

UNIVERSIDAD TECNOLÓGICA ISRAEL
FACULTAD DE SISTEMAS INFORMÁTICOS

ELABORACIÓN DE POLÍTICAS DE SEGURIDAD DIRIGIDO A
WEBMASTERS PARA PREVENIR ATAQUES DDOS A PORTALES
WEB

Estudiante

Víctor Alejandro Cáceres Puma

Tutor:

Ing. Marco Lituma

Cuenca Ecuador

Diciembre 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL
FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Marco Lituma, certifico que el señor Víctor Alejandro Cáceres Puma con C.C, No. 0104509971 realizó la presente tesis con el título “Elaboración de Políticas de Seguridad dirigido a Webmasters para prevenir ataques DDoS a Portales Web”, y que es autor intelectual del mismo, que es original, autentico y personal.

Ing. Marco Lituma

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

ACTA DE CESIÓN DE DERECHOS

Yo, Víctor Alejandro Cáceres Puma con C.C. N° 0104509971, autor del Proyecto TTP denominado **“Elaboración de Políticas de Seguridad dirigido a Webmasters para prevenir ataques DDoS a Portales Web”** presentado como requisito para optar el título de **Ingeniero en Sistemas Informáticos**, autorizo a la Universidad Tecnológica Israel para que con fines académicos, muestre al mundo la producción intelectual de la Universidad. A través de la visibilidad de su contenido de la siguiente manera:

- Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Biblioteca General y en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad Tecnológica Israel
- Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato impreso, CD-ROM o digital desde Internet, Intranet, etc. Y en fin cualquier formato conocido o por conocer.

Víctor Alejandro Cáceres Puma / C.C. 0104509971

UNIVERSIDAD TECNOLÓGICA ISRAEL
FACULTAD DE SISTEMAS INFORMÁTICOS

CERTIFICADO DE AUTORIA

El documento de tesis con título **“Elaboración de Políticas de Seguridad dirigido a Webmasters para prevenir ataques DDoS a Portales Web”** ha sido desarrollado por Víctor Alejandro Cáceres con C.C, 0104509971 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

Victor Alejandro Cáceres Puma

C.C. 0104509971

DEDICATORIA

Para poder llegar hasta este punto en mi vida estuvo una mujer al pie de la lucha conmigo apoyándome incansablemente con trabajo, sudor, lagrimas, ella es el pilar fundamental en mi vida, aquella mujer es mi madre, esa palabra lleva en sus letras el valor, coraje, humildad y perseverancia, valores que me enseñó, a pesar de todo lo que hemos tenido que afrontar, mi madrina un pilar fundamental en mi niñez, mi abuelita que pese a su estado de salud es infalible con sus consejos, y no puede faltar el cariño de mi hogar apoyándome en todo momento, así que esta tesis va dedicada a las 6 mujeres más importantes de mi vida, MamiAlicia, Mamirrebe, Mamirosa, Mary y mi princesa Leslie, y a mi madre celestial que apoya mis decisiones y me da fortaleza cuando lo necesito, Virgen del Cisne.

AGRADECIMIENTO

Agradezco a Dios por haberme dado la vida y poder disfrutar de las alegrías y tristezas que nos da la vida, y lo maravilloso que es compartir con los demás.

De manera especial agradezco a los profesores que confiaron en mí y apoyaron mi decisión de seguir adelante, para ello estuvieron presentes Ing. Freddy Narváez, Ing. Leopoldo Pauta e Ing. Marco Lituma, personas capaces que día a día buscan el bienestar estudiantil como meta en sus vidas.

RESUMEN

En los últimos años, las amenazas a los activos de una empresa no solamente se lo realizan físicamente, mediante robos, extorsiones etc. O tal vez por razones catastróficas, climáticas, sino con el gran auge de la tecnología que se ha venido implementando en las empresas desde una Pymes hasta una multinacional, los riesgos de sufrir pérdidas de información o vulnerabilidad en sus activos es más propenso.

Razón por la cual el objetivo de esta tesis es preparar al webmaster de la Empresa Interactive by Zenix para estar preparado para los ataques denominados DdoS(Ataques de Denegación de Servicio Distribuido), el cual se encuentra en auge e implementado por hackers para sus diversas acciones, ya que en los últimos meses se recibió correos con amenazas de hacer colapsar las redes de la empresa a nivel nacional a travez de DdoS.

Este tipo de ataque se encuentra bajo la mayor demanda por parte de hackers en especial Anonymous, los cuales los han utilizado para atacar a webs de carácter político, gubernamental e incluso webs de la policía en diversos lugares del planeta.

Una vez estudiadas todas las políticas que se pueden incorporar en el área de sistemas, se logrará disminuir la probabilidad de sufrir un ataque de este tipo.

SUMMARY

In recent years, threats to the assets of a company are done not only physically, through theft, extortion and so on. Or perhaps for reasons catastrophic weather, but with the growth of technology has been implemented in companies from Pymes to a multinational one, the risks of loss or vulnerability information assets are more likely.

Which is why the aim of this thesis is to prepare the webmaster by Interactive Company Zenix to be prepared for so-called DDoS attacks (Attacks Distributed Denial of Service), which is booming and implemented by hackers for their various actions because in recent months received emails with threats of collapse the company networks nationwide DdoS trough.

This type of attack is under increased demand by Anonymous hackers in particular, which have used to attack political websites, government websites and even the police in various parts of the planet.

After studying all the policies that can be incorporated into the systems area will be achieved reducing the likelihood of an attack of this kind.

TABLA DE CONTENIDOS

1. TEMA DE INVESTIGACION	17
1.1 Planteamiento del Problema	17
1.1.1 Antecedentes	17
1.2 Diagnóstico o planteamiento de la problemática general.	19
1.2.1.1 Causa – Efecto	19
1.2.2 Pronóstico y Control de Pronóstico	20
1.2.3 Análisis Costo Beneficio.....	21
1.2.3.1 Costos	22
1.2.3.2 Beneficio	23
1.2.3.3 Relación Costo - Beneficio.....	24
1.2.3.4 Conclusión.....	25
1.3 Formulación de la Problemática Específica.....	25
1.3.1 Problema Principal	25
1.3.2 Problemas Secundarios	25
1.4 Objetivos.....	26
1.4.1 Objetivo General.....	26
1.4.2 Objetivos Específicos.....	26
1.5 Justificación	26
1.5.1 Teórica	27
1.5.2 Metodológica	28
1.5.3 Práctica	28
1.6 Marco de Referencia.....	29
1.6.1 Marco Teórico	29
1.6.2 Marco Espacial	38
1.6.3 Marco Temporal.....	39
1.7 Metodología y Cronograma.....	39
1.8 Plan Analítico	41

2. INTRODUCCION	45
3. MARCO DE REFERENCIA.....	47
3.1. Marco Teórico	47
3.1.1. Política.....	47
3.1.1.1. Políticas de Privacidad	48
3.1.1.2. Políticas de Uso de Correo Electrónico	48
3.1.1.3. Política de Vínculos.....	49
3.1.1.4. Políticas Antispam.....	49
3.1.2. Seguridad Informática.....	50
3.1.2.1. Panorámica General de la Informática.....	51
3.1.2.2. Importancia de los mecanismos de Seguridad.....	53
3.1.2.3. Intercambio de información.....	53
3.1.2.4. Instalación de software dañino involuntariamente	54
3.1.2.5. Protección ante accesos no autorizados.....	55
3.1.2.6. Fallos de seguridad en la utilización del software	56
3.1.3. Auditoria Informática	57
3.1.4. Webmaster	59
3.1.5. DDOS	60
3.1.6. Portales Web.....	64
3.2. Marco Temporo/Espacial	66
3.3. Marco Legal	66
4. METODOLOGIA.....	68
4.1. Métodos	68
4.2. Técnicas	69
4.3. Instrumentos	69
5. IMPORTANCIA DE LA INFORMACION.....	77
5.1. Datos e información.	77
5.2. Sistemas de Información.....	78
5.2.1. Calidad de la Información:	78
5.2.2. Oportunidad De La Información:.....	78
5.2.3. Cantidad de Información:	79

5.2.4.	Relevancia de la Información:	79
5.3.	La información como el activo más importante dentro de la empresa	79
5.3.1.	¿Qué valor tiene proteger la información?	80
5.4.	El valor de la información en las empresas	81
5.5.	SGSI	82
5.5.1.	¿Cuál es la diferencia entre Seguridad de la Información e Informática? ...	84
5.5.2.	Objetivos de la implementación de un SGSI.....	85
5.6.	Certificación de Seguridad	85
5.6.1.	Importancia de la Certificación	85
5.7.	ISO 27001	86
5.7.1.	La serie 27000	87
5.7.2.	Implantación de la Certificación	88
5.7.3.	Beneficios de la Implementación de ISO 27001.....	89
5.8	Conclusiones	90
6.	NORMAS DE SEGURIDAD WEB Y CREACION DE PAGINAS WEB SEGURAS ...	91
6.1.	Antecedentes	91
6.2.	Normativas para aplicaciones Web Seguras.	91
6.2.1.	Autenticación.....	92
6.2.2.	Autorización.....	93
6.2.3.	Gestión de Cookies.....	94
6.2.4.	Validación de Entrada de Datos.....	94
6.2.5.	Gestión de Errores / Fuga de Información	95
6.2.6.	Log / Auditoría.....	96
6.2.7.	Cifrado de Datos.....	96
6.2.8.	Entorno de Código Seguro	97
6.2.9.	Gestión de Sesiones (Login / Logout).....	98
6.3.	Conclusión.....	98
7.	PREPARAR AL WEBMASTER PARA POSIBLES ATAQUES WEB FUTUROS. ...	100
7.1.	Implementación de Métodos de Seguridad Físico/Lógico.....	100
7.2.	Firewall	101
7.2.1.	Servidor Firewall	102

7.2.2.	Ventajas y Desventajas de un Firewall	103
7.3.	DMZ (Zona Desmilitarizada).....	104
7.3.1.	Arquitectura DMZ	105
7.3.2.	Características	105
7.8	Conclusión	106
8.	DDOS	108
8.1.	Introducción	108
8.2.	Redes Ip	108
8.3.	Importancia del Internet.....	111
8.4.	Ataques en redes IP.....	112
8.5.	Características Generales del ataque	113
8.6.	Definición de DDoS.....	114
8.7.	Virus y Ataques DdoS	115
8.8.	Propagación a través de Virus	115
8.9.	Clasificación de los ataques DDOS.....	116
8.10.	Consumo de Ancho de Banda.....	117
8.10.1.	Ataques directos.....	118
8.10.2.	Ataques indirectos.....	118
8.11.	Modelos de Ataque DDoS.....	119
8.11.1.	Trinoo	120
8.11.2.	<i>Tribe Flood Network</i>	124
8.11.3.	<i>Tribe Flood Network 2000 (TFN2K)</i>	127
8.11.4.	<i>Stacheldraht</i>	130
8.11.5.	<i>Shaft</i>	132
8.11.6.	<i>Mstream</i>	135
8.11.7.	<i>LOIC</i>	138
9.	POLÍTICAS DE SEGURIDAD.....	140
9.1.	Desarrollo de Políticas	142
9.2.	Políticas a implementar.....	143
9.3.	Plan de Contingencia.....	150
9.4.	Consideraciones	152

9.5. Conclusión	153
10. CONCLUSIONES Y RECOMENDACIONES	155
10.1. Conclusiones	155
10.2. Recomendaciones	156
11. BIBLIOGRAFIA	157
12. ANEXOS.....	161
12.1. Portada del Blog.....	161
12.2. Pregunta 1	161
12.3. Pregunta 2	161
12.4. Pregunta 3	162
12.5. Pregunta 4	162
12.6. Pregunta 5	162
12.7. Pregunta 6	162
12.8. Pregunta 7	162
12.9. Pregunta 8	163

LISTA DE ANEXOS

Anexo. 1 Portada de Blog	97
Anexo. 2 Pregunta 1	97
Anexo. 3 Pregunta 2	97
Anexo. 4 Pregunta 3	98
Anexo. 5 Pregunta 4	98
Anexo. 6 Pregunta 5	98
Anexo. 7 Pregunta 6	98
Anexo. 8 Pregunta 7	98
Anexo. 9 Pregunta 8	98

LISTA DE CUADROS Y GRAFICOS

Fig. 1 Ilustración de Seguridad en Redes	47
Fig. 2 Portales Web.....	64
Fig. 3 Pregunta 1.....	69
Fig. 4 Pregunta 2.....	70
Fig. 5 Pregunta 3.....	71
Fig. 6 Pregunta 4.....	72
Fig. 7 Pregunta 5.....	73
Fig. 8 Pregunta 6.....	73
Fig. 9 Pregunta 7.....	74
Fig. 10 Pregunta 8.....	75
Fig. 11 Conclusión	76
Fig. 12 Datos e Información	77
Fig. 13 Funcionamiento de un SGSI	83
Fig. 14 Estándar ISO.....	86
Fig. 15 Diagrama físico de la red de Serv. y Servicios de Internet de la CNT....	101
Fig. 16 Firewall.....	103
Fig. 17 Funcionamiento de un DMZ	106
Fig. 18 Modelo OSI (4 Capas).....	109
Fig. 19 Ruteado de paquetes por Internet.....	111
Fig. 20 Ataque típico DDOS.....	114
Fig. 21 Ataques DOS/DDOS directos e indirectos.	119

Fig. 22 Ataque Trinoo.....	122
Fig. 23 Ataque Trinoo – Inundación por tramas	123
Fig. 24 Tramas de sincronización TCP	124
Fig. 25 Control de ataque Tribe Flood.....	125
Fig. 26 Escenario Tribe Flood Network 2000	127
Fig. 27 Escenario Stacheldraht	130
Fig. 28 Comunicación Shaft	133
Fig. 29 Cifrado de César	134
Fig. 30 Modalidad MStream	136
Fig. 31 Utilización LOIC	139
Fig. 32 Transición de un Plan de Contingencia.....	150

CAPITULO I

1. TEMA DE INVESTIGACION

Elaboración de Políticas de Seguridad dirigido a Webmasters para prevenir ataques DDoS a Portales Web.

1.1 Planteamiento del Problema

1.1.1 Antecedentes

En los últimos años todo lo relacionado con la seguridad informática suscita un gran interés. Las empresas y particulares están más concienciados de los riesgos que conlleva su actividad electrónica. Esto es un hecho. También lo es que el desconocimiento general sobre estos temas todavía es demasiado grande. Hace mucho tiempo que este tema se convirtió por derecho propio en una rama específica de la informática.

Cada día se publican decenas de nuevos fallos en el software que utilizamos habitualmente. Hay cientos de sitios en Internet que ofrecen información, herramientas y métodos para vulnerar sistemas informáticos. Cada mes se publican nuevos libros con información sobre seguridad.

En vista a varios ataques a diversos Sitios Web uno de ellos la Empresa **Interactive by Zenix** para lo cual esta empresa cayo por dos días en vista que no pudo retomar sus servicios, debido a la infraestructura que posee al momento, además no cuenta con una correctas políticas dentro de la empresa para que en futuras ocasiones generen perdidas grandes como se dieron dentro de esta organización. La amenaza fue recibida por Anonymous al momento que empezaron a atacar a las paginas gubernamentales del país por la fecha del 10 de agosto del presente año, en la cual la amenaza fue hacer caer a los

principales ISP a nivel Nacional y entre ellos esta empresa, el mensaje por parte de estos activistas hackers se lo recibió vía e-mail a nivel nacional con el texto que indicaba las vulnerabilidades que presentaba la empresa.

Es necesario implementar este tema como suplemento hacia las diversas herramientas que existen en la actualidad para poder prevenirlos.

Y para este tipo de control existen diferentes tipos de Webmasters de acuerdo con el tipo de monitoreo que realizan en la web. Pero **nos centraremos en uno solo, aquel que custodie la información de un ISP, al cual tenemos el acceso.**

Estos les convierten en los custodios de la información que está a su cargo, ya que es lo más importante dentro de una organización un empresa, estas personas son las que deben estar preparadas para la creación, mantenimiento y soporte de los sitios web desarrollados.

Del mismo modo que en la vida cotidiana la seguridad es parte de nuestro comportamiento, con el tiempo también lo será en nuestro quehacer informático. La seguridad informática ha entrado en nuestras vidas impetuosamente, y está para quedarse.

Desde 1990 hasta nuestros días, se viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

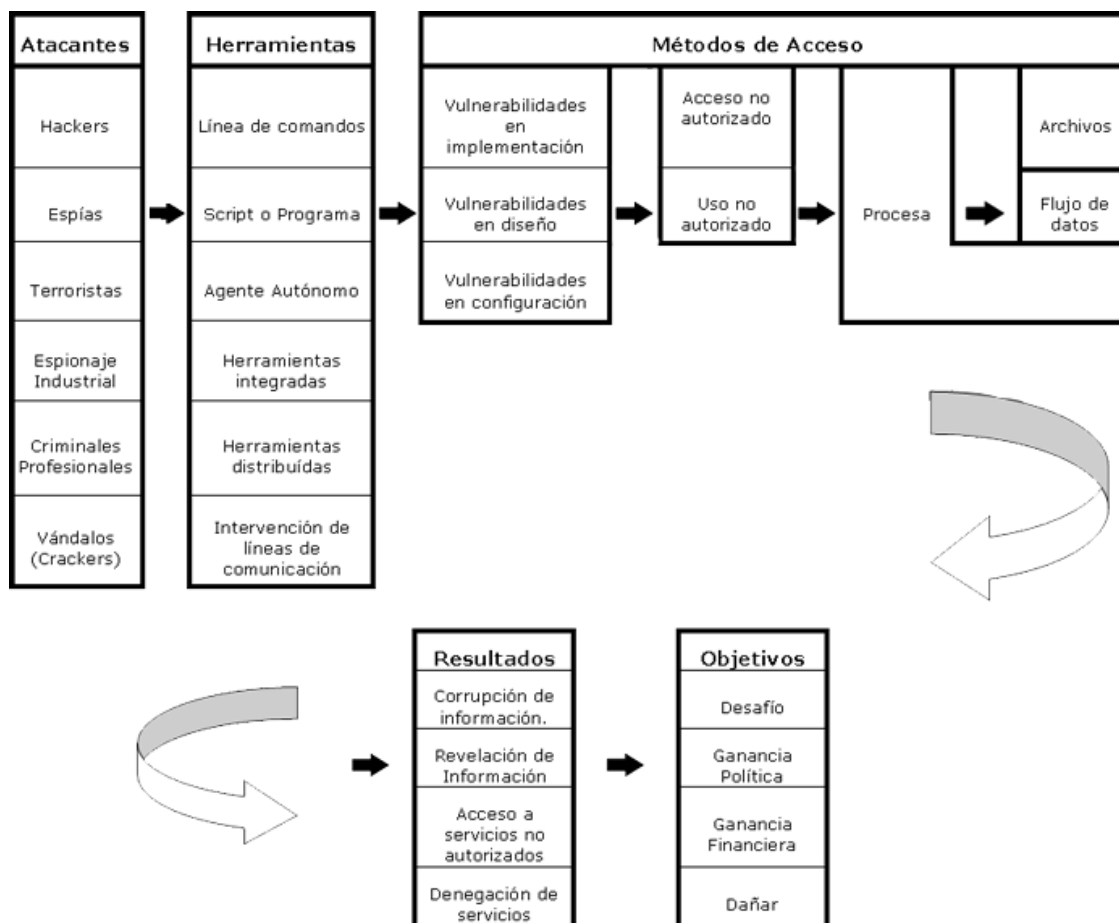


Tabla 7.2. Detalle de Ataques. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6-Página 71

1.2 Diagnóstico o planteamiento de la problemática general.

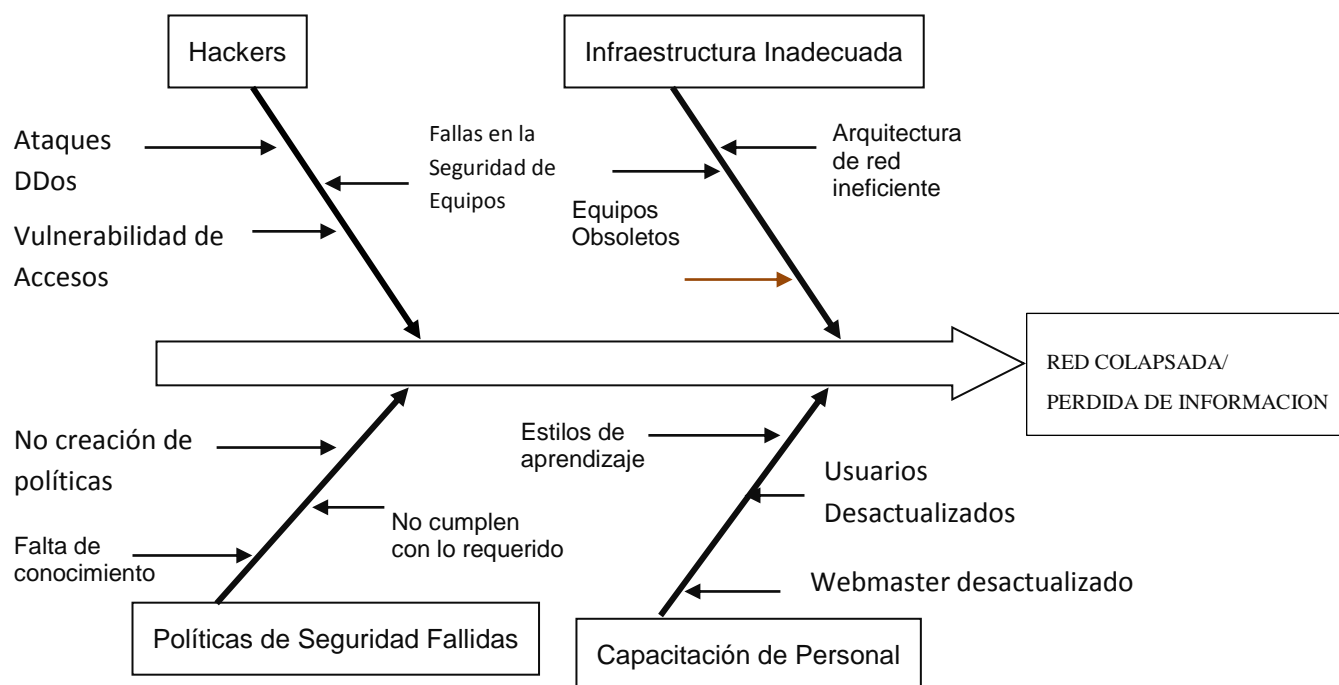
1.2.1.1 Causa – Efecto

Los causantes de estos ataques son personas denominada Hackers, los cuáles para demostrar sus habilidades, realizan ingresos no permitidos a Sitios Web en especial de Gobierno. Y están deberían ser controladas conjuntamente con aspectos técnicos que cumplan las características de seguridad correctas, llevadas de forma exhaustivamente correcta en todos sus puntos.

La indiferencia ante la seguridad que se debería tener implementado en los sitios web, hace que estas no cumplan con las normas de seguridad pertinentes

Con estas políticas lo que se obtendrá será mantener un Departamento de Sistemas conjuntamente con el Webmaster que cumpliendo paso a paso los puntos requeridos podrá prever y responder a los ataques web que se susciten en cualquier momento.

En conclusión tendría como causa la pérdida de información y colapso de sistemas web provocando pérdida de recursos económicos y tecnológicos en los que se verían afectados principalmente los aspectos financieros de una empresa.



1.2.2 Pronóstico y Control de Pronóstico

La mayoría de los protocolos de comunicación utilizados carecen de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación.

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.
- ***Existen constantes amenazas a los Portales Web.***

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de sus clientes bajaría enormemente.

Los Administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.

Los "advisories" (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, sería una de las formas en las que se estaría controlando esta falta de conocimiento y así los fallos de la seguridad serían controlados de manera oportuna. Se tomara en cuenta los Certificados emitidos por Software Engine Institute para la creación de las políticas de seguridad correspondientes.

1.2.3 Análisis Costo Beneficio

La técnica de análisis costo beneficio, tiene como objetivo fundamental proporcionar una medida de la rentabilidad de un proyecto, mediante la comparación de los costos previstos con los beneficios esperados en la realización del mismo.

1.2.3.1 Costos

Descripción	Cantidad	Costo Mensual	Costo	Costo total
Hardware Nuevo (Firewall - IDS . Routers)	3	n/a	\$ 2.500,00	\$ 2.500,00
Software Nuevo	3	n/a		\$ 950,00
Actualización Software	20	n/a	\$ 199,99	\$ 3.999,00
Sistema de Backup	4	n/a	\$ 850,00	\$ 3.400,00
ISP Alternativo	1	n/a	\$ 2.890,00	\$ 2.890,00
Capacitación Personal / Políticas	8	\$ 100	\$ 800,00	\$ 800,00
				\$ 14.539,00

- **Hardware Nuevo** Se realizara la adquisición de 3 equipos nuevos 1 Equipo Hp Proliant donde se instalara e Software Firewall, un Router Cisco con sistema IDS y un Equipo Zyxel USG 1000.
- **Software Nuevo** se comprará 1 Software Firewall Network Shield Firewall
- **Actualización (Software)** de computadoras Dell con Windows Xp SP2 a Windows 7 Home Premium
- **Sistema de Backup** - HP ProLiant ML110 G2 Server series utilizado para réplicas de Servidores de Aplicaciones, Web, Mail y BD.
- **ISP Alternativo** – Contratar un Isp alternativo que nos brinde servicio secundario.

- **Capacitación de personal** Ingeniero en Sistemas que estará visitando organización brindando adiestramientos de las políticas implementadas, se calcula dos meses con una vez por semana con una duración de 1 hora.

1.2.3.2 Beneficio

Descripción	Beneficio en Cifras
Hardware Nuevo (Firewall - IDS . Routers)	\$ 7.000,00
Software Nuevo ()	\$ 1.500,00
Actualizacion Software	\$ 6.000,00
Sistema de Backup	\$ 20.000,00
ISP Alternativo	\$ 5.500,00
Capacitacion Personal / Políticas	\$ 5.000,00
	\$ 45.000,00

Hardware Nuevo Obteniendo un hardware nuevo se estará menos expuesto a ataques por equipos obsoletos generando una ganancia del 70% debido a que no se perderá información y los servicios seguirán funcionando

- **Software Nuevo** Con la adquisición de este software Firewall se tendrá un mayor control de permisos de entrada y salida de conexiones de los usuarios locales y remotos.

- **Actualización (Software)** Al momento de realizar el Upgrade W7 se tendrá mayor protección en cuanto a parches y será más versátil con aplicaciones actualmente existentes.
- **Sistema de Backup** – Al adquirir los servidores Hp se colocaran replicas online de servidores en otro lugar de la ciudad o país.
- **ISP Alternativo** si existiere una amenaza que actúe infringiendo nuestras políticas y por ende cause daños en el sistema de la empresa, se contara un ISP alternativo que se encuentre online para poder seguir ofreciendo nuestros servicios.
- **Capacitación de personal** Todas las personas dentro de la empresa se someterán a capacitaciones e incentivos por mantener un orden específico dentro de la empresa generando así mayores ganancias y menos gastos en cuanto a mantenimiento de equipos.

Todos estos valores se los a calculado en base al dinero que mueve la empresa diariamente con cobros por servicio de Internet, Hosting, Mail y Asesoría.

1.2.3.3 Relación Costo - Beneficio

Una vez obtenido los costos y beneficios respectivos del proyecto se presenta la siguiente tabla.

Descripción	Costos	Beneficios	Beneficio/ Costo	Deseable	
				S	N
Hardware Nuevo (Firewall - IDS . Routers)	\$ 2.500,00	\$ 7.000,00	\$ 2,80	x	
Software Nuevo ()	\$ 950,00	\$ 1.500,00	\$ 1,58	x	
Actualización Software	\$ 3.999,00	\$ 6.000,00	\$ 1,50	x	
Sistema de Backup	\$ 3.400,00	\$ 20.000,00	\$ 5,88	x	
ISP Alternativo	\$ 2.890,00	\$ 5.500,00	\$ 1,90	x	
Capacitación Personal / Políticas	\$ 800,00	\$ 5.000,00	\$ 6,25	x	

1.2.3.4 Conclusión

Al revisar las cifras propuestas e investigadas podemos observar que en todo cambio que implementaremos tendremos una utilidad que nos solventa que el proyecto a implementar es factible ya que no genera pérdidas y se recuperara el valor en un año.

1.3 Formulación de la Problemática Específica

1.3.1 Problema Principal

Se origina en los diversos ataques a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima, generando pérdida de recursos (información, tecnología, financieros).

1.3.2 Problemas Secundarios

Si tomamos en cuenta el problema principal asimilando un ataque DDoS a una Entidad Financiera de Carácter Importante en la Economía, derivamos los problemas secundarios de este tenemos lo siguiente:

- Información Privada divulgada a los medios.
- Quiebre de Empresas por no cumplir una transacción fundamental determinada.
- Crisis económica al atacar una web principal en el ámbito de negocios.
- Falta de Confianza de las personas que confían información a este medio.

1.4 Objetivos

1.4.1 Objetivo General

Elaborar una guía de Políticas de Seguridad dirigido a Webmasters para actuar frente a ataques DDoS a Portales Web.

1.4.2 Objetivos Específicos

- Crear Normas de Seguridad contra ataques web
- Preparar al Webmaster para posibles ataques web futuros
- Explicar la importancia de la información como activo estratégico
- Ejemplificar los mecanismos de implantación de ataques DDoS
- Proteger la información que los Webmasters tienen a su custodia.
- Evitar la pérdida de información y recursos tecnológicos en base a las políticas implantadas.

1.5 Justificación

1.5.1 Teórica

Hoy en día las empresas que no se han preocupado por su seguridad pierden miles de millones de dólares en **los ataques DDoS** en todo el mundo. Miles de empresas en especial en constante búsqueda de las soluciones para prevenir ataques al servidor. Se tomará en cuenta los diferentes tipos de ataques ya suscitados como una forma de guía de lo que no se debería hacer.

A esto se le puede acotar las características principales de los temas a seguir en este módulo:

➤ DDoS

- Podríamos definir los ataques DOS (Denegation Of Service) como la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

➤ Hacker

- En la actualidad se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación para vulnerarlos y así sacar provecho.

➤ Seguridad Informática

- Se la considera como una derivada de la informática en vista de la constante implementación que se necesita aplicar en los diversos sistemas ya sean estos web o

de escritorio. Para ello se ha definido una serie de estándares, protocolos, métodos, etc. y así minimizar los riesgos suscitados en cualquier ámbito informático.

➤ Portal Web

- Es un conjunto de páginas web y que ofrecen información, herramientas y/o servicios a sus usuarios, de esta manera se le brinda al usuario, la facilidad de poder encontrar en dicho sitio todas sus necesidades sin salir de dicho portal.

1.5.2 Metodológica

Obteniendo todas las características que se encuentran implementadas en los diferentes sitios administrables, se podría crear una metodología que ofrezca los pasos correctos para llegar a obtener los resultados esperados, la información que se recopilara será en base a preguntas realizadas a diferentes webmasters de ISP que conocen los distintos tipos de ataques que han sido víctimas, y en caso de no haber receptado algún tipo de ataque se revisa las opiniones para crear las preguntas referentes a la seguridad del sitio.

La Metodología de la investigación se realizará en base a una encuesta electrónica o blog en la cual se invitara a Webmasters ISP que indiquen sus puntos de vista para sacar así un control estadístico de los sucesos relacionados en ataques hacker y llegar a posibles soluciones.

1.5.3 Práctica

En función de lo planteado anteriormente lo que se obtendrá es el manejo y administración de un Portal Web con su debido plan de contingencia en caso de ataque y

como mantener este sitio con las seguridades necesarias para que no sean violentadas en base a políticas generadas.

1.6 Marco de Referencia

1.6.1 Marco Teórico

Política

La **política** es una actividad orientada en **forma ideológica** a la toma de decisiones de un grupo para alcanzar ciertos objetivos (<http://definicion.de/politica/>). En informática se pretende aprovechar el potencial que ofrecen las Tecnologías de la Información con las que se cuentan actualmente.

De ellas podemos destacar o clasificar que las Políticas en cuanto a La protección de Datos Personales e Información, Redes y Telecomunicaciones son las que dentro de la informática tienen mayor importancia.

En cuanto a la Protección de Datos Personales e Información se promueve la confidencialidad de los datos personales y por ende la protección jurídica de la información producida en los sistemas de las Instituciones, por lo



que se establece que todos los sistemas y bases de datos que procesen o almacenen datos personales, deberán contar con políticas de administración de claves de acceso y medidas de seguridad lógica.¹

¹ Ley de Acceso a la Información Pública para el Estado Ecuatoriano.

Seguridad Informática

Es el estado de bienestar de la información y las infraestructuras, en las cuales la posibilidad que puedan realizarse con éxito y sin detectarse, el robo, alteración y parada del flujo de información, se mantienen en niveles bajos o tolerables. (Seguridad Informática – Unai Arronategui, s/a)

La seguridad informática es una derivada de la informática en vista de la constante implementación que se necesita aplicar en los diversos sistemas ya sean estos web o de escritorio. Para ello se ha definido una serie de estándares, protocolos, métodos, etc. y así minimizar los riesgos suscitados en cualquier ámbito informático.

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

a) Seguridad en Redes

Mantiene bajo protección los recursos y la información con que se encuentran en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado.

b) Seguridad Global

En cuanto a este tipo de red se la puede incluir todo tipo de recursos informáticos dentro de una organización, empresa u oficina, aun cuando estos no estén interconectados como las Redes de Área Local (LAN), Redes de Áreas Metropolitanas (MAN), Redes Nacionales e Internacionales Grandes (WAN) y Computadores personales, pequeños y grandes sistemas (<http://www.arcert.gov.ar>).

De manera que seguridad Global es mantener bajo protección todos los componentes de la red global. Además debemos tener en cuenta que dentro de un sistema los Usuarios son la parte que no hay que olvidar ni menospreciar, debido a que siempre hay que tener en cuenta que la seguridad comienza y termina con las personas.

Auditoria Informática

Conceptualmente la auditoria, toda y cualquiera Auditoria, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que las han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

1) Contenido	Una opinión
2) Condición	profesional
3) Justificación	Sustentada en determinados procedimientos
4) Objeto	Una determinada

	información obtenida en un cierto soporte
5) Finalidad	Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad

En todo caso es una función que posteriormente se somete a una relación con las actividades ya realizadas, sobre las que hay que emitir una opinión, tomando en cuenta las entidades que rigen este tipo de normas como ISACA² y COBIT³ (Auditoría Informática – Un enfoque práctico, Mario G. Piatini & Emilio del Peso /2001)

Además cuenta con los mecanismos para poder determinar qué es lo que sucede en el sistema, que es lo que hace cada uno de los usuarios, los tiempos y fechas de dichas acciones.

Estos dos últimos puntos son de extrema importancia, ya que en base a esto se diferencia entre “espíar” y “monitorear”, a sus usuarios, demostrando así la ética implantada por cada uno de sus administradores.

Finalmente todos estos aspectos y servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar

² Information System Audit and Control Association.

³ Control Objectives for Information and Related Technology

pasar por alto cuestiones importante con las que señalan dichos servicios. De esta manera es posible aplicar los derechos efectivos entre usuarios y administradores.

Webmaster

Debe tener habilidades de análisis de problemas, capacidad para razonamiento abstracto, proyección a futuro y resolución de problemas y muy útil tener cierta habilidad para el análisis de procesos.

Dependiendo del rol que juegue el Webmaster en una empresa, se especializará en un área en particular o deberá ir adquiriendo pericia en algunas tareas tales como Administración y Mantenimientos de Sistemas Web.

(<http://www.webtaller.com/maletin/articulos/definicion-webmaster.php>)

El webmaster es el sujeto principal en esta relación debido q que es la persona indicada en administrar los sitios web y estar pendiente a la notificación de algún ataque, además es el encargado y custodio de la información que está a su cargo, y a su vez hacer cumplir las normas y políticas generadas por la empresa.

DDOS

Se los define como Ataques Distribuidos de Denegación de Servicios⁴, este impide que los usuarios de un determinado sistema no puedan acceder a él, y por consiguiente a los servicios que proporciona. En las circunstancias actuales de la globalización, el daño económico y de imagen que sufre una empresa por un ataque de este tipo probablemente

⁴ En ingles Distributed Deny of Service

sea mucho mayor que el derivado de una simple intrusión; anteriormente con ataques DoS se enviaba ataques masivos a una maquina con el fin de imposibilitar la misma, pero en la actualidad con mecanismos más sofisticados y empleando las debilidades de los protocolos TCP/IP se puede generar grandes cantidades de paquetes sobre un sistema concreto lo que genera que el servicio quede inoperante.

Los ataques DoS se pueden ejecutar de manera coordinada a partir de varias fuentes al mismo tiempo (Distributed DoS, DDoS). Un ataque de denegación de la lógica se basa en una explotación inteligente de vulnerabilidades en el blanco. Por ejemplo, una dirección IP hábilmente construidas fragmentada datagrama se puede bloquear un sistema debido a un fallo grave en el software del sistema operativo (SO). Otro ejemplo de un ataque de la lógica es explotar falta de autenticación de requisitos mediante la inyección de información de enrutamiento falsa para evitar que el tráfico llegue a la víctima de la red

Entre los ataques DDoS más utilizados tenemos los siguientes:

- Trinoo
 - La forma en la que este tipo de ataque toma forma o se basa es en cuanto a que un sistema vulnerado deposita un repositorio de herramientas compiladas tales como: rastreo, ataque, Sniffers⁵, root kits. Este sistema poseerá un gran número de usuarios, y por consiguiente, una gran potencia de proceso y amplio ancho de banda en sus comunicaciones
- Tribe Flood Network

⁵Sniffer: Herramienta software que permite capturar y analizar todo el tráfico que circula por un segmento de red.

- Compuesto por un conjunto de programas clientes y demonios que implementan una herramienta de denegación de servicio distribuida, capaz de generar ataques por generación masiva de paquetes ICMP, SYN o UDP, así como ataques del tipo Smurfing⁶.
- Tribe Flood Network 2000 (TFN₂K)
 - Es una evolución del anteriormente comentado TFN.
 - De esta forma, se denomina Maestro al sistema informático en el que corre el Cliente, y Agente al sistema informático donde se ejecuta el Demonio. El TFN₂K permite a los Maestros explotar los recursos de un determinado número de Agentes con el fin de coordinar un ataque a una o más víctimas. El Maestro configura a los Agentes para atacar a una determinada lista de víctimas. Los Agentes atacan a las víctimas por inundación de paquetes.
- Stacheldraht
 - Dispone de un mecanismo similar a un Telnet (Stacheldraht Term) para la comunicación del cliente con el conductor que incluye cifrado mediante el uso de clave simétrica. Una vez establecida la comunicación entre el cliente y el conductor, se solicita un password que está cifrado mediante criptografía. A partir de ese momento toda la comunicación se realiza de forma cifrada mediante el algoritmo Blowfish.
- Sahft
 - En este tipo de ataque la comunicación entre los distintos niveles se lo utiliza de la siguiente forma:
 - Cliente a Conductor: 20432/TCP

⁶ Smurfing: Amplificación de peticiones broadcast.

- Conductor a Agente: 18753/UDP
- Agente a Conductor: 20433/UDP

Una de las novedades que presenta esta herramienta es el uso de *tickets* para garantizar el control sobre los agentes. Tanto el *password* como el *ticket* deben ser correctos para que un agente acepte las peticiones que le puedan llegar.

- Mstream

- Un ataque de este tipo presenta los siguientes síntomas: El sistema objeto del ataque baja su rendimiento debido al consumo de CPU por el tráfico de red que debe atender.

Se observa un consumo elevado de ancho de banda en la red como consecuencia del propio ataque. El sistema atacado ocupa aún más ancho de banda al intentar contestar con ramas TCP RST a los falsos remitentes de las tramas TCP ACK. Los routers contestarán a la víctima con tramas ICMP indicando que el destinatario de la trama TCP RST no existe, lo que también consume aún más ancho de banda.

Aunque cuando este tipo de ataque proviene de un único sistema no suele producir grandes efectos en el sistema atacado, pero cambia el panorama cuando son varios los sistemas atacados y muchos los atacantes, pues sólo tiene un enlace como la saturación de la red, si no la caída del sistema atacado, y por consiguiente la denegación de servicio, que es el objetivo final.

La arquitectura de este sistema es similar a los anteriormente vistos:

(Sistemas Distribuidos de Denegación de Servicio – Autor: Fernando Limón Martínez – Madrid, Junio de 2000)

Portales Web

Un portal es básicamente la “portada” de un grupo de Web Sites individuales que comparten la temática de su contenido, resumiendo la más relevante información de cada uno de éstos y permitiendo tener un panorama global de lo que sucede. También es considerado como la “portada” para un grupo de internautas que están buscando información precisa sobre algún tema.



Se la utiliza para referirnos a un Sitio Web que sirve de punto de partida para iniciar nuestra actividad de navegación en Internet, al cual visitamos con frecuencia y al que generalmente designamos como página de inicio⁷ en nuestro navegador.

El término Portal se refiere a un sitio que es punto de partida para la navegación en Internet, no nuestro sitio destino. Aún para los Portales especializados, existen requisitos que cumplir para recibir la denominación de Portal, lo cual no se limita simplemente a contar con un Sitio Web robusto. (Ing. Jorge Mendoza, Diciembre 2000).

⁷ Google.com por ejemplo.

Un Portal tiene como objetivo conseguir que los usuarios, cuando accedan a Internet lo hagan siempre a través de una WEB determinada. Para conseguir fidelizar a dichos usuarios se deberá dotar el Portal (WEB) de dos aspectos muy importantes, que son servicios (Correo Electrónico, Espacio para páginas Web, Chat, Comunidades Virtuales, Motor de Búsqueda o Índice) y contenidos (Información completa sobre el tema, Noticias de todo tipo y novedades).

Pueden existir diferentes tipos de portales en función de sus usuarios, éstos son los Portales Horizontales y los Verticales.

Portal Horizontal

Su objetivo son los usuarios en general. Suelen ofrecer motores de búsqueda, noticias, e-mail y otras posibilidades de comunicación. Ganan dinero mediante los anuncios. Los contenidos son absolutamente críticos, y se está evolucionando hacia la propia personalización del Portal.

Portal Vertical

Son portales especializados en determinados temas, que buscan públicos objetivos muy determinados. Se pueden a su vez clasificar en función de su objetivo teniendo los siguientes: Portal Intranet (Comunicación corporativa para los empleados), Portal Extranet (Comunicación corporativa para los proveedores / partners) y Portal Vertical (Comunicación corporativa con clientes).

(<http://www.desarrollandoweb.com>)

1.6.2 Marco Espacial

El presente tema tiene por desarrollarse en cualquier ámbito Web, es decir el Administrador de los Servicios Web tendrá las políticas disponibles para su autogestión.

1.6.3 Marco Temporal

El tiempo definido para este proyecto se llevara a cabo en dos meses a partir del 27/08/2011 con sus debidas presentaciones requeridas.

1.7 Metodología y Cronograma

Para la metodología se tomaría en cuenta lo siguiente:

a) Método

Cuantitativo – Cualitativo

b) Técnica

- **Encuestas:**

Este método será orientado a encuestas vía web a través de **Blogs**, el cual se publicara de manera pública, para que los webmasters que lo visiten pongan su opinión y las falencias que creen que pueda contar su sistema web, además contestaran preguntas como: Tipo de Redes que tienen, Sistema Operativo del Servidor de Alojamiento, Herramientas de Seguridad utilizada, etc. Esto permitirá contar con estadísticas de las seguridades aplicadas en los sitios web y así poder establecer las políticas que se pretenden realizar.

c) Instrumento

Formularios

Guías

1.8 Plan Analítico

- 1 **Capítulo I: Marco Teórico**
 - 1.1 Antecedentes
 - 1.2 Problema
 - 1.3 Justificación
 - 1.4 Objetivos
 - 1.4.1 Objetivo General
 - 1.4.2 Objetivos Específicos
 - 1.5 Justificación
 - 1.6 Metodología
 - 1.7 Resultados Esperados
 - 1.8 Resumen Capítulo I

- 2 **Capítulo II: Herramientas de Estudio**
 - 2.1 Seguridad Informática
 - 2.1.1 Internet
 - 2.1.2 Uso de los Sitios Web
 - 2.1.3 Ventajas y Desventajas
 - 2.2 Ataques Web
 - 2.2.1 Introducción
 - 2.2.2 Servicios web vulnerables
 - 2.2.3 Administración actual de los Webmasters y portales Web
 - 2.3 DDoS
 - 2.3.1 Definición

- 2.3.2 Características
- 2.3.3 Clasificación
- 2.3.4 Métodos de Ataque
- 2.3.5 Posibles inmunizaciones frente a ataques.
- 2.4 Resumen Capítulo II

- 3 **Capítulo III: Diagnóstico**
 - 3.1 Análisis de la Problemática
 - 3.2 Metodología Investigativa
 - 3.2.1 Método
 - 3.2.1.2 Cualitativo - Cuantitativo
 - 3.2.2 Técnica
 - 3.2.2.1 Blogs
 - 3.2.2.2 Encuestas Electrónicas
 - 3.3 Sector involucrado
 - 3.4 Creación del Blog
 - 3.5 Formato de la Encuesta
 - 3.6 Resumen Capítulo III

- 4 **Capítulo IV: Hallazgos**
 - 4.1 Estadísticas del Blog
 - 4.2 Resultados de las Estadísticas
 - 4.3 Resumen Capítulo IV

- Capítulo V: Conclusiones**

5

5.1 Creación de Políticas de Seguridad frente a DDoS.

5.2 Elaboración de planes posibles frente a amenazas

Capítulo VI: Referencias

1.9 Bibliografía

- <http://www.segu-info.com.ar/ataques/ataques.htm>
- https://www.owasp.org/images/2/2b/Conferencia_OWASP.pdf
- <http://www.tusistema.com/articulo.aspx?art=5>
- <http://internetng.dit.upm.es/ponencias-jing/2004/seguridad-en-web.pdf>
- http://foro.elhacker.net/seguridad/ataque_dos_muy_serio-t330080.0.html
- <http://foro.auditoriaswireless.es/index.php?topic=674.0>
- <http://www.elhacker.net/Textos1.html>
- <http://studies.ac.upc.edu/FIB/CASO/seminaris/2q0304/M8.pdf>
- <http://panoramix.fi.upm.es/~flimon/ddos.pdf>
- <http://www.cert.org/advisories/>
- Mario G. Piatini & Emilio del Peso. (2001). Auditoría Informática – Un enfoque práctico
2da Edición Ampliada y Revisada. Madrid: Ra-Ma Editorial
- <http://www.nuevoorden.es/2011/ataque-ddos-tumba-una-web-de-la/?adf8c1c0>
- http://www.segu-info.com.ar/ataques/img/ataques_detalle.png
- <http://www.nuevoorden.es/2011/ataque-ddos-tumba-una-web-de-la/?adf8c1c0>
- <http://www.maestrosdelweb.com/editorial/ddos/>
- <http://www.tusistema.com/articulo.aspx?art=5>
- <http://www.masadelante.com/faqs/servidor>

- [http://es.wikipedia.org/wiki/Ataque de denegaci%C3%B3n de servicio](http://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio)
- <http://foro.auditoriaswireless.es/index.php?topic=674.0>
- <http://www.informaticamilenium.com.mx/paginas/mn/articulo25.htm>
- <http://www.desarrollandoweb.com/internet/tipos-de-portales.php>

CAPITULO II

2. INTRODUCCION

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico donde nos encontremos. En ese sentido, ya no sorprende la transferencia de información en tiempo real o instantáneo y debido a que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizar el comercio en forma electrónica, con objeto de ser más eficientes. No obstante, al unirse en forma pública se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

El escenario electrónico actual en el cual las organizaciones enlazan sus redes internas a la Internet, crece a razón de más de un 10% mensual. Al unir una red a la Internet se tiene acceso también a las redes de otras organizaciones. Por ello, es fundamental tener protegida adecuadamente la red.

Es importante tener una política de seguridad bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la compañía, ya que la tienen en sus redes todos los recursos y merecen protegerse.

La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; este debe protegerse del acceso indebido del mismo modo

que otros bienes valiosos como la propiedad corporativa y los edificios de las oficinas.

Uno de los ataques más comunes es DDoS (Ataque de Denegación de Servicio Distribuido) el cual consiste en distribuir a varias máquinas por la Internet una Ip (víctima) a la que será atacada con el fin de hacerla colapsar y así poder subir webs malignas o generar pérdidas a la organización por transacciones no realizadas por caída de la página web

Las políticas son la clave donde las empresas marcan su frontera dentro de la Organización y establecen las disposiciones para cumplirlas.

CAPITULO III

3. MARCO DE REFERENCIA

3.1. Marco Teórico

3.1.1. Política

La política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos (<http://definicion.de>)

En informática se pretende aprovechar el potencial que ofrecen las Tecnologías de la Información con las que se cuentan actualmente.

De ellas podemos destacar o clasificar que las Políticas en cuanto a La protección de Datos Personales e Información, Redes y Telecomunicaciones son las que dentro de la informática tienen mayor importancia.

En cuanto a la Protección de Datos Personales e Información se promueve la confidencialidad de los datos personales y por ende la protección jurídica de la información producida en los



Fig. 1 Ilustración de Seguridad en Redes

sistemas de las Instituciones, por lo que se establece que todos los sistemas y bases de datos que procesen o almacenen datos personales, deberán contar con políticas de administración de claves de acceso y

medidas de seguridad lógica. (Ley de Acceso a la Información Pública para el Estado Ecuatoriano.)

Es importante que las empresas que tienen sitios web o prestan servicios en la Internet, expongan sus políticas sobre aspectos relevantes para sus usuarios, como el manejo de los datos personales, las condiciones comerciales de una venta o cualquier anuncio importante que pueda tener repercusiones de tipo legal para el sitio y sus usuarios.

Se puede deducir las siguientes políticas:

3.1.1.1. Políticas de Privacidad

Desde los datos más sensibles hasta los aparentemente insignificantes forman parte del **derecho a la privacidad e intimidad**, es decir, el que tiene toda persona a controlar la información sobre sí misma.

Si se recolecta datos personales por alguna razón o utiliza cualquier medio de recolección automática de datos, debe publicar una Política de Privacidad, que exponga claramente las prácticas de recolección y el manejo que le dará a los datos personales recolectados en el sitio.

3.1.1.2. Políticas de Uso de Correo Electrónico

Como herramienta suministrada por una empresa u organización a sus empleados, el correo electrónico se ha constituido en una de las más polémicas. Los despidos por su mal uso alrededor del mundo lo

confirman, lo mismo que las demandas por violación a la privacidad de empleados contra sus empleadores.

Por otro lado las medidas adoptadas en las políticas de seguridad de la empresa, pueden incluir unas limitaciones al envío y recepción de mensajes de correo electrónico que deben ser conocidas por los empleados para su acatamiento.

Las Políticas de Uso de Correo Electrónico se hacen necesarias en la medida en que se pretenda regular este uso, independientemente de las adoptadas por cada empresa u organización.

3.1.1.3. Política de Vínculos

Ya sea que al sitio web se lo vincule por cualquier otro o que usted no desee vínculos externos, es importante dar aviso de su preferencia a quienes desean vincular alguna página de su sitio web. Así lo están haciendo muchos mediante Políticas de vínculos o enlaces, que revelan al público cuál es la posición del sitio web en cuanto a ser destino de un vínculo externo.

3.1.1.4. Políticas Antispam

El spamming se ha convertido en una de las prácticas más rechazadas en el ciberespacio. A tal punto que muchos evitan proporcionar su dirección de correo electrónico a un sitio web, por temor a ser saturados de *spam* o correo no solicitado.

Si se respeta la privacidad de los usuarios y se ofrece algún boletín electrónico o cualquier otro tipo de correspondencia electrónica, una política antispam es recomendable para generar confianza en que ni por medio del Webmaster se enviará correo no solicitado.

3.1.2. Seguridad Informática

Es el estado de bienestar de la información y las infraestructuras, en las cuales la posibilidad que puedan realizarse con éxito y sin detectarse, el robo, alteración y parada del flujo de información, se mantienen en niveles bajos o tolerables. (Arronategui, S/A)

La seguridad informática es una derivada de la informática en vista de la constante implementación que se necesita aplicar en los diversos sistemas ya sean estos web o de escritorio. Para ello se ha definido una serie de estándares, protocolos, métodos, etc. y así minimizar los riesgos suscitados en cualquier ámbito informático.

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

c) Seguridad en Redes

Mantiene bajo protección los recursos y la información con que se encuentran en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo adecuado.

d) Seguridad Global

En cuanto a este tipo de red se la puede incluir todo tipo de recursos informáticos dentro de una organización, empresa u oficina, aun cuando estos no estén interconectados como las Redes de Área Local (LAN), Redes de Áreas Metropolitanas (MAN), Redes Nacionales e Internacionales Grandes (WAN) y Computadores personales, pequeños y grandes sistemas (<http://www.arcert.gov.ar>)

De manera que seguridad Global es mantener bajo protección todos los componentes de la red global. Además debemos tener en cuenta que dentro de un sistema los Usuarios son la parte que no hay que olvidar ni menospreciar, debido a que siempre hay que tener en cuenta que la seguridad comienza y termina con las personas.

3.1.2.1. Panorámica General de la Informática

Habitualmente los usuarios finales no tienen en consideración la seguridad cuando hacen uso de un sistema, ya que, frecuentemente se ignoran los aspectos relacionados con la seguridad. De igual forma, estos aspectos a veces pueden considerarse una molestia, ya que la

seguridad suele ser lo opuesto a la comodidad y facilidad de uso en la balanza del diseño de un sistema.

Es por esto que los usuarios a veces puedan tener una imagen negativa de la seguridad, por considerarlo algo molesto y que interrumpe su capacidad de realización de un trabajo determinado. En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas (como por ejemplo, recordar contraseñas, cambiarlas periódicamente, etc.) y que pueden limitar las operaciones que puede realizar así como los **recursos a los que se le permite acceder**.

Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico.

Por ejemplo, cuando se guardan cosas en una caja fuerte en un banco real, no se piensa que cualquier persona del mundo puede llegar a ésta de una forma inmediata como si se tratara, en lugar de un banco, de una estación de autobuses. En el mundo intangible de la informática, tan cerca de un servidor están sus usuarios legítimos como los usuarios que hacen uso de la misma red de comunicaciones. Algunos serán “usuarios legítimos” pero otros serán los causantes de catástrofes informáticas.

3.1.2.2. Importancia de los mecanismos de Seguridad

Para describir lo importante que consiste la seguridad en los ambientes informáticos se detalla 3 casos relevantes, con ellos se pretende mostrar alguno de los peligros, relativos a seguridad, de estar 'interconectados'. Para cada uno de ellos existen mecanismos de seguridad que permiten llevar a cabo las operaciones de manera satisfactoria.

3.1.2.3. Intercambio de información

Cuando se intercambia información con un ordenador remoto, esa información circula por una serie de sistemas intermedios que son desconocidos por el usuario (excepto en ámbitos muy específicos). Además, no sólo no se sabe cuáles serán estos sistemas intermedios, sino que además no se dispone de ningún control sobre ellos o sobre lo que puedan hacer con nuestros datos al pasar por ellos. Quizá el propietario original es de fiar pero su sistema ha sido comprometido por un atacante que toma posesión de los datos enviados.

Por otro lado tampoco se puede estar seguro de que el sistema al que uno se está conectando es quien dice ser. Existen diversos medios técnicos para suplantar la identidad de un sistema y engañar a un tercero cuando realiza la conexión.

En definitiva, no existe una certeza absoluta de que aquellos sistemas a los que uno envíe información sean realmente los auténticos; además,

en el caso de que lo sean no se sabe si llegará la información que se les envía, o si llegará sin cambios o si, aún si llega sin modificaciones, será leída por terceras partes. Este es el caso del software gratuito pero de gran acogida como los es: Logmein, Teamviewer, Hamachi, etc.

3.1.2.4. Instalación de software dañino involuntariamente

Otra posibilidad que no se debe descartar es que se instale software en un ordenador sin conocimiento del usuario o administrador. Esto puede ocurrir de muchas formas, algunas relacionadas con operaciones que se realizan todos los días. Algunos ejemplos son:

- Introducción de virus o troyanos por la descarga y ejecución de ficheros en servidores, en principio, confiables, por parte del usuario. El efecto de distribución puede ser, incluso, involuntaria si se hace uso de sistemas de archivos compartidos. En el caso de los virus el efecto destructivo se hará patente más pronto o más tarde. La instalación de troyanos puede, sin embargo, pasar desapercibida.
- Difusión de virus por correo electrónico. Lograda gracias a la malversación por parte del virus del programa utilizado como lector de correo (que lo ejecuta automáticamente sin intervención del usuario) o porque el usuario activa el virus inadvertidamente creyendo que se trata de otra cosa. Su efecto pernicioso es,

además del destructivo habitual de un virus, la distribución a las direcciones conocidas convirtiendo su propagación en exponencial.

- Explotación de una vulnerabilidad de un servicio que se está ofreciendo a través de Internet. Como por ejemplo un servidor web. Este software dañino no sólo puede obtener o borrar información del sistema en el que se instala, también puede servir como plataforma de ataque a otros sistemas.

Es por esto que todo ordenador, máxime cuando se encuentra expuesto a recibir información del exterior, debe protegerse con las medidas de seguridad adecuadas aunque se considere que no tiene información ni servicios de gran importancia.

3.1.2.5. Protección ante accesos no autorizados

Cuando se ofrecen servicios o información en una red para sus usuarios legítimos, al mismo tiempo se abre la puerta a posibles intrusos en estos sistemas. Protegerse de esta posibilidad implica tener un especial cuidado con todo el software empleado, desde el sistema operativo hasta la última de las aplicaciones instalada, y cuidar en gran medida su configuración.

Pero tampoco debería olvidarse la posibilidad de que existan intrusos que accedan físicamente al sistema. La evolución de las

comunicaciones ha hecho que se preste una gran atención a la posibilidad de accesos remotos, pero de nada sirve evitar esta posibilidad si se permite el acceso físico al sistema a personas no autorizadas. Es por esto que, en algunos casos pueda ser necesario tomar las medidas de seguridad adecuadas sobre el propio hardware para evitar robos, o pérdidas de información por estos accesos inadecuados. En definitiva un buen sistema de seguridad debe proteger los sistemas vulnerables ante el posible acceso físico o remoto de intrusos no autorizados. Evidentemente, el nivel de seguridad establecido tendrá que ser consecuente con un análisis previo de los riesgos, considerando el impacto de dicho acceso no deseado contra las posibilidades de que este se produzca.

Algunas medidas de seguridad que se pueden implantar en estos casos van desde el cifrado de información sensible para impedir su acceso sin la clave adecuada, métodos físicos de destrucción de la información en caso de manipulación mecánica de la misma, etc.

3.1.2.6. Fallos de seguridad en la utilización del software

Se puede hacer un análisis agrupando los fallos de seguridad que se pueden dar en el software. Este análisis va a permitir enfocar, cómo distintos tipos de software ayudan a solventarlos. De una forma simple, se pueden dividir en tres bloques:

- Fallos debidos a errores desconocidos en el software, o conocidos sólo por terceras entidades hostiles. Se lo puede dirigir a la calidad del código
- Fallos debidos a errores conocidos pero no arreglados en la copia en uso del software.
 - Este fallo se refiere a la capacidad y rapidez de arreglo de los errores descubiertos en el código por parte del proveedor del mismo y a la capacidad del administrador de recibir e instalar nuevas copias de este software actualizado.
- Fallos debidos a una mala configuración del software, que introduce vulnerabilidades en el sistema
 - Este tipo de vulnerabilidades puede dirigirse, sin embargo, a una falta de documentación del software o una falta de formación adecuada de los administradores para hacer una adaptación correcta del mismo a sus necesidades.

3.1.3. Auditoria Informática

Conceptualmente la auditoria, toda y cualquiera Auditoria, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que las han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

1) Contenido	Una opinión
2) Condición	profesional
3) Justificación	Sustentada en determinados procedimientos
4) Objeto	Una determinada información obtenida en un cierto soporte
5) Finalidad	Determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad

En todo caso es una función que posteriormente se somete a una relación con las actividades ya realizadas, sobre las que hay que emitir una opinión, tomando en cuenta las entidades que rigen este tipo de normas como ISACA⁸ y COBIT⁹ (Auditoría Informática – Un enfoque práctico, Mario G. Piatini & Emilio del Peso /2001)

⁸ Information System Audit and Control Association.

⁹ Control Objectives for Information and Related Technology

Además cuenta con los mecanismos para poder determinar qué es lo que sucede en el sistema, que es lo que hace cada uno de los usuarios, los tiempos y fechas de dichas acciones.

Estos dos últimos puntos son de extrema importancia, ya que en base a esto se diferencia entre “espíar” y “monitorear”, a sus usuarios, demostrando así la ética implantada por cada uno de sus administradores.

Finalmente todos estos aspectos y servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importante con las que señalan dichos servicios. De esta manera es posible aplicar los derechos efectivos entre usuarios y administradores.

3.1.4. Webmaster

Debe tener habilidades de análisis de problemas, capacidad para razonamiento abstracto, proyección a futuro y resolución de problemas y muy útil tener cierta habilidad para el análisis de procesos.

Dependiendo del rol que juegue el Webmaster en una empresa, se especializará en un área en particular o deberá ir adquiriendo pericia en algunas tareas tales como Administración y Mantenimientos de Sistemas Web. (www.webtaller.com)

El webmaster es el sujeto principal en esta relación debido q que es la persona indicada en administrar los sitios web y estar pendiente a la notificación de algún ataque, además es el encargado y custodio de la información que está a su cargo, y a su vez hacer cumplir las normas y políticas generadas por la empresa.

3.1.5. DDOS

Se los define como Ataques Distribuidos de Denegación de Servicios, este impide que los usuarios de un determinado sistema no puedan acceder a él, y por consiguiente a los servicios que proporciona. En las circunstancias actuales de la globalización, el daño económico y de imagen que sufre una empresa por un ataque de este tipo probablemente sea mucho mayor que el derivado de una simple intrusión; anteriormente con ataques DoS se enviaba ataques masivos a una maquina con el fin de imposibilitar la misma, pero en la actualidad con mecanismos más sofisticados y empleando las debilidades de los protocolos TCP/IP se puede generar grandes cantidades de paquetes sobre un sistema concreto lo que genera que el servicio quede inoperante.

Los ataques DoS se pueden ejecutar de manera coordinada a partir de varias fuentes al mismo tiempo (Distributed DoS, DDoS). Un ataque de denegación de la lógica se basa en una explotación inteligente de vulnerabilidades en el blanco. Por ejemplo, una dirección IP hábilmente construidas fragmentada datagrama se puede bloquear un sistema debido a

un fallo grave en el software del sistema operativo (SO). Otro ejemplo de un ataque de la lógica es explotar falta de autenticación de requisitos mediante la inyección de información de enrutamiento falsa para evitar que el tráfico llegue a la víctima de la red

Entre los ataques DDoS más utilizados tenemos los siguientes:

3.1.5.1. Trinoo

- La forma en la que este tipo de ataque toma forma o se basa es en cuanto a que un sistema vulnerado deposita un repositorio de herramientas compiladas tales como: rastreo, ataque, Sniffers¹⁰, root kits. Este sistema poseerá un gran número de usuarios, y por consiguiente, una gran potencia de proceso y amplio ancho de banda en sus comunicaciones

3.1.5.2. Tribe Flood Network

- Compuesto por un conjunto de programas clientes y demonios que implementan una herramienta de denegación de servicio distribuida, capaz de generar ataques por generación masiva de paquetes ICMP, SYN o UDP, así como ataques del tipo Smurfing¹¹.

3.1.5.3. Tribe Flood Network 2000 (TFN₂K)

¹⁰Sniffer: Herramienta software que permite capturar y analizar todo el tráfico que circula por un segmento de red.

¹¹ Smurfing: Amplificación de peticiones broadcast.

- Es una evolución del anteriormente comentado TFN. De esta forma, se denomina Maestro al sistema informático en el que corre el Cliente, y Agente al sistema informático donde se ejecuta el Demonio. El TFN2K permite a los Maestros explotar los recursos de un determinado número de Agentes con el fin de coordinar un ataque a una o más víctimas. El Maestro configura a los Agentes para atacar a una determinada lista de víctimas. Los Agentes atacan a las víctimas por inundación de paquetes.

3.1.5.4. Stacheldraht

- Dispone de un mecanismo similar a un Telnet (Stacheldraht Term) para la comunicación del cliente con el conductor que incluye cifrado mediante el uso de clave simétrica. Una vez establecida la comunicación entre el cliente y el conductor, se solicita un password que está cifrado mediante criptografía. A partir de ese momento toda la comunicación se realiza de forma cifrada mediante el algoritmo Blowfish.

3.1.5.5. Sahft

- En este tipo de ataque la comunicación entre los distintos niveles se lo utiliza de la siguiente forma:
 - Cliente a Conductor: 20432/TCP
 - Conductor a Agente: 18753/UDP
 - Agente a Conductor: 20433/UDP

Una de las novedades que presenta esta herramienta es el uso de *tickets* para garantizar el control sobre los agentes. Tanto el *password* como el *ticket* deben ser correctos para que un agente acepte las peticiones que le puedan llegar.

3.1.5.6. Mstream

- Un ataque de este tipo presenta los siguientes síntomas: El sistema objeto del ataque baja su rendimiento debido al consumo de CPU por el tráfico de red que debe atender.

Se observa un consumo elevado de ancho de banda en la red como consecuencia del propio ataque. El sistema atacado ocupa aún más ancho de banda al intentar contestar con ramas TCP RST a los falsos remitentes de las tramas TCP ACK. Los routers contestarán a la víctima con tramas ICMP indicando que el destinatario de la trama TCP RST no existe, lo que también consume aún más ancho de banda.

Aunque cuando este tipo de ataque proviene de un único sistema no suele producir grandes efectos en el sistema atacado, pero cambia el panorama cuando son varios los sistemas atacados y muchos los atacantes, pues sólo tiene un enlace como la saturación de la red, si no la caída del sistema atacado, y por consiguiente la denegación de servicio, que es el objetivo final. (Martínez, 2000)

3.1.6. Portales Web

Un portal es básicamente la “portada” de un grupo de Web Sites individuales que comparten la temática de su contenido, resumiendo la más relevante información de cada uno de éstos y permitiendo tener un panorama global de lo que sucede. También es considerado como la “portada” para un grupo de internautas que están buscando información precisa sobre algún tema.

Se la utiliza para referirnos a un Sitio Web que sirve de punto de partida para iniciar nuestra actividad de navegación en Internet, al cual visitamos con frecuencia y al que generalmente designamos como página de inicio en nuestro navegador.



Fig. 2 Portales Web

El término Portal se refiere a un sitio que es punto de partida para la navegación en Internet, no nuestro sitio destino. Aún para los Portales especializados, existen requisitos que cumplir para recibir la denominación de Portal, lo cual no se limita simplemente a contar con un Sitio Web robusto. (Mendoza, Diciembre 2000)

Un Portal tiene como objetivo conseguir que los usuarios, cuando accedan a Internet lo hagan siempre a través de una WEB determinada. Para conseguir fidelizar a dichos usuarios se deberá dotar el Portal (WEB) de dos aspectos muy importantes, que son servicios (Correo Electrónico, Espacio para páginas Web, Chat, Comunidades Virtuales, Motor de Búsqueda o Índice) y contenidos (Información completa sobre el tema, Noticias de todo tipo y novedades).

Pueden existir diferentes tipos de portales en función de sus usuarios, éstos son los Portales Horizontales y los Verticales.

3.1.6.1. Portal Horizontal

Su objetivo son los usuarios en general. Suelen ofrecer motores de búsqueda, noticias, e-mail y otras posibilidades de comunicación. Ganan dinero mediante los anuncios. Los contenidos son absolutamente críticos, y se está evolucionando hacia la propia personalización del Portal.

3.1.6.2. Portal Vertical

Son portales especializados en determinados temas, que buscan públicos objetivos muy determinados. Se pueden a su vez clasificar en función de su objetivo teniendo los siguientes: Portal Intranet

(Comunicación corporativa para los empleados), Portal Extranet (Comunicación corporativa para los proveedores / partners) y Portal Vertical (Comunicación corporativa con clientes).

(<http://www.desarrollandoweb.com>)

3.2. Marco Temporo/Espacial

El presente tema va dirigido a todos los Webmaster que desea implementar las políticas desarrolladas frente a ataques DdoS en la Web, es decir el Administrador de los Servicios Web tendrá las normativas disponibles para su autogestión. El tiempo de vigencia de las políticas implementadas tendrán una duración entre la cual estas dejen de ser provechosas y pasen a ser obsoletas. Este proyecto se llevara al cabo de dos meses a partir del 27/08/2011 con sus debidas presentaciones requeridas

3.3. Marco Legal

Para la realización de la tesis, me he basado en la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 2002-67) de la República del Ecuador, la cual en los siguientes artículos tipifica las sanciones respectivas en caso de violentar información no autorizada.

Título V

DE LAS INFRACCIONES INFORMÁTICAS

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos enumerados:

- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."

CAPITULO IV

4. METODOLOGIA

4.1. Métodos

Se utiliza la metodología de la Investigación basada en encuestas, ya que aplicando la tecnología se la realizó electrónicamente a través de un Blog que está expuesto en la web y enviado a varios Webmasters que puedan proporcionar información acerca de sus experiencias en cuanto si han sido víctimas de algún tipo de ataque web.

Los mails de los webmaster que contestaron el blog son los siguientes:

btipanluisa@interactive.com.ec

mcamacho@telconet.net

rbarbecho@punto.net.ec

webmaster@austronet.net

patricio.abril@etapanet.net

mrubio@interactive.net.ec

info@intercom.com

sistemas@servicable.com

r.flore@tvcable.com

El link en el cual se creó el Blog es el siguiente:

<http://seguridadwebecuador.blogspot.com/>

4.2. Técnicas

Para realizar las distintas preguntas que se encuentran en el blog se realizara un formulario en el cual estarán descritas una serie de preguntas en bases a la Guía OWASP dirigida a Administradores web, se recopilará temas de gran relevancia en cuanto a seguridad y medidas de prevención, esto nos ayudara conocer en qué estado de seguridad se encuentran los sitios web en nuestro medio y si cuentan con un plan de contingencia de rápida acción en el caso de amenazas graves.

4.3. Instrumentos

La técnica en base a la investigación realizada son las siguientes preguntas:

¿Posee usted un sistema de Gestión en N Capas con acceso web, o portales de tipos transaccionales a su custodia?

- Si ()
- No ()

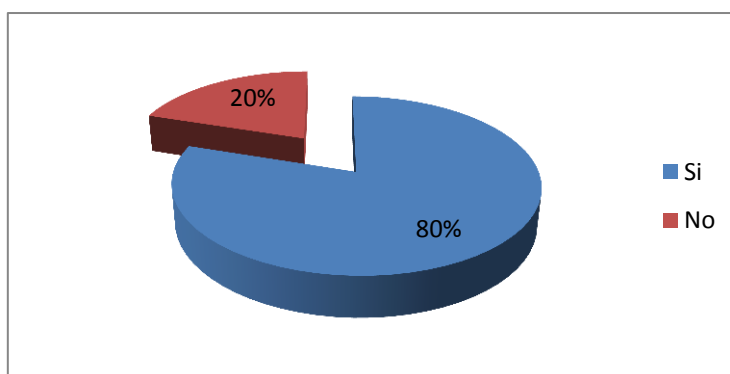


Fig. 3 Pregunta 1

Estos resultados nos indica que las transacciones o la mayoría de trámites se lo realiza en ambientes web (internet), esta estadística nos indica cuan en auge se encuentra la implementación de la tecnología en las empresas.

¿Recibe simultáneamente entradas a sus sistemas ya sea login de usuarios, transacciones, mantenimiento, etc.?

- Si ()
- No ()
- En proceso de Implementación ()

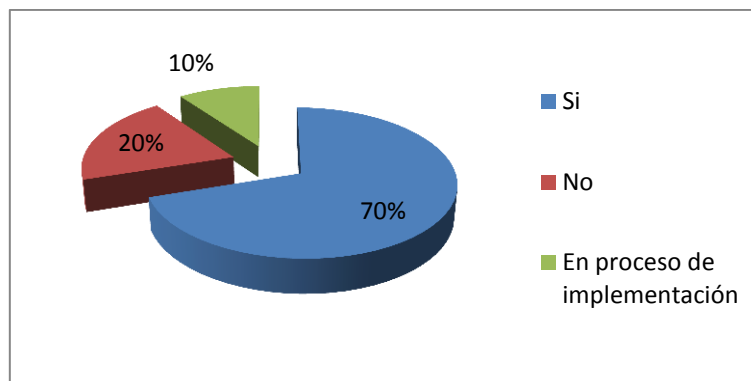


Fig. 4 Pregunta 2

Cada vez las empresas implementan sistemas web a sus aplicaciones como mejora en sus ambientes tecnológicos, y si aún no lo tienen piensan en desarrollarlos.

¿El área geográfica de mayor ingreso a su portal es en el lugar donde se encuentran sus servidores?

- Si ()

- El ingreso se lo hace en varias partes del mundo ()

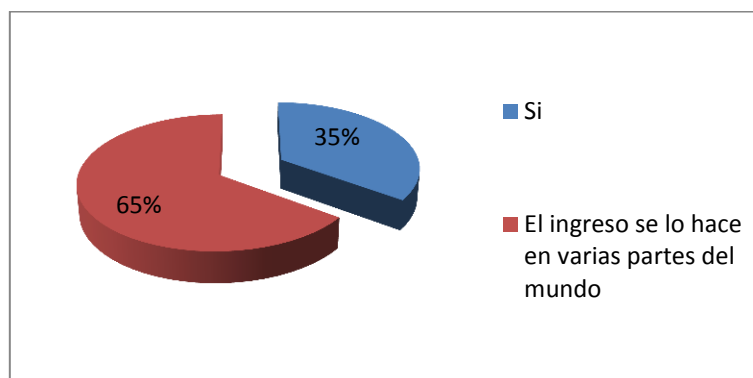


Fig. 5 Pregunta 3

Ese es el propósito de las aplicaciones web, el ingreso desde cualquier lugar, lo cual nos indica que tan expuesta se encuentra nuestra información, demostrando superioridad de las aplicaciones web frente a las aplicaciones Cliente/ Servidor.

¿Su empresa cuenta con Políticas de Seguridad Web implementadas y utilizadas?

- Si, implementadas y utilizadas ()
- Implementadas pero no utilizadas ()
- No cuento con políticas. ()

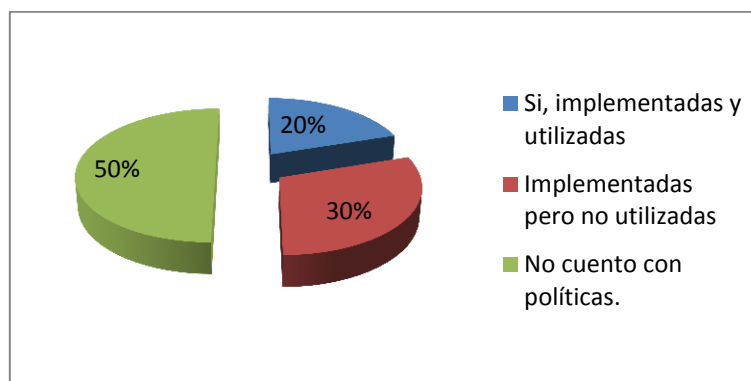


Fig. 6 Pregunta 4

La mayor parte de los webmasters o las áreas de IT, no cuentan con políticas de seguridad, demostrando así una gran falencia en la organización de la seguridad, en cuanto a los siguientes resultados sobre las organizaciones que cuentan con políticas pero no las implementan se da en varias empresas dentro de nuestra región y finalmente solamente un grupo minoritario cuenta con una organización efectiva en cuanto a la seguridad.

¿Ha sufrido ataques web, que tipo de ataque lo consideró?

- DdoS ()
- Phishing ()
- SQL Injection ()
- Otro tipo de ataque ()
- No he sufrido ataques Web. ()

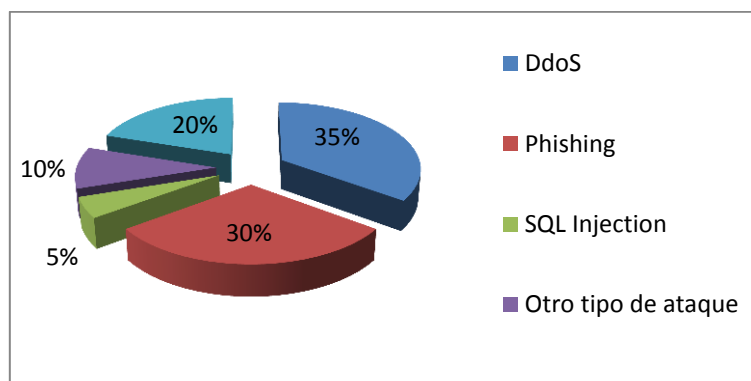


Fig. 7 Pregunta 5

Las estadísticas demuestran que la mayor afluencia de ataques a los diversos servicios web se los da por parte de ataques DdoS, seguido de uno de los más grandes ataques como es el phishing, y tan solo un grupo pequeño de encuestados no conoce que tipo de ataque sufrió o quizá no lo experimentó aun.

¿Cuenta con un plan de contingencia en caso de sufrir ataques web?

- Si ()
- No ()

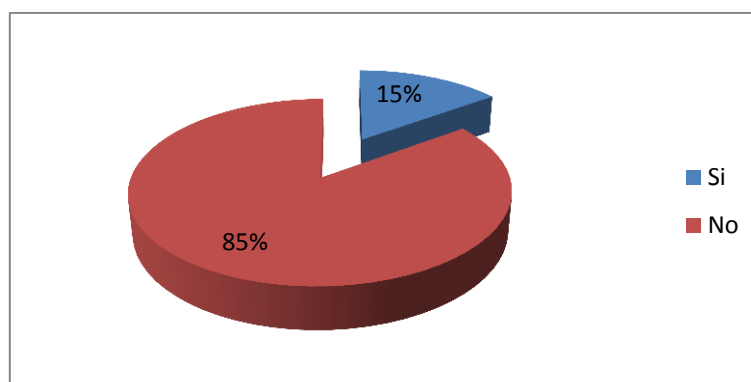


Fig. 8 Pregunta 6

Las estadísticas nos indican que en caso de sufrir percances, el área de sistemas no cuenta con un plan de contingencia para implementarlo inmediatamente, estos resultados demuestran que no estamos preparados para sufrir pérdidas de información.

¿La arquitectura de su red cuenta con los equipos y software de protección (Firewall, DMZ, Routing, Proxy, Backup server) necesarios para prevenir estos tipos de ataques?

- Si, totalmente implementados ()
- No cuento con los recursos financieros necesarios ()
- Mi arquitectura requiere actualización ()

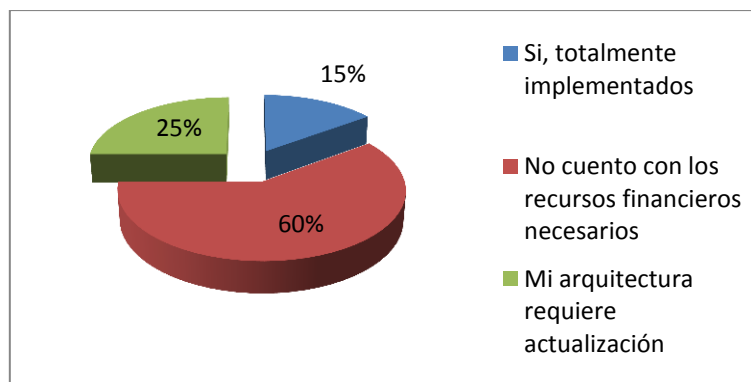


Fig. 9 Pregunta 7

Una de las razones por no tener implementadas una buena arquitectura en cuanto a equipos informáticos son los recursos económicos para el área de informática, lo que se recomienda es considerar al área IT como un área vital de la empresa, otorgando los recursos necesarios para su correcto funcionamiento.

¿Cree usted estar preparado para prevenir ataques DDoS?

- Si ()
- No, necesito capacitación ()

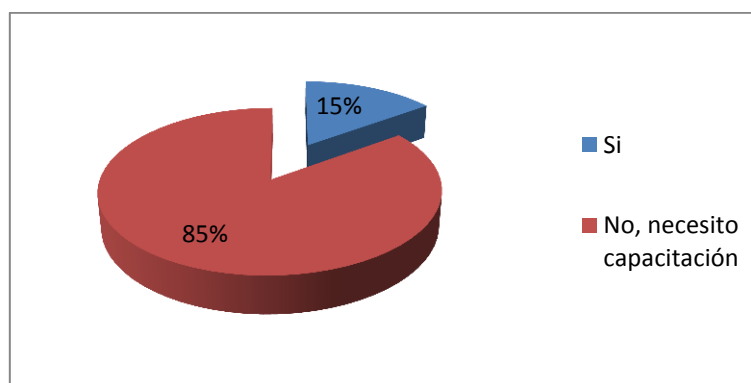


Fig. 10 Pregunta 8

Podemos verificar que la mayoría de nuestros encuestados requieren capacitación previa para la implementación de una buena política de seguridad en la empresa que se encuentra a cargo.

1.4 Conclusión

Esta es la lista de las preguntas expuestas en el blog, con sus resultados tabulados dándonos a conocer que la actual situación de nuestros sitios web no cuentan con políticas de seguridad implementadas, en el caso de tenerla no dan el uso adecuado de las mismas y en su defecto no cuentan con planes de contingencia en el caso de amenazas, demostrando así que las organizaciones no dan la importancia debida al área IT como se

debería, ya que es la más importante por custodiar la información que fluye dentro de la empresa.

Esta estadística representa la realidad intelectual en cuanto a capacitación tecnológica en base a Webmasters de ISP's tenemos en la actualidad

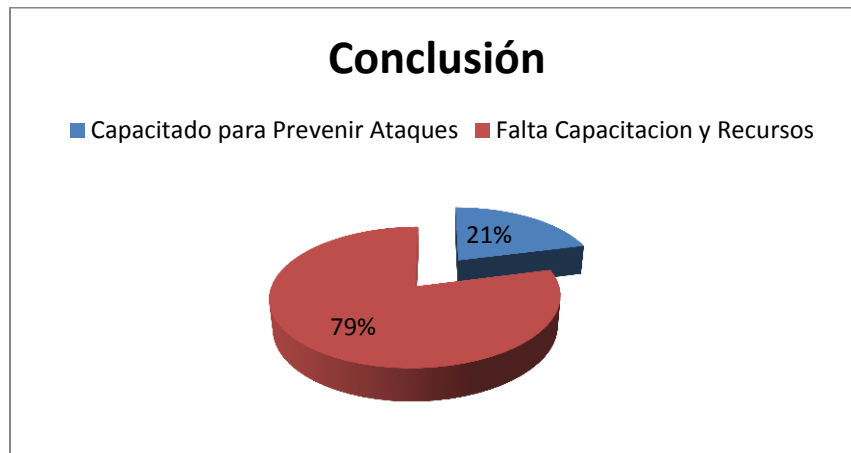


Fig. 11 Conclusión

CAPITULO V

5. IMPORTANCIA DE LA INFORMACION

5.1. Datos e información.

Necesitamos definir que son los **Datos**: hechos y cifras que tienen relativamente poco significado para el usuario ejm.: cualquier formulario que llenamos, una historia clínica, valores de pago, etc. y diferenciarlos de lo que es la **Información**: Datos procesados o datos con un significado para el usuario, ejm.: los grupos de edad con un diagnóstico determinado, número de usuarios con privilegios administrables, valores a pagar en una transacción, etc. Es decir son los datos que han sido sometidos a un proceso, que han sido clasificados, ordenados sintetizados y/o asociados, los cuales nos permiten concluir algo, estos se transforman en información.

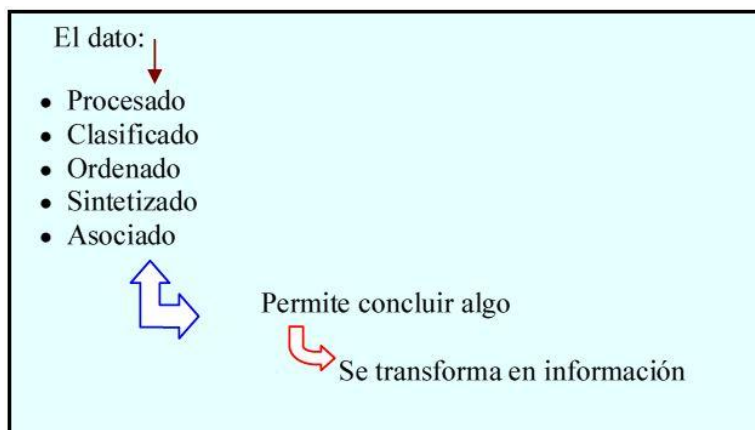


Fig. 12 Datos e Información

5.2. Sistemas de Información

Un sistema de información es un conjunto de procedimientos ordenados que, al ser ejecutados, proporcionan información para apoyar la toma de decisiones y el control de la Institución. La información se define como una entidad tangible o intangible que permite reducir la incertidumbre acerca de algún estado o suceso. Los sistemas de información administrativa están volviéndose indispensables, a gran velocidad, para la planificación, la toma de decisiones y el control. La velocidad y exactitud con que los directivos pueden recibir información sobre lo que está funcionando bien o lo que está funcionando mal determinarán, en gran medida, la eficacia que tendrán los sistemas de control.

La información que proporcionen los SI deberá ser evaluada en cuatro sentidos:

5.2.1. Calidad de la Información:

Cuanto más exacta la información, tanto mayor su calidad y tanta mayor confianza pueden depositar los directivos en ella para tomar decisiones. Sin embargo, en general el costo de obtener información aumenta conforme la calidad deseada se eleva.

5.2.2. Oportunidad De La Información:

Para tener un control más efectivo, se deben aplicar medidas correctivas antes de que la desviación del plan o la norma sea demasiado grande. Por

tanto la información ofrecida por un sistema de información debe estar al alcance de la persona indicada, en el momento oportuno, para que se emprendan las medidas adecuadas.

5.2.3. Cantidad de Información:

Los directivos no pueden tomar decisiones exactas y oportunas si no cuentan con suficiente información. No obstante, con frecuencia, los directivos reciben demasiada información irrelevante o inútil. Si reciben más información de la que pueden usar en forma productiva, quizá pasen por alto la información sobre problemas graves.

5.2.4. Relevancia de la Información:

Asimismo, la información que reciben los directivos debe ser relevante para sus funciones y labores. El director de personal seguramente no necesita saber cuáles son los niveles de inventarios, y el directivo a cargo de reordenar los inventarios no necesita saber nada de la condición del personal de otros departamentos.

5.3. La información como el activo más importante dentro de la empresa

El nuevo escenario socio-económico ha conllevado infinitos cambios, pero quizás el mayor se sitúa en la información. El crecimiento de la información ha sido exponencial y así seguirá siendo en el futuro. Esto indica que obligatoriamente se debe disponer no de unos eficaces sistemas de

almacenamiento sino de establecer una estrategia concreta que marque pautas perfectamente definidas sobre la gestión de esa información.

No se trata de almacenar, sino de gestionar. Es lo más importante. No hay que olvidar, que son muchos los valores que definen a una compañía, pero por encima de todos está la información.

Esto es algo asumido por todos ya que es el valor máspreciado de cualquier empresa. De su correcta gestión depende la viabilidad de la propia empresa u organización. Ciertoes que la complejidad tecnológica es importante, pero también lo es el que la mayoría de empresas comprometidas con este segmento de almacenamiento son capaces de gestionar esa complejidad haciéndola prácticamente invisible para el usuario, y además, permitir la generación de eficiencias en la empresa. Es lo que ya se define como almacenamiento inteligente, un concepto que articula la criticidad de los datos en base a una jerarquía concreta y específica según las necesidades de las empresas.

5.3.1. ¿Qué valor tiene proteger la información?

El momento de tener a custodia personal información de una organización se debe realizar las siguientes preguntas:

- ¿Qué pasaría si algún día perdiera la información de su empresa?
- ¿Si no pudiera acceder a ella?
- ¿Si personal no autorizado pudiera modificarla?

- ¿Si la competencia tuviera acceso a su información?
- El 94% de las empresas cerrarían a los 2 años de una pérdida severa de la información en sus sistemas.
- El 70% no sobreviviría a más de 4 días sin sus datos. (university of texas)

5.4.El valor de la información en las empresas

Hoy en día uno de los principales activos de cualquier empresa, es la información contenida en sus sistemas informáticos. Dicha información es susceptible de ser perdida, deteriorada, revelada o incluso de robada (www.legal-protect.com)

El siglo XX ha sido el escenario de los mayores cambios tecnológicos de la historia y, desgraciadamente. El creciente sector de las tecnologías de la información y la comunicación no sólo ha sido un resultado más de ello, sino quizás su principal protagonista, pues ha transformado la manera de relacionarse las personas y de funcionamiento de las organizaciones, posibilitando que lo que ayer era una estrategia para ellas, hoy en día haya pasado a formar parte de su estructura o infraestructura.

Uno de los muchos ejemplos de ello, es su uso en el sector de la banca, al acercar el banco a los clientes a través de las TIC (Tecnologías de la Información y la Comunicación).

La banca virtual empezó siendo una estrategia más no exenta de incertidumbre; hoy en día sin embargo, no concebimos ningún banco que no

haya asumido dentro de su infraestructura, cuando abre una oficina nueva, la instalación de un cajero, o bien simplemente facilitar el acceso al mismo a través de Internet.

Las preguntas principales serian si la información para las organizaciones:

- ¿Es una estrategia o un activo sin el que no se concibe una organización?
- ¿Cuánto nos importa su seguridad?

Afortunadamente, empresas, instituciones y administración hace tiempo que aplican seguridad informática; sin embargo algo relativamente nuevo, es lo que afecta a la seguridad la información.

5.5. SGSI

Se puede definir un SGSI (Sistema de Gestión de Seguridad de la Información) como una herramienta de gestión que nos va a permitir:

- Conocer
- Gestionar
- Minimizar

Los riesgos que atente contra la seguridad de la información en nuestra empresa.

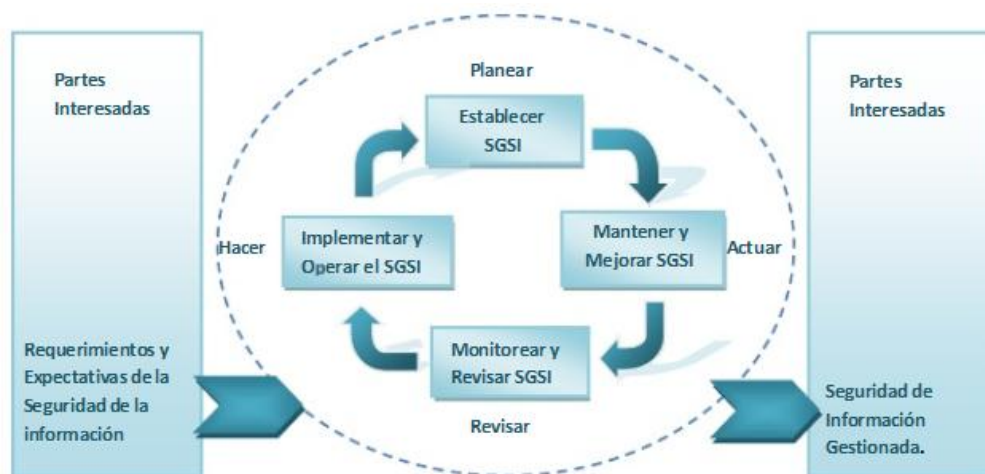


Fig. 13 Funcionamiento de un SGSI

Para comprender estos sistemas es necesario diferenciar entre seguridad de la información y seguridad informática.

Seguridad Informática: se refiere a la protección de las infraestructuras de las tecnologías de la información que soportan nuestro negocio

Seguridad de la información: se refiere a la protección de los activos de la información fundamentales para el éxito de cualquier organización, entre estos pueden estar los correos electrónicos, páginas web, imágenes, bases de datos, etc.

Al tener identificadas las fuentes de información tenemos que tener en cuenta considerar el ciclo de vida de la información, ya que lo que hoy puede ser crítico para la empresa puede dejar de tener importancia con el tiempo.

5.5.1. ¿Cuál es la diferencia entre Seguridad de la Información e Informática?

La **Seguridad Informática** es una característica concreta de cualquier sistema informático que nos indica que éste está libre de peligro, daño o riesgo. Podríamos concluir entonces diciendo que la Seguridad Informática consiste la implantación un conjunto de medidas técnicas destinadas a preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

Para definir la **Seguridad de la Información** es necesario fijarse en la totalidad de información que se maneja en una organización. En la actualidad las empresas se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes, que pueden dañar de forma importante sus sistemas de información y sus activos tanto documentales como informatizados de información y pueden poner en peligro la continuidad del negocio.

De todo ello se deduce que una correcta política de Seguridad de la Información es aquel conjunto de medidas técnicas, organizativas y legales, que permiten a la empresa asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Se puede decir que los documentos ya sean digitales o no, en las organizaciones, tiene más que ver con la seguridad de la información que con el conjunto de medidas técnicas.

Parece lógico pensar que las organizaciones coordinan esfuerzos técnicos, organizativos y legales, en el ejercicio de su actividad, si bien no suele ser tan común que esa coordinación se dé desde el punto de vista de la seguridad, quizás por falta de apoyo y concienciación de la dirección, sin la cual no se podrá implementar con éxito un sistema gestión de seguridad de la información (SGSI).

5.5.2. Objetivos de la implementación de un SGSI

La mejor seguridad continuamente está limitada por los recursos disponibles, lo que supone que muy pocas organizaciones puedan acceder a ella; sería un objetivo deseable, pero de difícil o de imposible alcance. La consistencia y coherencia de la seguridad debe ser nuestro objetivo plausible, definiendo previamente cómo tratar el riesgo: evitándolo, transfiriéndolo, reduciéndolo o asumiéndolo.

5.6. Certificación de Seguridad

Se puede regir a los sistemas de certificación tales como la ISO/IEC 27001 o ISO 17799, estas metodologías se basan en varios controles, en los que precisamente reside el valor de la misma, en el establecimiento de un marco de actuación en la aplicación de la seguridad.

5.6.1. Importancia de la Certificación

Para conseguir alcanzar la excelencia en la Seguridad de la Información, estableciendo, como su propio contenido indica, debemos también hacer de

la certificación, un elemento riguroso de control y supervisión de la seguridad.

La información es un elemento vivo en las organizaciones, y de igual modo un SGSI sigue varias fases: planificación, implantación, testeo y la corrección del mismo, en un ciclo denominado PDCA. Todas ellas estarían presentes en cualquier ámbito que defina el SGSI, incluido el proceso de gestión documental.

5.7. ISO 27001



ISO 27001

Fig. 14 Estándar ISO

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO

(International Organization for Standardization) e IEC

(International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution,) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

5.7.1. La serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados

por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

5.7.2. Implantación de la Certificación

La implantación de la norma ISO/IEC 27001 en una organización es un proyecto que puede tener una duración entre 6 meses y un año, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido SGSI elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 2700n, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o

Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información, personas totalmente certificadas por un SGSI.

5.7.3. Beneficios de la Implementación de ISO 27001

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001.).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

5.8 Conclusiones

Son 133 controles los que esta norma maneja, la Seguridad de la Información es un proceso que se basa en personas a las cuales se debe orientarse al riesgo que puedan causar. Un buen SGSI es un sistema rentable para la organización.

Un proyecto SGSI requiere un equipo de trabajo de multiconocimiento y repartido en las diversas áreas de la empresa, además indica que con un buen manejo de la información se puede establecer características especiales para una política correcta.

CAPITULO VI

6. NORMAS DE SEGURIDAD WEB Y CREACION DE PAGINAS WEB SEGURAS

6.1. Antecedentes

Desde desbordamientos de búfer a SQL Injection (inyección de cadenas SQL), los hackers tienen muchas técnicas a su alcance para atacar a las aplicaciones web, además de nuevos métodos que surgen constantemente. Los ataques a aplicaciones Web pueden costarle a las organizaciones mucho tiempo y dinero debido a las brechas de seguridad de fácil acceso a los datos, debido a esto se ha creado estrategias y mecanismo de defensa en general para el uso de las organizaciones. Una de estas organizaciones es Interactive by Zenix en la cual aplicaremos las normativas expresadas en este documento.

6.2. Normativas para aplicaciones Web Seguras.

Para la creación de normativas para aplicaciones web Seguras podemos basarnos en la revisión del Código (Lógicamente) y Los equipos para el alojamiento, distribución y protección de la información (Físicamente).

La revisión de código debe cubrir las siguientes áreas:

- Autenticación
- Autorización
- Gestión de Cookies

- Validación de Entrada de Datos
- Gestión de Errores / Fuga de Información
- Log / Auditoría
- Cifrado de Datos
- Entorno de Código Seguro
- Gestión de Sesiones (Login/Logout)

6.2.1. Autenticación

- Asegura que todas las peticiones pasan por un formulario de autenticación, y que éste no se puede saltar (ojo con las URLs de acceso directo, que deberemos asegurar que pasan por una autenticación)
- Asegurar que todas las páginas cumplen el requisito de autenticación.
- Asegurar que siempre que se pasen credenciales de autenticación (o cualquier información sensible), sólo se aceptará la información vía HTTP POST y nunca con GET.
- Cualquier página para la que se descarte el mecanismo de autenticación debe ser revisada para asegurarse de que no tiene brechas de seguridad.
- Asegurar que no hay “puertas traseras” en el código en producción

- Asegurar que las credenciales de autenticación no van en blanco (este requisito se cumple siempre que utilicemos el protocolo HTTPS. Por eso cuando rellenemos la plantilla de creación de aplicaciones, tenemos que indicar que queremos SSL.)

6.2.2. Autorización

- Asegurar que tenemos mecanismos de autorización (control de acceso y gestión de roles).
- Asegurar que la aplicación tiene claramente definidos los tipos de usuario y sus privilegios.
- Asegurar que asignamos los mínimos privilegios necesarios.
- Asegurar que los mecanismos de autorización funcionan bien y no pueden saltarse.
- Asegurarnos de chequear la autorización en todas las peticiones (este requisito debe de ser comprobado por el programador, ya en gran parte es su tarea indicar las comprobaciones de seguridad en cada elemento de la petición).
- Asegurar que no hay “puertas traseras” en el código de producción.

6.2.3. Gestión de Cookies

- Asegurarnos de no comprometer información sensible(la cookie utilizada, solamente debería almacenar el identificador de la sesión y no almacenar información sensible).
- Asegurar que no se puedan hacer operaciones no autorizadas manipulando cookies.
- Asegurarnos de usar cifrado (este requisito se cumple siempre que utilicemos el protocolo HTTPS, se debería considerar utilizar algoritmos públicos fuertes como AES, MD5 o SHA-1).
- Determinar si todas las transiciones de estados en el código de la aplicación, verifican el uso seguro de cookies.
- Asegurarnos de validar los datos de la sesión.
- Asegurarnos que las cookies contienen la mínima información privada posible.
- Asegurarnos de cifrar una cookie completa si contiene información sensible.
- Definir todas las cookies que usa la aplicación, sus nombres y para qué son necesarias (Estandarización).

6.2.4. Validación de Entrada de Datos

- Asegurarnos de tener mecanismos de validación de datos(Captcha).

- Asegurarnos de validar todas las entradas que pueden ser modificadas por un usuario malicioso: cabeceras HTTP, Input fields, hidden fields, drop down lists, etc.
- Asegurarnos de comprobar las longitudes de todas las entradas.
- Asegurarnos de validar todos los campos, cookies, http headers/bodies y form fields.
- Asegurarnos de formatear los datos convenientemente y que sólo contienen caracteres conocidos como buenos.
- Asegurarnos de validar los datos en el servidor.
- Asegurar que no hay “puertas traseras” en el modelo de validación.
- *REGLA DE ORO: Cualquier entrada externa, sea cual sea, será examinada y validada.*

6.2.5. Gestión de Errores / Fuga de Información

- Asegurar que todas las llamadas a métodos/funciones que devuelven un valor tienen su control de errores y además se comprueba el valor devuelto (Este requisito depende del programador).
- Asegurarnos de gestionar adecuadamente las excepciones y los errores.
- Asegurar que al usuario no le devolvemos errores del sistema.

- Asegurarnos de liberar los recursos en caso de error.

6.2.6. Log / Auditoría

- Asegurar que no registramos información sensible en el log en caso de error.
- Asegurarnos de definir y controlar la longitud máxima de una entrada de log.
- Asegurar que no registramos datos sensibles en el log: cookies, método HTTP “GET”, credenciales de autenticación.
- Determinar si la aplicación auditará las operaciones lanzadas desde el cliente, sobre todo la manipulación de datos: Create, Update, Delete (operaciones CRUD).
- Asegurarnos de registrar en el log las operaciones de autenticación (fallidas o exitosas).
- Asegurarnos de registrar en el log los errores de la aplicación.
- Determinar si al hacer debug estamos registrando en el log datos sensibles.

6.2.7. Cifrado de Datos

- Asegurar que no transmitimos datos sensibles en blanco , interna o externamente.

- Asegurar que la aplicación implementa buenos y conocidos métodos criptográficos.

6.2.8. Entorno de Código Seguro

- Examinar en la estructura de ficheros si hay algún componente que no debe estar directamente accesible para los usuarios.
- Comprobar la gestión de memoria (reservar/liberar).
- Comprobar si la aplicación usa SQL dinámico y determinar si es vulnerable a inyecciones de código.
- Comprobar si la aplicación tiene funciones “main()” ejecutables y depurar “puertas traseras”.
- Buscar código comentado (aunque sea para pruebas) que pueda contener información sensible.
- Asegurar que todas las bifurcaciones de código tengan su cláusula default (if-else, switchdefault,etc.) Es decir que todos los variables y constantes tengan su inicio y fin correctos.
- Asegurar que no hay “development environment kits” en los directorios en explotación.
- Buscar llamadas al sistema operativo así como aperturas de ficheros, y comprobar las posibilidades de error.

6.2.9. Gestión de Sesiones (Login / Logout)

- Comprobar cómo y cuándo se crean las sesiones de usuario, ya sean autenticadas o no.
- Comprobar el ID de sesión y verificar que tiene la complejidad necesaria para “ser fuerte”.
- Comprobar cómo se almacenan las sesiones: en base de datos, en memoria, etc.
- Comprobar cómo la aplicación hace el seguimiento de las sesiones (track sessions).
- Determinar qué hace la aplicación en caso de encontrar un ID de sesión inválido (debería redirigir a una página de error, informando del error y proporcionando un enlace a la página de autenticación).
- Comprobar la invalidación de sesiones.
- Determinar cómo se gestionan las sesiones multithreaded/multi-user.
- Determinar el timeout de inactividad de la sesión HTTP.
- Determinar cómo funciona el log-out.

6.3. Conclusión

Con la creación de normas de seguridad, se refleja el buen manejo de un programador en base a los sistemas desarrollados, en el caso de Interactive el sistema generado por el webmaster encargado, funcione de manera

óptima y sin intromisiones de terceros no autorizados, reflejado en cifras que indican que el haber perdido un negocio que se dio en el mes de noviembre hubiese generado una pérdida de 100.000\$ que cuenta con la implementación de un sistema SOFLO para monitorización de taxis dentro de la ciudad. Se puede decir que la implementación de estas normas aseguro el cierre de un negocio virtual al 100%.

CAPITULO VII

7. PREPARAR AL WEBMASTER PARA POSIBLES ATAQUES WEB FUTUROS.

Dentro de este marco al webmaster se lo preparará de una manera conceptual y poniendo en práctica las diversas opciones que nos brinda la tecnología para protegernos de los ataques informáticos a través de :

- Implementación de Métodos de Seguridad Físico/Lógico.
- Crear un plan de contingencia en caso de pérdida de información.

7.1. Implementación de Métodos de Seguridad Físico/Lógico.

Para el correcto funcionamiento y explotación de los recursos que el webmaster tiene a su custodia sería factible implementar varios métodos de protección tanto físicamente como lógicamente.

La implementación de un Firewall, DMZ, Proxy y una tabla de ruteo sería esencial para la protección de la información y los recursos informáticos de la empresa.

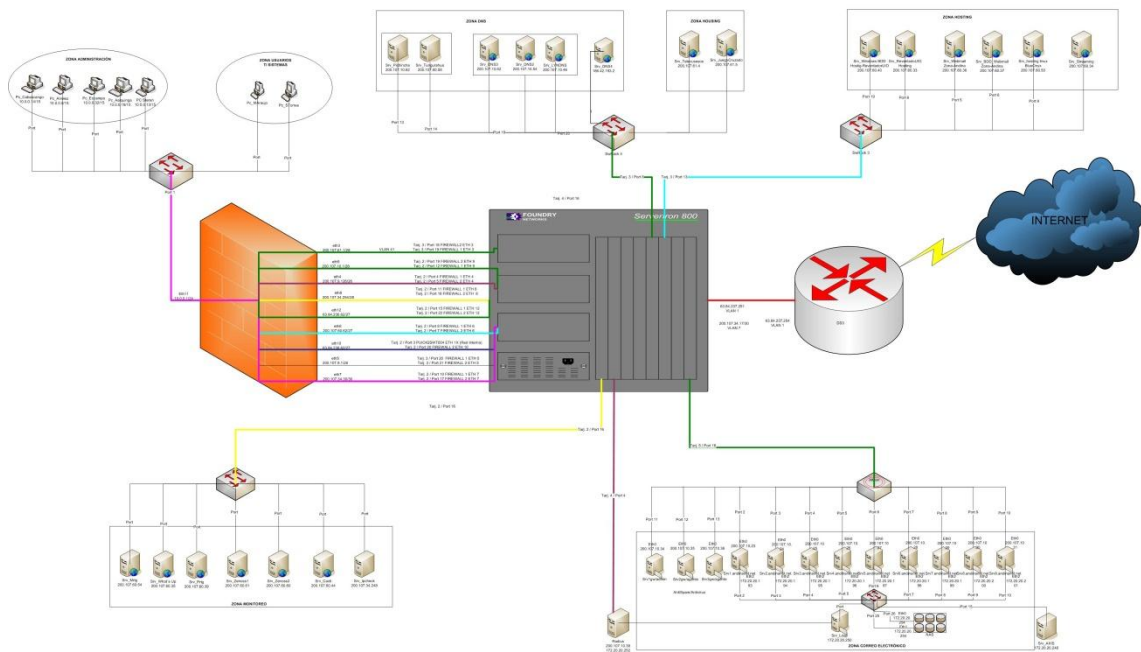


Fig. 15 Diagrama físico de la red de Servidores y Servicios de Internet de la CNT

7.2. Firewall

Firewall (cortafuegos), es el mecanismo que permite, que las comunicaciones entre una red local e Internet se realicen conforme a las políticas de seguridad de quien los instala. Estos sistemas, suelen incorporar elementos que garantizan la privacidad y autenticación, con lo que se impide el acceso no autorizado.

Cualquier servidor, ya sea un servidor web, servidor de correo, servidor de archivos, etc..., dispone de un firewall configurado para sí mismo. Por ejemplo, para un servidor web, únicamente se permite la entrada por el puerto 80 (web) y puerto 21 (FTP). Además, se puede definir, que se utilice el programa de FTP

únicamente desde sus instalaciones, o desde unos ordenadores concretos de sus instalaciones y/o externos.

De esta manera, la configuración y seguridad es máxima.

Los principales riesgos de una organización con salida a Internet son los mismos que debemos tener en cuenta a la hora de proteger un sistema cualesquiera: confidencialidad, integridad, autenticidad y disponibilidad. Los siguientes son los ataques más frecuentes y populares que vulneran estos principios:

- Rastreadores o *Sniffers*.
- Suplantaciones de IP o *Spoofing*.
- Ataques de contraseñas
- Control de salida de ilegal información sensible desde una fuente interna.
- Ataques de Hombre en el medio (o *man-in-the-middle attacks*).
- Ataques de Denegación de Servicio Distribuido , *Denial Distributive of Service* o ataques DDoS.
- Ataques a nivel de aplicación para explotar vulnerabilidades conocidas.
- Caballos de Troya (*Trojan Horses*), Virus y otros códigos maliciosos.

7.2.1. Servidor Firewall

Se puede generar un servidor, para que realice la función de firewall para toda la organización, haciendo de puente entre la red interna de la oficina con Internet (Fig. 7). Al hacer de puente, permite controlar todo el tráfico

que pasa a través del mismo, en las dos direcciones (Internet-red interna y red interna-Internet). Debido a este control, podemos impedir el acceso desde el exterior de cualquier persona no autorizada, se puede especificar para cada usuario, que aplicaciones de Internet puede utilizar, ya sea el Messenger, correo, web, eMule, etc... También permite especificar, que direcciones web se pueden visualizar y cuáles no.

El firewall con las aplicaciones del servidor actualizadas, nos garantiza la completa seguridad del sistema.

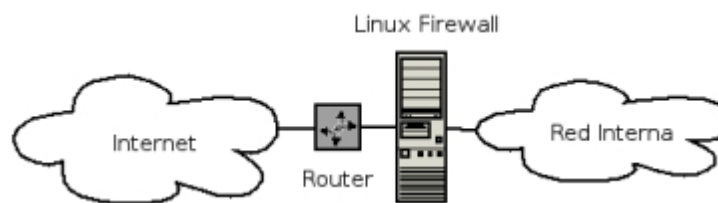


Fig. 16 Firewall

7.2.2. Ventajas y Desventajas de un Firewall

Ventajas

- Administran los accesos provenientes de Internet hacia la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Por ello la seguridad en la red privada depende de la "dureza" con que el firewall cuente.
- Administran los accesos provenientes de la red privada hacia el Internet.
- Permite al administrador de la red mantener fuera de la red privada a los

usuarios no-autorizados (hackers, crackers y espías), prohibiendo potencialmente la entrada o salida de datos.

- El firewall crea una bitácora en donde se registra el tráfico más significativo que pasa a través de él.
- Concentra la seguridad y Centraliza los accesos

Desventajas

- Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación. Por ejemplo, si existe una conexión PPP (POINT-TO-POINT) al Internet.
- El firewall no puede prohibir que se copien datos corporativos en disquetes o memorias portátiles y que estas se substraigan del edificio.
- El firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él, pues el firewall no es un antivirus.
- El firewall no puede ofrecer protección alguna una vez que el agresor lo traspasa.

7.3. DMZ (Zona Desmilitarizada)

Los firewall permiten definir reglas de acceso entre dos o más redes. Sin embargo, en la práctica, las empresas tienen generalmente varias subredes

con políticas de seguridad diferentes. Es la razón por la cual es necesario instalar arquitecturas de sistemas firewall que permitan aislar las diferentes redes de la empresa.

7.3.1. Arquitectura DMZ

Cuando ciertas máquinas de la red interna tienen que ser accesibles desde el exterior (servidor web, servidor de mensajería, servidor FTP público, etc.), normalmente es necesario crear una nueva política para una nueva red, accesible tanto desde la red interna como desde el exterior, sin correr el riesgo de comprometer la seguridad de la empresa. Se habla entonces de una "zona desmilitarizada" (DMZ para DeMilitarized Zone) para designar esta zona aislada que aloja aplicaciones a disposición del público. El DMZ sirve como una zona intermedia entre la red a proteger y la red hostil.

7.3.2. Características

Los servidores situados en la DMZ se llaman "bastiones" debido a su posición anterior en la red de la empresa.

La política de seguridad aplicada en la DMZ, normalmente es la siguiente:

- Tráfico de la red externa hacia la DMZ autorizada;
- Tráfico de la red externa hacia la red interna prohibida;
- Tráfico de la red interna hacia la DMZ autorizada;
- Tráfico de la red interna hacia la red externa autorizada;
- Tráfico de la DMZ hacia la red interna prohibida;

- Tráfico de la DMZ hacia la red externa rechazada.

La DMZ tiene un nivel de protección intermedio. Su nivel de seguridad no es suficiente para almacenar datos críticos de la empresa.

Es necesario notar que es posible instalar una DMZ internamente, para compartir la red interna de acuerdo a los diferentes niveles de protección y así evitar las intrusiones que vienen desde el interior.

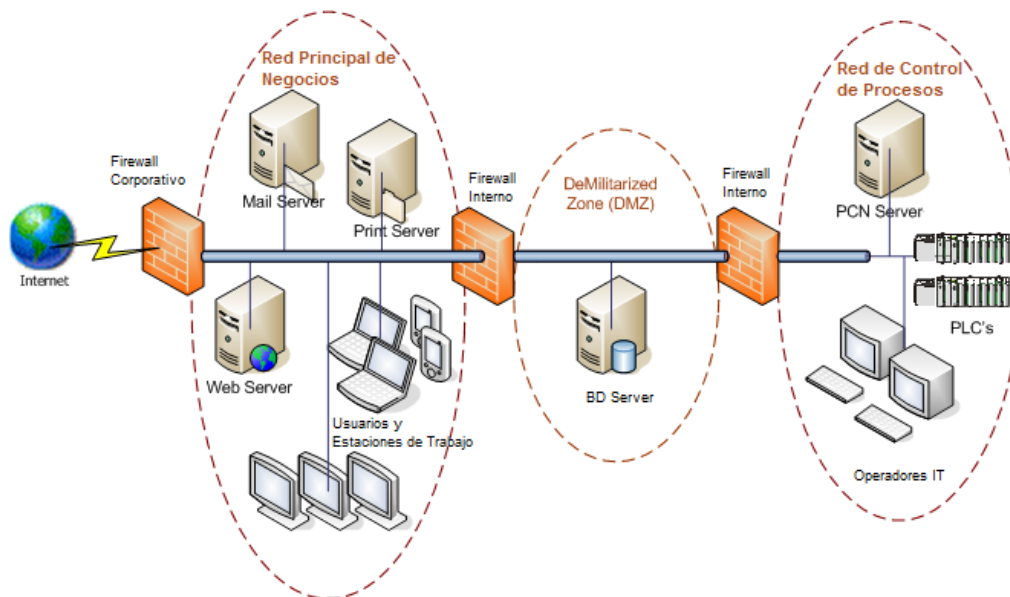


Fig. 17 Funcionamiento de un DMZ

7.8 Conclusión

El webmaster fue capacitado en varias organizaciones entre ellas Megamicro, Telconet y CNT, en el cual participó en Foros y Charlas que indicaban el modo de mejorar la seguridad dentro de la empresa, además una vez demostradas las técnicas expuestas en este proyecto se logró que el webmaster las implemente dentro de su ámbito laboral lo que favoreció ya que disminuyó el gasto por

mantenimiento de equipos a los cuales los usuarios instalaban cantidades innecesarias de software por su parte y se evitó la pérdida de clientes por insatisfacción en el servicio, ya que al caer los servidores todos los servicios a nivel nacional caen, generando así malestar y razón para cancelar el servicio con la empresa.

En conclusión el webmaster está capacitado para generar y mantener las políticas generadas en este proyecto ya que conoce la arquitectura exacta de la red así como las falencias con las que contaba el ámbito de red anterior, por lo tanto siguiendo estas normativas se generaran excelentes webmaster capacitados para afrontar diferentes ataques web.

CAPITULO VIII

8. DDOS

8.1. Introducción

Como ilustración de su presencia en la sociedad digital actual analizaremos cómo cientos de miles de ordenadores domésticos pueden ser utilizados para desencadenar un terrible ataque que puede obligar a cualquier empresa a cesar todo servicio por Internet durante varios días y poner en dificultades los servicios Web

8.2. Redes Ip

El protocolo de comunicaciones facilita un sistema no fiable de entrega de datagramas o paquetes de información entre dos ordenadores cualesquiera conectados a internet.

Esta simplicidad de funcionamiento del protocolo IP permite que sea utilizado como base para la definición de otros protocolos de comunicación utilizados comúnmente en la red Internet

A continuación se detallan los más comunes junto a sus características principales:

- **ICMP** (*Internet Control Message Protocol*) es un protocolo no fiable encargado de regular el flujo de las comunicaciones.

- **UDP** (*User Datagram Protocol*) es un protocolo no fiable de transmisión de datos sin conexión.
- **TCP** (*Transmission Control Protocol*) es un protocolo fiable de transmisión de datos con conexión.

Definiremos las **redes IP** como aquellas redes que utilizan los protocolos TCP/IP para su funcionamiento. Internet es una red IP.

Las redes IP se caracterizan por haber sido construidas siguiendo un esquema de capas. Cada capa es la responsable de cada una de las diferentes facetas de la comunicación. De esta forma, se puede definir la familia de protocolos TCP/IP como una combinación de cuatro capas según el modelo OSI.

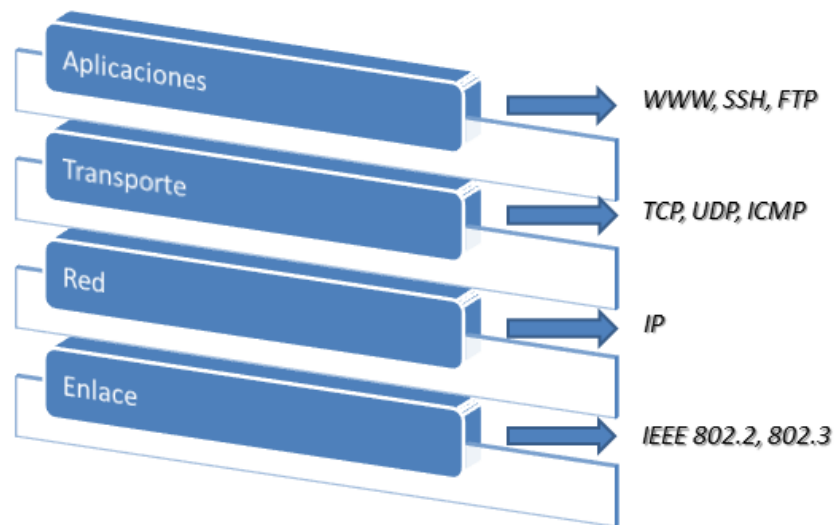


Fig. 18 Modelo OSI (4 Capas).

Este sistema incremental en su construcción permite una independencia entre las diferentes capas y obliga a que la comunicación entre dos ordenadores se

realice mediante una comunicación entre las capas del mismo nivel de los dos ordenadores.

De este modo, la comunicación en Internet se produce mediante el intercambio de paquetes de información entre los distintos ordenadores. Estos paquetes de información, también denominados **datagramas**, viajan por los diferentes ordenadores que están conectados a Internet hasta que alcanzan su destino o son descartados por algún motivo.

De esta forma, en la comunicación de dos ordenadores por Internet podemos diferenciar dos tipos de funciones que pueden desempeñar los ordenadores por los cuales se transmiten los paquetes de información:

1. Ordenador **emisor/receptor** (*end-system o end-host*): Aquí se englobaría el ordenador origen o destinatario de la comunicación.
2. Ordenador **intermedio** (*intermediate-system, router o gateway*): Serían todos los ordenadores por los que van pasando los datagramas o paquetes de información hasta el ordenador destino de la comunicación o hasta el origen (en el caso de una respuesta).

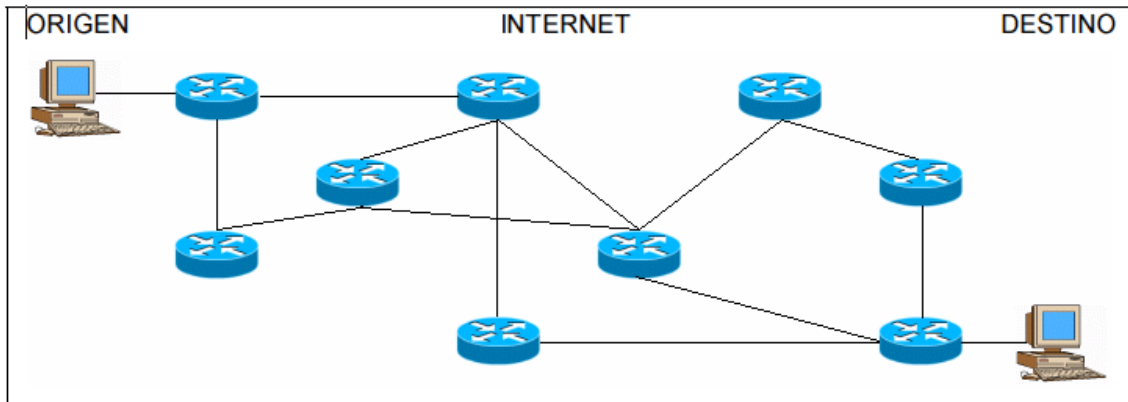


Fig. 19 Ruteado de paquetes por Internet

8.3. Importancia del Internet

En la actualidad casi todas las empresas sean importantes o naturales disponen de servicios “*on-line*” que abarcan desde simples catálogos de sus productos hasta la posibilidad de realizar compras desde cualquier sitio del mundo.

Las empresas digitales (Yahoo, Google, Amazon...) tienen una relevancia y peso económico considerable, ya que actualmente cotizan en bolsa y mueven cientos de millones de dólares al igual que hacen otras empresas más tradicionales como bancos, eléctricas o petroleras.

El envío de *spam* o publicidad indiscriminada, las apariciones regulares de virus, las acciones judiciales en contra de la atentados a la privacidad de los usuarios, hacen que la realidad de Internet sea catastrófica.

8.4. Ataques en redes IP

Desde un punto de vista sociológico, en cualquier grupo social un pequeño porcentaje de su población es malévolo. Con los datos de utilización de Internet anteriormente comentados, podemos observar como si tan sólo el 1 por cien de la población pertenece a este sector tenemos casi 6 millones de posibles atacantes. Incluso suponiendo sólo un uno por mil tenemos la cantidad de casi seiscientos mil peligros potenciales. Cabe notar que esta cifra aumenta progresivamente con la propia expansión de Internet.

Los ataques en redes IP son aquellos perpetrados por usuarios de la propia red que utilizan los protocolos o servicios existentes con el objetivo de conseguir algo de forma ilegal y/o ilegítima.

De esta forma, podemos observar como a diferencia de lo que ocurre en otros medios masivos la propia tecnología que lo sustenta puede utilizarse en su contra.

La gran variedad de protocolos, tecnologías y servicios que sustentan Internet hacen que la posibilidad de realizar un ataque a cualquiera de estos elementos sea elevada, ya que entre otros problemas, la seguridad nunca fue un elemento clave del diseño inicial de Internet.

De la gran cantidad de ataques posibles (Phishing, SQL Injection, Smurfing, DdoS, Etc.) Nos centraremos en aquellos denominados ataques de denegación de servicio distribuido o DDOS (*Distributed Deny Of Service*).

8.5. Características Generales del ataque

Ya que la cantidad de protocolos y servicios existentes en Internet es muy grande y no deja de aumentar. Podemos encontrarnos desde servicios sencillos como resolver nombres (DNS) hasta sistemas complejos.

Las posibilidades de ataque a estos protocolos o servicios son múltiples y aumentan cada día. De esta forma, nosotros nos centraremos concretamente en los ataques de denegación de servicio distribuido principalmente por los siguientes motivos:

- Los ataques distribuidos aprovechan la universalidad de conexión en Internet, lo que hace que proliferen y aumenten su virulencia a medida que crezca el acceso de la sociedad a la red. Cuantos más nodos se conecten, más posibilidades existirán de verse envueltos en ataques. Ya sea como orígenes (un atacante toma el control y lo usa contra un tercero) o como destino de algún ataque.
- Este tipo de ataques continua siendo válido, generalmente, con nuevos protocolos y servicios al igual que lo es con los ya existentes.
- Actualmente no existe ninguna solución universalmente aceptada contra este tipo de ataques.
- De la posibilidad de conseguir una red “segura” para todos sus usuarios depende en gran medida el éxito o fracaso a medio y largo plazo de Internet.

8.6. Definición de DDoS

Podemos definir un **ataque de denegación de servicio (DOS Attack)** como *“la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso”*.

Una vez de definidos los objetivos de un ataque de denegación de servicio realizaremos una ampliación del concepto sumándole la capacidad de acceso simultáneo y desde cualquier punto del mundo que ofrece Internet.

De esta forma definiremos los ataques de denegación de servicio distribuido o DDOS como *“un ataque de denegación de servicio (DOS) dónde existen múltiples focos distribuidos y sincronizados que focalizan su ataque en un mismo destino”*.

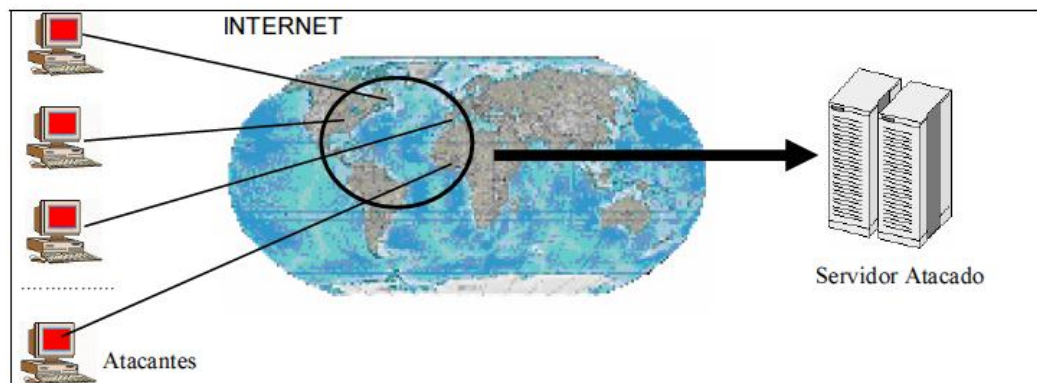


Fig. 20 Ataque típico DDOS

8.7. Virus y Ataques DdoS

EL procedimiento de preparación para un ataque consiste en dos pasos fundamentales:

1. **Conseguir acceso a un ordenador vulnerable.** Este paso conlleva la comprobación de cientos de exploits ¹²para cada una de las posibles víctimas. Pese a existir programas semi-automáticos encargados de las comprobaciones, este no deja de ser un método de fuerza bruta (prueba y error) que consume mucho tiempo y no siempre garantiza resultados.
2. **Instalación del kit de DDOS.** Una vez que se ha conseguido el acceso al ordenador, se debe instalar/compilar (y este paso sí que es manual) los programas necesarios para que el atacante tome en control del ordenador y lo integre en su red de ataque.

Estos dos puntos se han de repetir una y otra vez para cada ordenador que se añada a la red de los atacantes. De esta forma, los ataques proliferan su distribución.

8.8. Propagación a través de Virus

MyDoom, cabe notar que existen actuales mutaciones que posteriormente que modifican su comportamiento, pero el fin básico es el mismo ya que se

¹² Exploit. Es un fragmento de datos automatizado que aprovecha un error causando comportamientos no deseados o imprevistos en los programas informáticos

propaga a través del correo electrónico y afecta únicamente a sistemas operativos Windows.

En la actualidad más del 90% de los ordenadores existentes utilizan la plataforma Microsoft como sistema operativo , lo que nos lleva potencialmente a varios cientos de millones de ordenadores.

El comportamiento de este virus consistía en lanzar desde el ordenador infectado un ataque de denegación de servicio a la dirección que ese momento deseaba ser atacada (páginas de gobierno, comercio, correo, etc.) hasta la fecha que el activista deseaba.

Se hace prácticamente imposible determinar de forma exacta la cantidad de peticiones realizadas por los ordenadores infectados. En cualquier caso, el éxito de este ataque puede ser tan rotundo que la dirección atacada pueda permanecer fuera de uso durante más de una semana.

Este caso puede llevar a la dirección atacada a cambiar de dominio.

Por otro lado, ya no son necesarios conocimientos tan específicos y tiempo para realizar ataques de fuerza bruta. Cualquier persona que simplemente modifique en el código del virus el destino de su ataque (a su colegio, empresa, universidad...) puede fácilmente lanzar DDOS siendo prácticamente imposible demostrar su implicación en el hecho.

8.9. Clasificación de los ataques DDOS

Los clasificaremos en base al estudio de sus dos características fundamentales que comparten todos los ataques DdoS que son las siguientes:

8.10. Consumo de Ancho de Banda

1. La finalidad principal de todo ataque de denegación de servicio simple o distribuido es conseguir el cese temporal de la actividad proporcionada por el objetivo.

Todo y que se pueda alcanzar mediante el uso de distintas técnicas (ataques Trinoo, Tribe Flood Network, Stacheldraht, Shaft y Mstream.) en la práctica siempre acaba mostrando un consumo total de todo el ancho de banda que dispone el nodo atacado.

Las mínimas medidas de seguridad ante ataques DOS/DDOS actualmente consisten por un lado en ampliar la capacidad de la pila IP para poder absorber más peticiones de conexión, y por otro en añadir más servidores para que las conexiones se distribuyan de forma balanceada y no colapsen al servidor.

2. Los ataques DOS/DDOS que se registran pueden realizarse de forma directa (dónde el datagrama utilizado en el ataque ha sido creado en la dirección de origen), indirecta (dónde la dirección de origen ha sido falseada directamente o mediante técnicas de reflexión) o híbrida.

De esta forma podemos clasificar los ataques de denegación de servicio, y por tanto sus soluciones, en dos grupos:

8.10.1. Ataques directos.

Son aquellos en que los datagramas o peticiones recibidas por el objetivo del ataque provienen realmente de la dirección de origen especificada.

Estos ataques son realizados desde ordenadores esclavos (*slaves*) dónde un atacante ha conseguido acceso de forma ilegal, ya sea infectándolo mediante un virus/troyano (MyDoom por ejemplo) o mediante un exploit o root kit¹³, y los utiliza como plataforma de ataque remota.

8.10.2. Ataques indirectos.

En este grupo ubicaremos los distintos ataques que falsean la dirección de origen con el objetivo de esconder su ubicación real y minimizar las posibles contra-medidas adoptadas por el objetivo del ataque.

¹³ Root kit. conjunto de herramientas informáticas que consiguen acceder ilícitamente a un sistema informático para su control remotamente

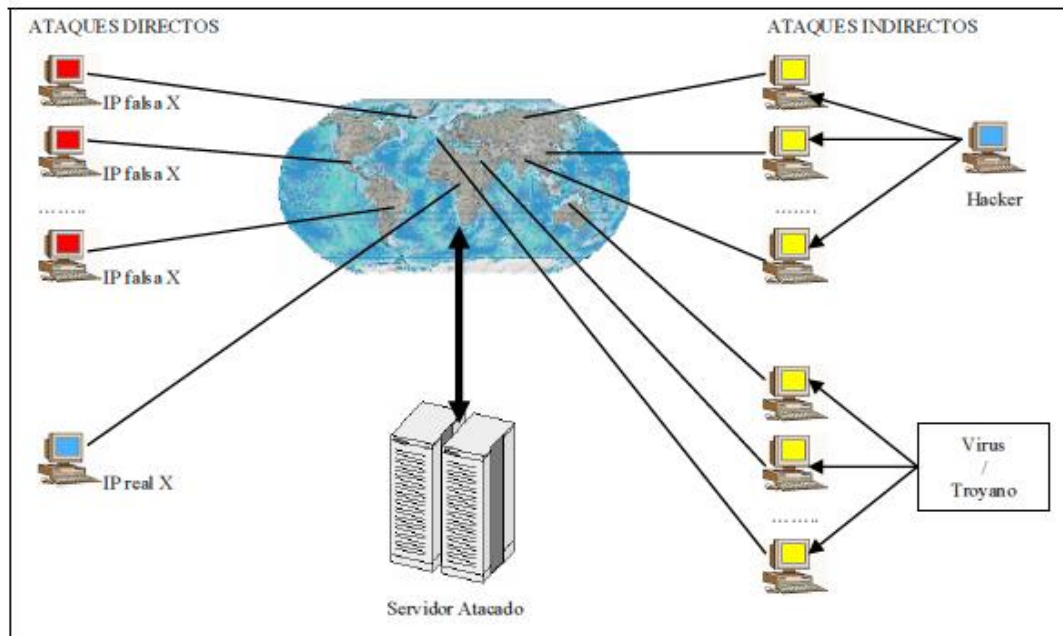


Fig. 21 Ataques DOS/DDoS directos e indirectos.

8.11. Modelos de Ataque DDoS

Un escenario en el que se disponga de un sistema más sofisticado de coordinación, y en el que se pudieran involucrar cientos o miles de ordenadores, supondría disponer de una herramienta de ataque por denegación de servicio que difícilmente podría combatirse. Si resulta difícil defenderse de un ataque de denegación procedente de un único sistema, puede afirmarse que puede resultar imposible en modo coordinado.

En la actualidad se conocen cinco sistemas básicos de ataque distribuido de denegación de servicio:

- **Trinoo,**

- **Tribe Flood Network,**
- **Stacheldraht,**
- **Shaft y**
- **Mstream.**

8.11.1. Trinoo

Los primeros demonios de Trinoo se localizaron en 1999 en forma binaria y en varios sistemas Solaris 2.X que habían sido asaltados utilizando problemas de buffer¹⁴.

En un análisis preliminar se pensó que era un mecanismo evolucionado, basado en protocolo UDP, para la recuperación automática de los resultados obtenidos mediante sniffers. Revisando la fuente (código) del demonio, se vio que el propósito era otro y su funcionamiento era mucho más complejo. El demonio se compiló y ejecutó en Solaris 2.5.1 y Red Hat Linux 6.0. El maestro pudo compilarse y ejecutarse el Red Hat Linux 6.0.

Escenario

En una cuenta de un sistema asaltado se deposita un repositorio de herramientas precompiladas: rastreo, ataque, sniffers, root kits , así como demonio y maestro de Trinoo. El sistema idóneo para un asalto dispondrá

¹⁴ Buffer. Es una ubicación reservada de la memoria en un disco para el almacenamiento temporal de información.

de un gran número de usuarios, y por consiguiente, una gran potencia de proceso y amplio ancho de banda en sus comunicaciones.

Se realiza un rastreo buscando posibles nuevos destinos para posteriores ataques.

Suelen buscarse sistemas Solaris y Linux, dada la disponibilidad de herramientas (Sniffers y root kits) para estos entornos.

Se elabora una lista de sistemas vulnerables que posteriormente se utiliza en un procedimiento de comandos que realiza el asalto. El resultado es una lista de sistemas asaltados dispuestos para alojar *Sniffers* o demonios y maestros Trinoo.

Se seleccionan aquellos sistemas más idóneos para incorporarse a la red y se crea otro procedimiento de comandos que automatiza la instalación de los procesos Trinoo. De esta forma crece la red Trinoo.

Una red Trinoo está formada por Atacantes, Maestros, Demonios y Víctimas, y tendría una estructura como la reflejada en la siguiente figura.

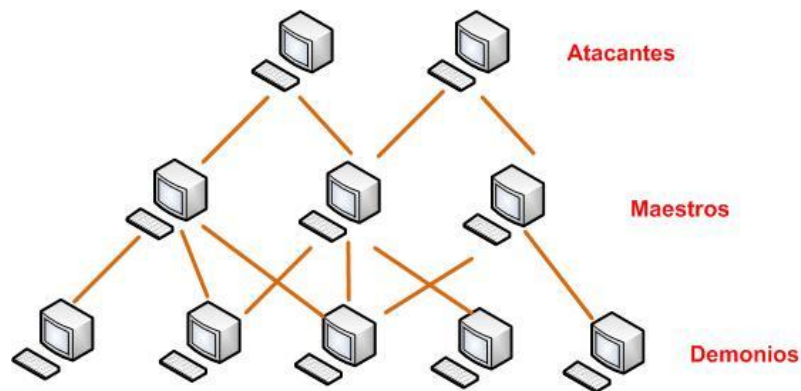


Fig. 22 Ataque Trinoo

El atacante controla uno o más maestros. Cada maestro controla a gran cantidad de demonios. Los demonios son los que reciben la orden coordinada de realizar un ataque contra una o más víctimas por lo general estos son los puertos utilizados:

- Atacante a Maestro: 27665/TCP
- Maestro a Demonio: 27444/UDP
- Demonio a Maestro: 31335/UDP

La comunicación entre el atacante y el maestro, así como la del maestro y el demonio están protegidas por claves de acceso.

Las claves se emplean en forma simétrica, de manera que se almacenan cifradas tanto en el maestro como en el demonio, procediéndose a su comparación con la clave que se proporciona y transporta sin cifrar por la

red. Ciertos comandos enviados por el maestro al demonio también están protegidos por claves, que igualmente se transmiten sin cifrar por la red.

El maestro mantiene una lista de demonios activos, que se almacena y cifra mediante el sistema Blowfish¹⁵. El ataque de Trinoo es del tipo de inundación por tramas UDP.

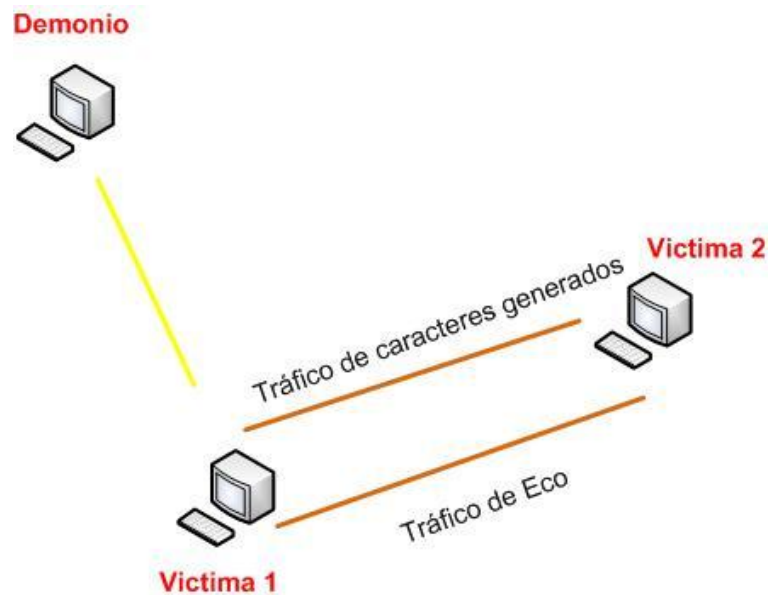


Fig. 23 Ataque Trinoo – Inundación por tramas

En los ataques de este tipo, el atacante (que en este caso en particular sería el demonio) envía tramas UDP con dirección de origen falsa y que consigue enlazar el servicio de generación de caracteres (chargen) de una de las víctimas con el servicio de eco (echo) de la otra. La primera

¹⁵ Blowfish. Conjunto de codificadores y productos de cifrado.

comienza a enviar caracteres que la segunda responde. El volumen de tráfico se va incrementando hasta que los dos sistemas terminan por inundar la red.

8.11.2. *Tribe Flood Network.*

También conocido como TFN, compuesto por un conjunto de programas clientes y demonios que implementan una herramienta de denegación de servicio distribuida, capaz de generar ataques por generación masiva de paquetes ICMP, SYN o UDP, así como ataques del tipo smurfing.

Las tramas SYN, o tramas de sincronización, representan el inicio de una comunicación TCP:



Fig. 24 Tramas de sincronización TCP

Se demuestra que el Sistema 1 solicita iniciar una comunicación (SYN), el Sistema 2 contesta afirmativamente (SYN ACK) al establecimiento de la misma, y el primero termina confirmando el comienzo de sesión (ACK).

En el caso de ataques por inundación con tramas SYN, el sistema atacante, utilizando una dirección inexistente o inoperante, envía multitud de solicitudes de establecimiento de conexión (SYN) al sistema víctima del ataque. Tantas como para llenar la cola de solicitudes pendientes al no contestar los supuestos peticionarios. Esta situación lleva a que las solicitudes reales no puedan ser atendidas, consiguiéndose de esta forma la denegación de servicio. Una red TFN está formada por Atacantes, Clientes, Demonios y Víctimas, con la siguiente estructura:

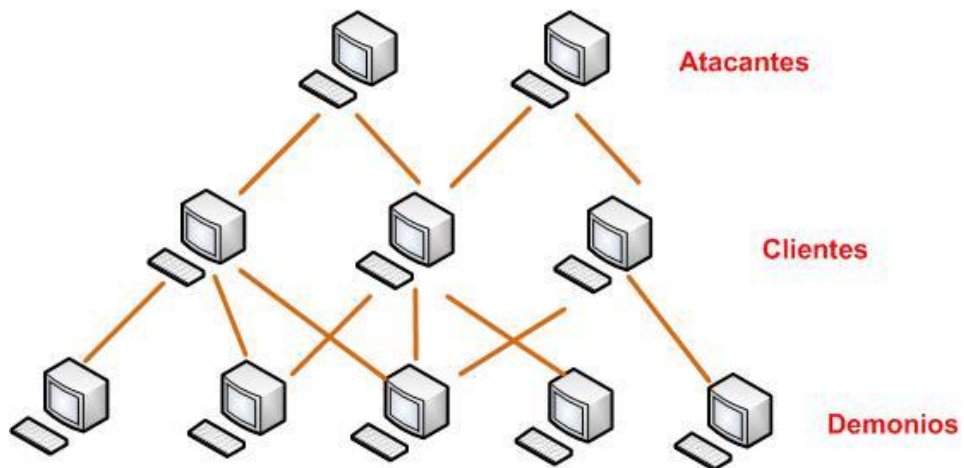


Fig. 25 Control de ataque Tribe Flood

El atacante controla uno o más clientes. Cada cliente controla a gran cantidad de demonios. Los demonios son los que reciben la orden de realizar un ataque coordinado contra una o más víctimas.

El control de la red TFN se realiza mediante comandos enviados al programa cliente.

Estos comandos pueden transmitirse mediante diversos métodos de conexión: shell remoto a un determinado puerto TCP, shell remoto basado en conexiones UDP cliente/servidor, shell remoto basado en conexiones ICMP cliente/servidor, sesión SSH, o un simple Telnet a un puerto TCP.

La comunicación entre los clientes y los demonios se realiza mediante paquetes ICMP_ECHOREPLY, por lo que no existe comunicación del tipo TCP o UDP entre ambos tipos de procesos.

Uno de los puntos fuertes de esta herramienta de ataque por denegación de servicio es que muchas herramientas de monitorización de redes no analizan todo el abanico de paquetes de tipo ICMP o simplemente no muestran la parte de datos de estos paquetes, por lo que la detección de este diálogo puede resultar compleja.

Aunque el acceso a los clientes no está protegido por palabra clave, los comandos que el cliente envía a los demonios van codificados en forma de número binario en dos *bytes*, siendo fijo el número de secuencia del paquete: 0x0000, lo que puede hacer que parezca como el primer paquete generado por un comando *ping*.

Tanto los clientes como los demonios necesitan ejecutar con privilegio de root 5, pues utilizan *sockets*¹⁶. Por otra parte, el cliente necesita disponer del fichero conteniendo la lista de direcciones IP de los demonios (ip list), por lo que localizado el cliente se dispone de la relación de demonios.

8.11.3. *Tribe Flood Network 2000 (TFN2K).*

TFN2K es una evolución del anteriormente comentado TFN. La estructura es similar, aunque cambia la terminología.

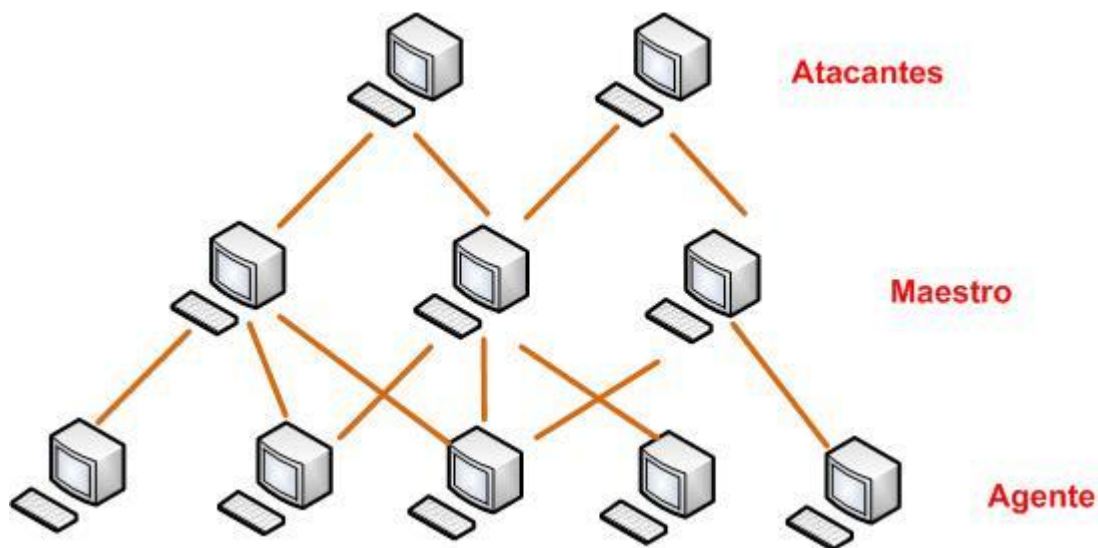


Fig. 26 Escenario Tribe Flood Network 2000

De esta forma, se denomina Maestro al sistema informático en el que corre el Cliente, y Agente al sistema informático donde se ejecuta el Demonio.

¹⁶ Socket. Método para la comunicación entre un programa del cliente y un programa del servidor en una red

El TFN2K permite a los Maestros explotar los recursos de un determinado número de Agentes con el fin de coordinar un ataque a una o más víctimas. El Maestro configura a los Agentes para atacar a una determinada lista de víctimas. Los Agentes atacan a las víctimas por inundación de paquetes.

La comunicación entre el Maestro y el Agente se realiza de forma cifrada mediante el algoritmo CAST-256. La clave se define en el momento de realizar la compilación, y se utiliza como clave de acceso cuando se ejecuta el cliente. Todos los datos cifrados se codifican en Base 64 antes de ser transmitidos.

Con el fin de complicar un posible rastreo de la comunicación entre Maestro y Agente, ésta se mezcla con una serie de tramas trampa enviadas a direcciones IP aleatorias.

Tanto la comunicación Maestro-Agente como el ataque en sí mismo puede realizarse utilizando de forma aleatoria paquetes TCP, UDP o ICMP. Para finalizar hay que añadir el hecho de que el Maestro falsifica su dirección IP (*spoof*¹⁷) en las tramas que envía.

Al contrario de su predecesor, TFN2K es absolutamente silencioso y no contesta a los comandos que recibe. Los comandos no se basan en secuencia de caracteres, sino que van codificados en un *byte*, viajando como datos de la trama los parámetros particulares de cada comando.

¹⁷ Spoof (Spoofing). Hace referencia al uso de técnicas de suplantación de identidad

El agente de TFN2K intenta ocultarse cambiando su contenido, es decir, cambiando el nombre del proceso. El nombre falso se define en el momento de compilación y puede variar de unas instalaciones a otras. Esto le permite camuflarse como un proceso normal, por lo que difícilmente podrá detectarse en una simple revisión de la tabla de procesos activos.

En cualquier caso ha de destacarse lo sofisticado y complejo del desarrollo del TFN2K, así como la dificultad que implica su localización.

Se han encontrado Agentes en plataformas Linux, Solaris e incluso Windows NT. En cualquier caso, la herramienta es fácilmente portable a otras plataformas. Por lo que se ha visto, la detección de TFN2K resulta muy compleja, pero con un estudio exhaustivo, o por un simple error, en la codificación a Base 64 siempre aparece una marca al final de cada paquete. Al final de cada trama se introduce una colección de ceros (entre 1 y 16) que al ser codificados en Base 64 quedan como 0x41 (carácter A). De esta forma, el número de 0x41 que aparecen al final de cada paquete es variable, pero siempre aparece por lo menos uno. La presencia de esta marca permite rastrear y localizar los paquetes de comandos.

Otros errores que pueden ayudar en la detección de tramas generadas por TFN2K son:

- La longitud de los paquetes UDP (la que aparece en la cabecera UDP) es tres bytes mayor que la real.

- La longitud de las cabeceras TCP (la que aparece en la cabecera TCP) es siempre cero, lo que nunca podría ocurrir.
- Los *checksums*¹⁸ de las tramas UDP y TCP no incluyen los 12 bytes de las cabeceras y por lo tanto son incorrectos.

8.11.4. **Stacheldraht.**

El término de origen alemán Stacheldraht podría traducirse por *alambre de espino* o *alambrada de espinos*. Combina características de Trino y TFN, y añade mecanismos de cifrado en la comunicación entre el cliente y el conductor, así como mecanismos de actualización automática de los agentes.

Su estructura, es similar a los anteriores sería:

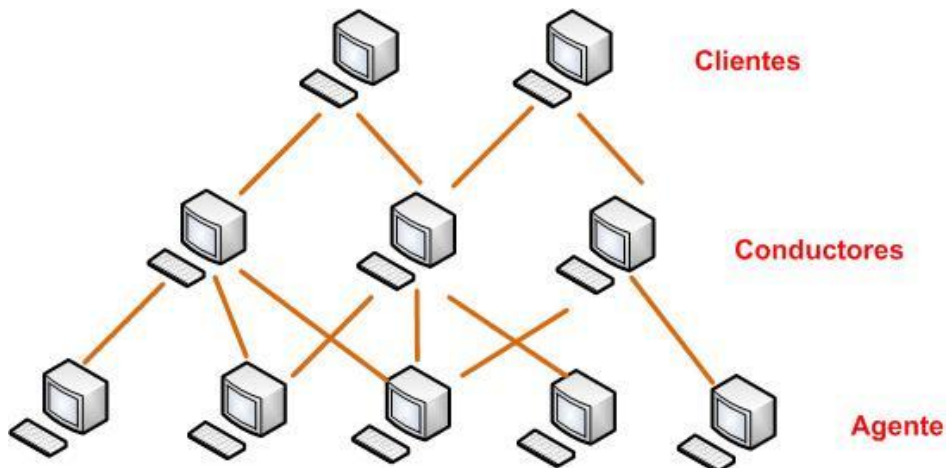


Fig. 27 Escenario Stacheldraht

¹⁸ Checksums. Es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos

Este ataque de denegación de servicio lo realiza mediante avalancha de tramas ICMP, SYN y UDP, así como ataques mediante técnicas de amplificación de *broadcast* (*smurf*).

Stacheldraht dispone de un mecanismo similar a un Telnet (Stacheldraht Term) para la comunicación del cliente con el conductor que incluye cifrado mediante el uso de clave simétrica. Una vez establecida la comunicación entre el cliente y el conductor, se solicita un password que está cifrado mediante crypt(). A partir de ese momento toda la comunicación se realiza de forma cifrada mediante el algoritmo Blowfish.

La comunicación entre los distintos niveles se realiza de la siguiente forma:

- Cliente a Conductor: 16660/TCP
- Conductor a/desde Agente: 65000/TCP, ICMP_ECHOREPLY

La mayor novedad que presenta Stacheldraht respecto a otras herramientas anteriormente analizadas es la posibilidad de ordenar a los agentes su actualización. Para ello se utiliza el comando rcp (514/tcp) sobre una cuenta robada en cualquier máquina de la red. Los agentes borran la actual copia del programa, descargan la nueva versión y arrancan ésta usando nohup. En ese momento finaliza la ejecución de la antigua copia.

En el momento de arranque de un agente, éste intenta leer un fichero de configuración en el que se le indica qué conductores le pueden controlar. Este fichero contiene una relación de direcciones IP y está cifrado mediante

Blowfish. Para los casos en que falle la localización del mencionado fichero, el propio agente lleva definido en el código una serie de direcciones que debe usar por defecto.

Una vez que el agente ha arrancado y dispone de la lista de conductores, comienza a transmitir tramas del tipo ICMP_ECHOREPLY con ID 666 y conteniendo en el campo de datos la palabra "skillz". Todos aquellos conductores que reciben esta trama contestan con otra del mismo tipo, con ID 667 y en el campo de datos la palabra "ficken". El diálogo entre conductor y agente se mantiene de forma periódica, lo que permite detectar la presencia de Stacheldraht mediante la monitorización pasiva de la red a través de un Sniffer.

8.11.5. Shaft.

Es una de las últimas herramientas en detectarse, se piensa es contemporánea a TFN por su modo de operar y mecanismos de control. De hecho, su estructura básica es similar:

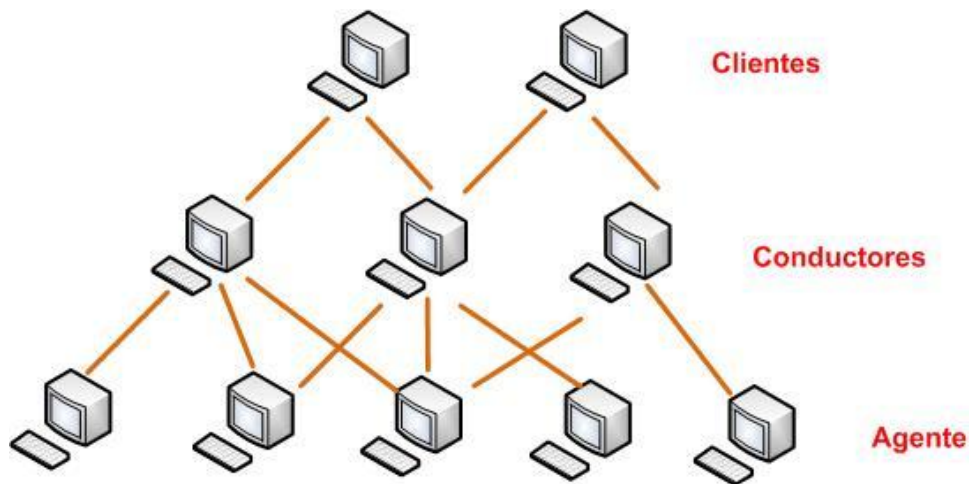


Fig. 28 Comunicación Shaft

La comunicación entre los distintos niveles se realiza de la siguiente forma:

- Cliente a Conductor: 20432/TCP
- Conductor a Agente: 18753/UDP
- Agente a Conductor: 20433/UDP

Una de las novedades que presenta esta herramienta es el uso de *tickets* para garantizar el control sobre los agentes. Tanto el password como el ticket deben ser correctos para que un agente acepte las peticiones que le puedan llegar.

Tanto el conductor como el agente disponen de su propio conjunto de comandos. Aunque el atacante sólo interactúa con el conductor mediante comandos a través de una conexión Telnet.

A través del análisis del código fuente se ha podido detectar la existencia de un cliente por defecto, y definido de la siguiente forma:

```
#define MASTER "23:/33/75/28"
```

que restando 1 al valor decimal de cada carácter (Cifrado de Cesar ⁶¹⁹) obtendremos una dirección IP ejm. 174.25.226.67, que corresponde a www.google.com

Por otra parte, el programa por sí mismo intenta camuflarse como un proceso habitual, como puede ser por ejemplo httpd.

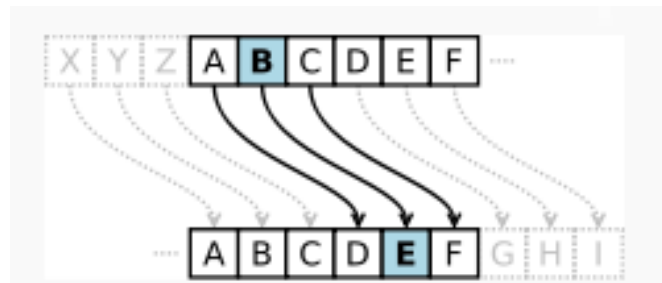


Fig. 29 Cifrado de César

Los autores de Shaft han demostrado tener un interés muy especial por disponer de estadísticas. En concreto, el radio de generación de paquetes de cada uno de los agentes. Es posible que esta información les permita optimizar el número de agentes necesarios para ejecutar un ataque, o añadir más en caso de disminuir el nivel estimado de carga para que el ataque proporciones los resultados esperados.

¹⁹ Cifrado de César. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra.

8.11.6. Mstream.

Ha sido diseñada para bloquear una red ahogando determinados sistemas mediante la generación de gran cantidad de tramas.

Su estructura es muy similar a los sistemas anteriormente citados: un módulo controlador y un módulo agente. El controlador es el encargado de gestionar las relaciones con los agentes. De esta forma, un atacante conecta con el controlador mediante una sesión Telnet para controlar a los agentes.

El tipo de ataque que generan los agentes es una modificación del ataque conocido como “stream.c”, pues la mayor parte del código del agente se basa en dicho programa. El agente envía paquetes TCP ACK al sistema que es objeto del ataque, aunque con la particularidad que dichas tramas se encaminan a puertos seleccionados de forma aleatoria y conteniendo una dirección IP de remitente falsa.

Un ataque de este tipo presenta los siguientes síntomas: El sistema objeto del ataque baja su rendimiento debido al consumo de CPU por el tráfico de red que debe atender. Se observa un consumo elevado de ancho de banda en la red como consecuencia del propio ataque. El sistema atacado ocupa aún más ancho de banda al intentar contestar con tramas TCP RST a los falsos remitentes de las tramas TCP ACK. Los *routers* contestarán a la

víctima con tramas ICMP indicando que el destinatario de la trama TCP RST no existe, lo que también consume aún más ancho de banda.

Aunque cuando este tipo de ataque proviene de un único sistema no suele producir grandes efectos en el sistema atacado, pero cambia el panorama cuando son varios los sistemas atacados y muchos los atacantes, pues sólo tiene un desenlace: la saturación de la red, si no la caída del sistema atacado, y por consiguiente la denegación de servicio, que es el objetivo final.

La arquitectura de este sistema es similar a los anteriormente vistos:

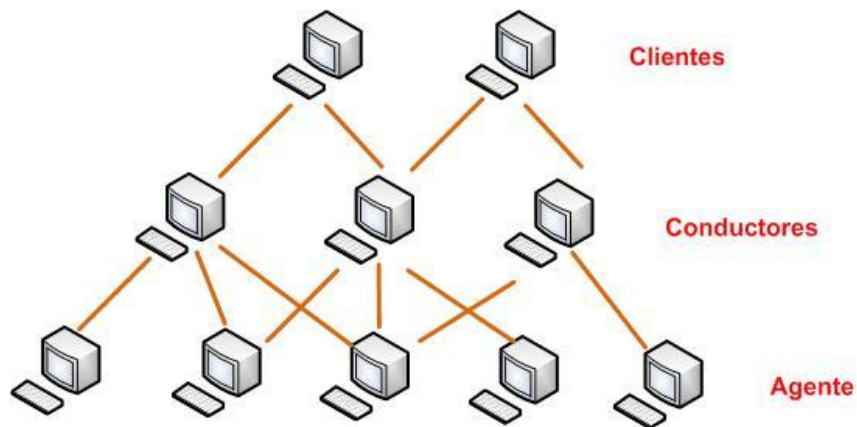


Fig. 30 Modalidad MStream

El cliente es la máquina que el atacante emplea para lanzar el ataque. El conductor coordina a todos los agentes. Y son éstos los que realizan el ataque a la víctima. Cada conductor puede coordinar un número indeterminado de agentes, y cada agente puede estar coordinado por un número indeterminado de conductores. Los agentes necesitan ejecutar con privilegio de root(Administrador.

Se han encontrado tres versiones de esta herramienta, y en cada una de ellas varían los puertos y los passwords utilizados para la comunicación entre los distintos componentes.

Los agentes pueden transmitir dos tipos distintos de paquetes. Uno es un “pong”, como respuesta a una petición “ping”. El otro es un “newserver”, indicando que la dirección IP indicada se añade a la lista de agentes. Dicha lista se mantiene en el fichero “.sr”. Las direcciones IP se codifican añadiendo 50 al valor ASCII de cada carácter de la dirección IP (Cifrado de Cesar).

Por otra parte, cada agente lleva incluido en el propio código la lista de posibles conductores autorizados, con un máximo de tres, lo que obliga a definirlos en el momento de compilar.

Los agentes atienden por el puerto 7983/UDP los posibles comandos que les puedan transmitir los controladores. A parte del comando “ping”

anteriormente citado, pueden recibir el comando “Mstream”, cuyo formato es:

```
Mstream/a1.b1.c1.d1:a2.b2.c2.d2: .../T
```

Donde ax.bx.cx.dx representan las direcciones IP de los sistemas que deben ser atacados, y T representa la duración del ataque expresado en segundos. Existe también el comando “stream”, que es similar a “Mstream”, pero que sólo permite lanzar el ataque a una única dirección IP, y en este caso la dirección IP del atacante es la real y no una falsa.

8.11.7. LOIC

Low Orbit Ion Cannon es una aplicación diseñada para realizar un ataque de denegación de servicio distribuido, usando el lenguaje de programación C#. La aplicación realiza un ataque de denegación de servicio del objetivo enviando una gran cantidad de paquetes TCP, paquetes UDP o peticiones HTTP con objeto de determinar cuál es la cantidad de peticiones por segundo que puede resolver la red objetivo antes de dejar de funcionar.

LOIC incorpora la posibilidad de que el usuario delegue voluntariamente el control de la aplicación LOIC al operador de un canal IRC, que puede controlar de esta manera un ataque coordinado empleando todos los clientes conectados a dicho canal. Esta característica se denomina

comúnmente como inteligencia de enjambre (*Hive Mind*) y permite la organización rápida de una botnet formada por voluntarios. La versión con control remoto por IRC se denomina habitualmente IRCLOIC.

También funciona en sistemas Linux con los paquetes Mono o Wine.

En las últimas versiones se ha añadido una opción para iniciar el programa oculto como un servicio de Windows.



Fig. 31 Utilización LOIC

CAPITULO IX

9. POLÍTICAS DE SEGURIDAD

A la hora de implantar una política de seguridad en la empresa hay que partir de la base de que el sistema o la red 100% segura no existen. Se ha de hacer una valoración de los recursos a proteger, de tal manera que el esfuerzo y coste de la implementación del sistema de seguridad sea proporcional a su valor. Incluso se pueden definir áreas de la red interna de la empresa con información más valiosa o confidencial que deberían ser protegidas con mayor cuidado que otras.

Una técnica que empieza a implantarse en la política de seguridad es la realización de Auditorías de Seguridad. Estas pueden ser llevadas a cabo por el personal de la propia empresa o por sus consultorías externas. Una auditoria de seguridad comprende entre otras las siguientes actividades:

- Evaluación de los recursos y la información a proteger
- Evaluación de los sistemas de seguridad implementados y de aquellos que se podrían implementar
- Prueba del estado de seguridad de la red informática en general y de cada uno de los sistemas conectado a ella en particular, mediante la ejecución de programas o el empleo de técnicas que traten de explotar y pongan de manifiesto los posibles agujeros de seguridad.
- Elaborar planes de contingencia y de seguridad.

La seguridad de una red informática pasa por involucrar o concienciar a todos los usuarios y administradores de sistemas en los temas de seguridad y las implicaciones legales del uso de una red informática.

Cada vez que se viola la política de seguridad, el sistema está sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando esta sea violada, en ese caso debe modificarse la política implanta para eliminar aquellos elementos que no sean seguros.

La política de seguridad y su implementación deben ser lo menos obstructivas posible. Si la política de seguridad es demasiado restrictiva, o no está bien explicada, es probable que sea violada o desactivada.

Al margen del tipo de política que se implemente, algunos usuarios tienen la tendencia a violarla. En ocasiones las violaciones a la política son evidentes; otras veces estas infracciones no son detectadas. Al momento que se detecte la violación a la política de seguridad, debe determinar si esta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia de la política vigente.

La política implementada debe contener lineamientos acerca de las acciones correctivas para las fallas de seguridad. Es razonable esperar que el tipo y severidad de la acción dependan de la gravedad de la violación.

9.1.Desarrollo de Políticas

La siguiente lista puede usarse como lineamiento para ayudar a determinar cuando el sitio debe usar una política. La estrategia de la implementación se la puede ayudar en las siguientes circunstancias.

- Si los recursos de la red no están bien protegidos de los intrusos.
- Si la continua actividad del intruso pudiera resultar en daños y riesgos financieros considerables.
- Si el costo de la demanda es demasiado elevado, o si no existe voluntad o posibilidad de demandar.
- Si existen considerables riesgos para los usuarios actuales de la red.
- Si en el momento del ataque no se conocen los tipos de usuario de una gran red interna.
- Si el sitio está sujeto a demandas judiciales por parte de los usuarios.
- Esto se aplica a las compañías de seguros, bancos, formas de seguridad, proveedores de red, etc.
- Si existe gran rotación de personal en la organización
- Si los usuarios son autores de continuos daños en los sistemas ya sean de gestión u operativos.

Estos lineamientos son los más comunes dentro de las organizaciones por lo cual se tomara en cuenta estas características para la creación de políticas de seguridad.

9.2. Políticas a implementar.

Ante la delicada situación que puede presentarse a corto plazo, se contempla una serie de recomendaciones dirigidas a Responsables de Informática, Administradores de Sistemas, Proveedores de Servicios de Internet y Grupos de Respuesta a Incidentes.

Desgraciadamente, y más que nunca, es necesario insistir en que la mejor medida adoptable es la prevención. La versión de los protocolos IP actualmente en uso (IPv4) no permiten mayores mecanismos de seguridad, y hasta que se generalice el uso de IPv6, se seguirá sufriendo ataques como los hemos visto

En general, puede decirse que la única forma que tiene una organización de detener un ataque DDoS es el identificar los demonios que lo están generando y filtrarlos individualmente al router principal. Esto es una labor lenta, pero efectiva.

Para el desarrollo de las políticas se presentan las siguientes características:

- **Asignar propiedad a información y equipos.**
 - Al momento de la entrega de un equipo a un usuario se debe firmar un check list con las características físicas y lógicas del computador (Ram, SO, Procesador, Mainboard, Unidad CD/DVD y Estado del PC) y almacenarlo en bitácoras ya que al momento de cambio de

equipos o cambio de usuario se revise las características con las que se recibe y así poder tomar decisiones en cuanto a descuentos.

- **Enfocar la expresión de políticas de forma positiva.**
 - Crear charlas a nivel general con los Jefes de cada área y sus empleados generando así confianza entre empleador y empleado, indicando que los equipos se encuentran a disposición del empleado con el debido cuidado que los utilice.
- **Recordar que empleados y usuarios son personas**
 - Por esta razón los equipos están propensos a diferentes tipos de daños, entre ellos virus, spam, mal funcionamiento del SO ya que el humano por naturaleza es inquieto, a lo que se tomaría las medidas de restringir los permisos del equipo en:

Panel de Control/Usuarios/Administrar Cuentas/Tipo de Cuenta y establecerla en usuario Estándar, además ejecutar el comando Gpedit.msc el cual nos abrirá las directivas de grupo y administración del equipo y cambiar las características a modo RESTRINGIDO.
- **Educar a los usuarios.**
 - Se debe aplicar la técnica IHC (Interacción Humano Computador) que nos enseña a entender y conceptualizar la interacción entre HC, entender al usuario e identificar necesidades y establecer requerimientos.
- **Responsabilidad debe conllevar autoridad.**

- En la empresa se debe tener en cuenta que lo laboral es lo laboral y las amistades son después de la hora de salida, no ceder a peticiones que indique la habilitación de características restringidas para diversión del usuario.
- **Conocer el perímetro de seguridad (portátiles, PDAs, redes inalámbricas, ordenadores utilizados en casa, DVDs, discos extraíbles, visitas, impresoras, copiadoras, fax,..)**
 - En el router que se instale se debe realizar un control de MAC a los equipos que ingresen a la red, el cual impedirá el ingreso de otros equipos a la red, y cada sesión de equipos que pidan autorización deberán tener un tiempo estimado de habilitación en la red, además este Router deberá estar separado de la red interna de la empresa por cuestiones de sniffing.
 - La configuración del Firewall en la Opción de Ingress filtering tendrá el máximo de 3 ingresos al sistema por minuto, caso contrario será bloqueada la Ip y reportada en el visor de sucesos del equipo. Al igual que en el sistema el usuario podrá loginearse hasta 10 veces al día ya que el sistema se bloque cuando no funciona por 1 hora.
- **Niveles independientes y redundantes de defensa a varios niveles, con auditoría y monitorización**
 - Se creara dos tipos de Técnicos (Nivel 1 y Nivel 2)

- Técnico Nivel 1 – será el encargado de realizar el soporte y el ingreso de equipos a la red, además configurar los parámetros de cada computador como administrador y usuario
 - Técnico Nivel 2- Interactuará con el Webmaster en la generación de habilitaciones y restricciones a cada usuario dentro de la red y remotamente, además serán los encargados de capacitar a los empleados en las políticas implantadas.
- **Mantener actualizados los sistemas, aplicando los parches destinados a eliminar vulnerabilidades**
 - Mantener un sistema de servidores, firewall con los últimos parches y/o actualizaciones de sus sistemas respectivos ya que estas cuentan con la seguridad respectiva de la actualidad. En el caso de los computadores de los usuarios que cuentan con el SO Windows 7 debería estar actualizado con la versión KB2641690, en cuanto al equipo Zyxel, Cisco y Firewall contar con el ultimo firmware ya que este resuelve los problemas de fabricación de los equipos en este caso de estos equipos serían los siguientes:
 - Zyxel USG 1000 Versión 2.20(AQV.1)
 - Cisco1841 Versión 12.3(11)
 - Firewall Networkshield Versión 2.70.0410

- **Filtrar todos los puertos, dejando únicamente operativos aquellos que sean estrictamente necesarios.**
 - El filtrado de tráfico de salida o *“egress filtering”* tiene por objetivo el control de las direcciones IP utilizadas en la red dónde esté aplicado. De esta forma podemos poner un filtro que compruebe todo el tráfico de salida y elimine todos aquellos paquetes que no pertenezcan al rango de IP válido. En este caso en el firewall será habilitado el puerto 3128, 80, 8200 que será el puerto que utiliza el sistema de gestión de la empresa
 - EL filtrado de tráfico de entrada o *“ingress filtering”* tiene como objetivo asegurar que todos los datagramas que entran a nuestra red provienen de direcciones IP reales o existentes. En el equipo Zywall USG 1000 cuenta con la opción de Detección de Intrusos (IDS) el cual nos ayudara con el monitoreo del trafico existente en la red.
- **Actualización de sistemas antivirus y software para detección de intrusiones. Para esto son de gran utilidad herramientas de auditoría de sistemas y auditoría de redes.**
 - En este caso la aplicación de un Sistema de Detección de intrusos (IDS) que es un sistema para realizar una defensa reactiva en cuanto a intrusiones en este caso se utilizara el IDS de

Zywall USG 1000. En la práctica se utilizan para registrar y actuar frente ataques o intentos de ataque. por lo general, actúan a nivel de aplicación mediante el uso de diversas técnicas: desde detección de patrones estáticos o expresiones hasta técnicas de inteligencia artificial y/o data mining. El antivirus con el que cuenta la empresa es Kaspersky 2011 Corporate, el cual se actualiza diariamente a través del Internet.

- **Es fundamental la existencia del Centro de Emergencia de Datos como medida de prevención de desastres**, pero también es fundamental que los ataques del tipo DDoS entren dentro de lo que podría denominarse desastre, teniendo previstos los mecanismos que permitan continuar la actividad en un plazo mínimo de tiempo.
 - Para esta medida se adquirió los 4 servidores HP Proliant los cuales harán réplicas online de los Servidores que se encuentra en funcionamiento dentro de la organización mediante la herramienta Hamachi con Licencia la cual cuenta con Firewall, IDs, Proxy, https, para sus conexiones seguras, el punto que se encontraran estos servidores será el Área de Chilibulo donde se encuentra El nodo Matriz de la Empresa, el cual tendrá un Acceso dedicado para estos servidores a través de Telconet.

- **Modificar las contraseñas de acceso tanto del usuario como del administrador del sistema, según sea necesario para mantener la seguridad del sistema.**

- La creación de contraseñas serán creadas por parte del administrador de la red o Webmaster y serán guardadas en su respectiva BD, ya que al estar dentro de un Domino estas deberán ser cambiadas en un lapso de 3 meses, el modo de creación de las contraseñas será en base a las siguientes normas : las siguientes:

- 3 primeras letras del Área ejm. Contabilidad
- 4 primeras letras o iniciales Nombre de Equipo ejm Auxiliar 1
- Numero de Trimestre del año. Ejm si estamos en noviembre será 4.

De este modo tendríamos la siguiente contraseña para la Computadora del Auxiliar 1 en el área de contabilidad: conaux14.

- La creación de un plan de contingencia al momento de sufrir un ataque al que no se le pueda detener rápidamente la organización debería contar con un plan de emergencia al respecto que justifique la pronta acción de un Área de sistemas aplicado a la realidad.

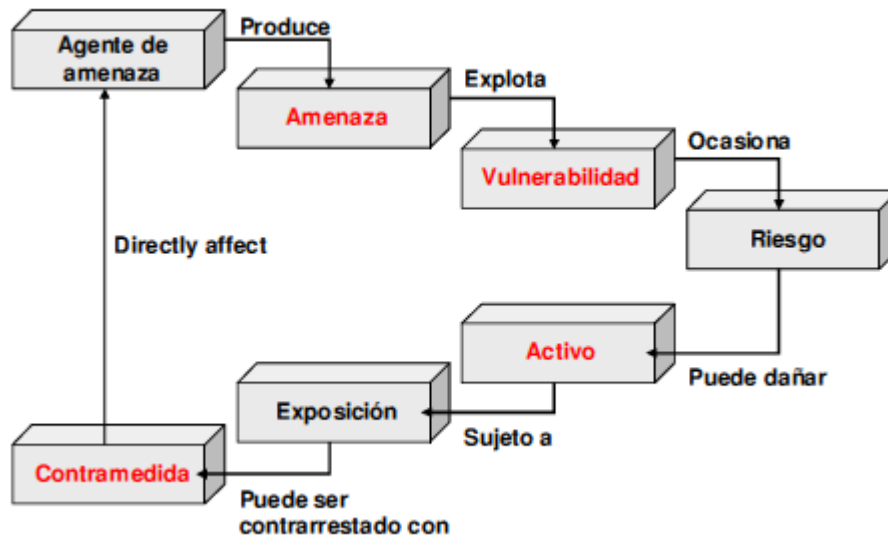


Fig. 32 Transición de un Plan de Contingencia

9.3. Plan de Contingencia.

Al momento de que una amenaza resulte imposible detenerla en un tiempo definido se debe tener en marcha un plan de contingencia que permita recuperar la integridad de sus sistemas expuestos. Pero como toda planificación al respecto necesita contemplar características necesarias como las siguientes:

- **Personal necesario**
 - 2 Técnicos de planta en la Oficina principal y Webmaster en el Área de Respaldo de Servidores.
- **Lugares de operación**

- Oficinas donde se encuentran los servidores principales (Edificio Concorde 2 piso) y donde se encuentran los servidores de Backup (Chilibulo)
- **Equipamiento alternativo**
 - Router CISCO 1841 en el área de Servidores Backup, Antena Nanostation Rocket M5 para crear un enlace punto a punto desde Chilibulo hasta la oficina principal con el proveedor alterno.
- **Configuraciones a utilizar**
 - Se configurara y se dará de alta al sistema de gestión a través del puerto 8023 en los servidores de Backup, con un enlace punto a punto hacia la oficina principal, recuperando así el sistema a nivel nacional, se reportara vía mail a las plazas a nivel nacional el nuevo link de ingreso al sistema.
- **Tiempo**
 - El tiempo estimado será de 2 horas de gestión con traslado desde la oficina principal hacia los servidores Backup, el cual regresara a la normalidad una vez solventado el ataque en horas de la noche 10 pm.
- **Solución de Inconvenientes.**
 - Revisión de configuración de equipos firewall, IDS, en caso de no detectarla se procederá con el reseteo del equipo y la

configuración manualmente de las características del equipo.

Esto permitirá la detección de la Ip que nos envía el ataque.

Resulta muy importante comprender cómo las distintas tareas automatizadas, van a ser ejecutadas manualmente si esto fuera requerido.

9.4. Consideraciones

Para que las políticas creadas puedan tomarse en consideración debería tener los siguientes aspectos:

- **Debe ser dictada por un Comité de Seguridad.**
 - Crear un comité que con una lluvia de ideas genere las acciones y relaciones que puedan las amenazas en la empresa. Esta puede ser conformada por el Gerente Técnico, los Supervisores Técnicos a nivel nacional y el Gerente General en calidad de usuario
- **Debe ser aprobada por las máximas autoridades.**
 - Contando con la presencia de las personas idóneas para la creación de las políticas será más fácil llegar a un acuerdo con las áreas de mayor relevancia dentro de la empresa.
- **Debe ser comunicada a todo el personal y terceros.**
 - Crear reuniones con el fin de promover el uso de las políticas implantadas dentro de la organización.

- **El personal y los terceros debe aceptar formalmente la Política.**
 - La reunión realizada quedará firmada en un acta en la cual se hace constancia de la fecha en la cual se implementa las políticas, para más adelante poder definir la relevancia que genere dentro de la organización.
- **Debe integrarse con la Política de Gestión de Riesgos.**
 - Es parte principal la integración de estas normativas en la Gestión de Riesgos, ya que estas previenen que estos se den.
- **Debe ser escrita en lenguaje claro sin ambigüedades.**
 - Toda política debe ser entendida claramente por los usuarios que se encuentran a cargo de la organización ya que va dirigido a ellos para evitar los ataques internos/externos tanto voluntarios como involuntarios.
- **Debe ser consistente con las normativas legales y corporativas existentes.**
 - Al momento de crear estas políticas no deben interferir con la integridad del usuario, se debe respetar su privacidad pero a la vez controlar que las actividades laborales se den conforme a lo establecido en las normativas administrativas de la empresa

9.5. Conclusión

Para que los procesos de seguridad sean eficientes requieren de la participación de todos los miembros de la empresa; en tanto que la responsabilidad de la

gestión de la seguridad corresponde a la alta dirección.

La persona encargada de realizar esta gestión debe tener un control absoluto sobre los procedimientos de seguridad implementados ya que es quien asume la responsabilidad última de su funcionamiento.

Tomando en cuenta todas estas características se ve reflejada la labor realizada en base a la tranquilidad que se obtiene al contar con medidas de seguridad para evitar ataques y planes de contingencia en últimas instancias.

CAPITULO X

10. CONCLUSIONES Y RECOMENDACIONES

10.1. Conclusiones

En base al estudio Realizado se puede definir que la mayoría de pequeñas y grandes empresas cuenta con sus servicios web ya sea informativos o transaccionales, además cuentan con sus respectivas áreas de informática, pero no la mayoría no se encuentran preparadas para afrontar ataques web, ya sea porque no tienen las políticas informáticas respectivas, o en su defecto las tienen pero no las utilizan.

Con la implementación de las políticas dentro de la Empresa Interactive by Zenix, se puede decir que los factores de infección por parte de virus o ataques a disminuido dentro de la empresa, se puede decir que tanto los usuarios como el webmaster llevan un control de orden en las distintas actividades que se realizan en los equipos informáticos dentro de la organización.

Dentro de las estadísticas establecidas en conjunto con la empresa, el webmaster indica que disminuyo el daño de equipos por parte de los usuarios y el mantenimiento de la red es mucho más fácil, debido al control que se tiene por cada uno de los equipos en bitácora.

En conclusión la implementación de una política en general dentro de una organización implica la inversión de una cantidad de dinero que al final se la ve reflejada por un buen trabajo en un excelente ambiente de trabajo y con la

seguridad de que se está capacitado para prever algún tipo de amenaza informática.

10.2. Recomendaciones

Se recomienda la creación de normas y políticas que ayuden combatir los ataques web que generan la pérdida de información, así como la pérdida de recursos financieros ya sea por caída de servicio o ingresos no deseados. O en su defecto si la empresa cuenta con las políticas establecidas, llevarlas a cabo tal y como son expuestas, esto ayudara con llevar de mejor manera el control de la información.

Además se requiere recomendar que como usuario mantener la ética en la empresa, al realizar filtraciones de información a lugares indebidos, así como la mala utilización de los recursos otorgados por la organización

CAPITULO XI

11. BIBLIOGRAFIA

Arronategui, U. (S/A). *Seguridad Informática*.

<http://definicion.de>. (s.f.). Obtenido de <http://definicion.de/politica>

<http://www.arcert.gov.ar>. (s.f.). Obtenido de

<http://www.arcert.gov.ar/seguridadweb.html>

<http://www.desarrollandoweb.com>. (s.f.).

Ley de Acceso a la Información Pública para el Estado Ecuatoriano. (s.f.).

Martínez, F. L. (2000). *Sistemas Distribuidos de Denegación de Servicio*. Madrid.

Mendoza, I. J. (Diciembre 2000).

www.legal-protect.com. (s.f.). Obtenido de ([http://www.legal-](http://www.legal-protect.com/index.php?option=com_content&task=view&id=247&Itemid=2)

[protect.com/index.php?option=com_content&task=view&id=247&Itemid=2](http://www.legal-protect.com/index.php?option=com_content&task=view&id=247&Itemid=2))

www.webtaller.com. (s.f.). Obtenido de www.webtaller.com:

<http://www.webtaller.com/maletin/articulos/definicion-webmaster.php>

<http://msdn.microsoft.com/es-es/library/ms345212%28v=sql.100%29.aspx>

<http://www.forosdelweb.com/f20/firewall-para-servidor-web-216600/>

<http://es.scribd.com/doc/52089734/36/FIGURA-2-10-Implementacion-de-Firewall-con-DMZ>

<http://www.computing.net/answers/security/firewall-vs-proxy-server/162.html>

http://www.totemguard.com/content/products/prod_fw.php

<http://www.mpsnet.com.mx/servicios/equipamiento/firewalls/ventajas>

<http://www.desarrolloweb.com/articulos/996.php>

<http://forum.pfsense.org/index.php?topic=28151.0>

<http://delta.cs.cinvestav.mx/~gmorales/OwnSecurity/InternetYArquitectura.pdf>

http://www.isaserver.org/articles_tutorials/archive/2011/

http://www.munilapunta.gob.pe/transparencia_standard/planeamiento_organizacion/Informacion_adicional/PLAN%20DE%20CONTINGENCIA%20MDLP-F.pdf

http://www.munilapunta.gob.pe/transparencia_standard/planeamiento_organizacion/Informacion_adicional/PLAN%20DE%20CONTINGENCIA%20MDLP-F.pdf

<http://www.compuseguridad.com/consultoria/contingencia-informatica.html>

<http://msdn.microsoft.com/es-es/library/zdh19h94%28v=vs.80%29.aspx>

<http://proxy-server-firewall.smartcode.com/>

<http://www.segu-info.com.ar/politicas/contingencia.htm>

<http://www.s21sec.com/servicios.aspx?sec=47&apr=51>

<http://www.tecneca.com/servicio.php?serv=hardware>

<http://www.isa.uniovi.es/docencia/redes/Apuntes/tema8.pdf>

<http://www.zentense.com/zenweb/es/portfolio/;jsessionid=i8te598oswkr>

http://www.siaa.udg.mx/html/pronad/doctos/introduccion_siia.pdf

<http://www.youblisher.com/p/6868-No-Title/>

<http://www.gestiopolis.com/Canales4/mkt/simparalas.htm>

<http://www.madridteacher.com/politica.htm>

<http://webpolitica.blogspot.com/>

<http://www.youblisher.com/files/publications/2/6868/pdf.pdf>

http://www.vistnet.com/images/network_map.png

<http://www.viajes123.com/wp-content/uploads/2011/05/guia-de-viajes-de-paris.jpg>

<http://seguridadwebecuador.blogspot.com/>

https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf

<http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf>

<http://www.bitdefender.es/seguridadinformatica/%C2%BFsera-el-internet-controlado-por-ataques-ddos.html>

http://www.emarket.cl/dir/umayor/topinf/065_Manual%20de%20Contingencia%20Informatico.pdf

https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf

CAPITULO XII

12. ANEXOS

12.1. Portada del Blog



Mantienes Politicas de Seguridad al Establecer tu Portal Web ?

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico donde nos encontremos.

En ese sentido, ya no sorprende la transferencia de información en tiempo real o instantáneo y debido a que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizar el comercio en forma electrónica, con objeto de ser más eficientes.

No obstante, al unirse en forma pública se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

Complete el siguiente formulario Por Favor.

DDOS / ANONYMOUS !!!

con la tecnología de 

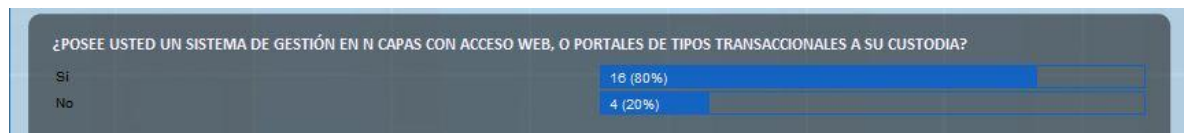
DATOS PERSONALES
Netsystems Corp.
Ver todo mi perfil

SEGUIDORES

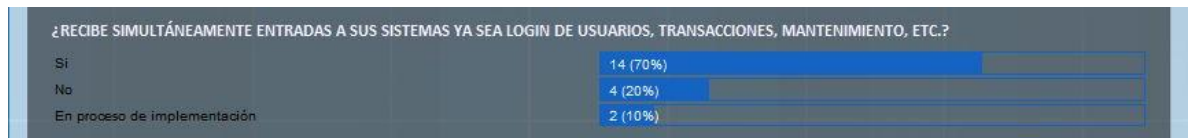
Participar en este sitio 
Google Friend Connect

Todavía no hay miembros.

12.2. Pregunta 1



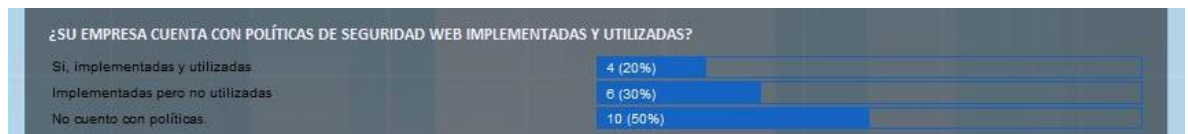
12.3. Pregunta 2



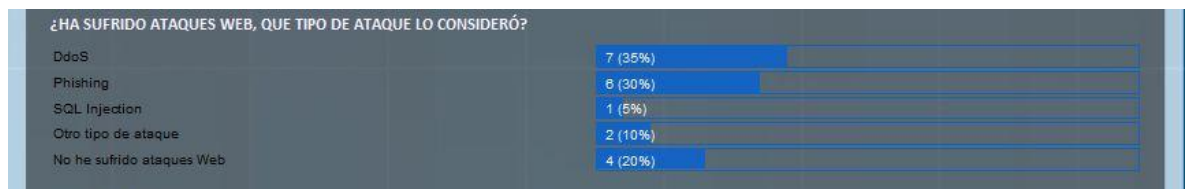
12.4. Pregunta 3



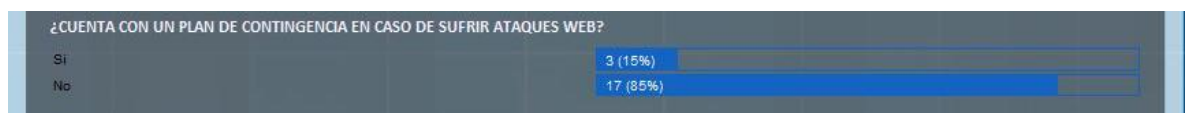
12.5. Pregunta 4



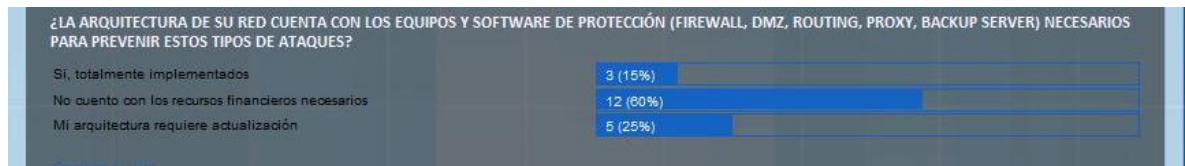
12.6. Pregunta 5



12.7. Pregunta 6



12.8. Pregunta 7



12.9. Pregunta 8

