,50
9	Respaldo.	7,9	1452,74	114,89	14,36	1,20
10	Bases de datos.	11,8	1452,74	170,84	21,35	1,78
11	Software de aplicación, programas fuente, sistemas operativos.	8,7	1452,74	126,69	15,84	1,32
12	Servidores y switch central.	15,0	1452,74	217,82	27,23	2,27
13	Administrador de sistemas (Departamento de sistemas).	11,4	1452,74	165,96	20,74	1,73
		100,0	**18885,59**	**1452,74**	**181,59**	**15,13**

Tabla V. Costo promedio de Factores de Riesgo en la Empresa

FACTORES DE RIESGOS EN TÉRMINOS MONETARIOS.

En la tabla anterior nos podemos dar cuenta que el departamento de sistemas representa apenas el 10%($373.353,51) de las ventas anuales de la empresa. Además, los factores de riesgo más críticos para la empresa son: Servidores, Switch central, Datos en tránsito, datos de configuración, datos en medios externos y Bases de datos, y el de menor riesgo son los datos de usuarios.
En otras palabras a la empresa le costaría $27,23 tener fuera de servicio los Servidores y Switch central, $22,47 por perder los Datos en tránsito, datos de configuración, datos en medios externos, y $ 21,35 por tener fuera de servicio la base de datos, cada uno durante una hora. En el peor de los casos, es decir, que este fuera de servicio absolutamente todo el Departamento de Sistemas le costaría $181,59 por hora.

Finalmente, la empresa debería establecer un esquema de seguridad, reforzando principalmente y especialmente los factores de riesgos más críticos, ya que el descuido de estos, provocaría una pérdida de dinero significativa a la empresa por cada hora que estuviera fuera de servicio.

CONCLUSIONES

La seguridad de las redes de comunicaciones, y concretamente el Internet, evoluciona a pasos agigantados cada minuto que transcurre. Nuevas vulnerabilidades y utilidades, tanto para explotarlas como para combatirlas, son distribuidas públicamente en la red. La información disponible al respecto es inmanejable, por lo que el diseño de un sistema de seguridad debe basarse en la fortaleza de las tecnologías empleadas, y no en la ocultación de las mismas.

La seguridad de la empresa XYZ S.A., no debe basarse en una sola técnica de protección, sino que debe ser reforzada por varias metodologías que permitan monitorear y gestionar cada uno de los aspectos de la red. LA gerencia junto con el Administrador de la red, tendrán que revisar periódicamente los procedimientos y políticas actuales y actualizarlas de ser necesario, de tal forma que estas se ajusten conforme avanzan las vulnerabilidades del sistema informático. Además hay que concienciar y capacitar a los usuarios en lo que concierne a seguridad informática.

Finalmente, con nuestro trabajo por lo menos estamos asegurando el 60% en los tres pilares fundamentales de la seguridad como son la integridad de la información, la privacidad y la confidencialidad.

REFERENCIAS

a) Tesis
M. Dolores Cerini Y Pablo Ignacio Prá "Plan De Seguridad Informática" (Tesis, Facultad De Ingeniería En Sistemas, Universidad De Córdova, 2002).

b) Tesis
Antonio Villalón Huerta, "Seguridad En Unix Y Redes" (Tesis, Universidad Politécnica de Valencia, Versión 2.1, 2002)

c) Tesis
Cristian F. Borghello, "Seguridad Informática: Sus implicancias e implementación" (Tesis, Universidad Tecnológica Nacional de Argentina, 2001).

d) Libro
Red Hat, Inc., Red Hat Linux 9: Red Hat Linux Security Guide, (2002).

e) Artículo de Internet
Kaleem Anwar Muhammad Amir Ahmad Saeed Muhammad Imran, "The Linux Router", Revista Linux Journal, Jueves 01 agosto, 2002. http//www.linuxjournal.com

f) Artículo de Internet
Ricky M. Magalhaes. "Host-Based IDS vs Network-Based IDS, Part 2 - Comparative Analysis", Windows Security, Jul 23, 2004. http://www.windowsecurity.com/articles/Hids_vs_Nids_Part2.html.

g) Sitios Web consultados

Qmail, Agente de Transporte de Correo
http://www.qmail.org

h) Sitios Web consultados

Comparativas de Proxies
http://cacheoff.ircache.net/

_____
Ing. Albert Espinal Santana, M.S.I.G
Director de Tópico