UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA SOLUCION DE SEGURIDAD DE LA INFORMACIÓN PARA LAS REDES DE UNA EMPRESA QUE CURSA INFORMACIÓN CRÍTICA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

HENRY ALEXANDER GÓMEZ CHIROQUE

PROMOCIÓN
2004 - I

LIMA – PERÚ
2009

DISEÑO DE UNA SOLUCIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LAS REDES DE UNA EMPRESA QUE CURSA INFORMACIÓN CRÍTICA

DEDICATORIA

Dedico este informe a mis seres queridos, en reconocimiento y gratitud al amor que me brindan, que es siempre una motivación para ser cada vez mejor.

SUMARIO

En el presente trabajo se exponen los riesgos y amenazas que atentan contra la información de una organización, considerando a la información como un "activo" muy valioso para las organizaciones. Asimismo se expondrá las tecnologías y plataformas existentes en el mercado de la seguridad de la información para mitigar y minimizar esos riesgos y amenazas, la manera de operarlos e integrarlos a las redes y sistemas de una organización que desee preservar su información.

INDICE

PRÓLOGO

El presente trabajo tiene como propósito exponer las distintas amenazas a la seguridad de la información que tienen las redes de las empresas, y a su vez mostrar como afrontarlas de manera que estas amenazas no afecten la integridad, confidencialidad y disponibilidad de la información de las empresas, información que constituye un valioso activo para las empresas.

Dependiendo de cuanto las empresas valoran la información que cursan por sus redes y de cuanto estén ellas dispuestas a invertir en seguridad de la información, las medidas tomadas para proteger sus redes pueden ser cada vez más complejas.

A fin de mostrar como proteger las redes de una compañía frente a amenazas de seguridad que podrían comprometer la información de la empresa, se diseñará una solución perimetral integral de seguridad de la información para las redes de una empresa que cursa, a su consideración, información crítica.

La solución contempla control de accesos a la red, protección contra accesos indebidos, control de navegación en Internet de los usuarios, filtro de contenidos Web, detección de correos no deseados y antivirus para el correo corporativo, acceso remoto seguro desde Internet para conectarse a la red de la empresa, y protección contra intrusos.

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA DE INGENIERÍA

1.1 Necesidades informáticas de una organización

Las organizaciones actualmente requieren de múltiples tecnologías de la información y comunicaciones sobre los que se puedan montar sus sistemas de información.
Sobre estos sistemas de información se ingresa, modifica y procesa toda la información de la actividad empresarial de dicha organización.

Mencionemos algunas necesidades concretas de las organizaciones actualmente:

- Interconexión entre las computadoras de los empleados ubicados en un mismo edificio a fin de compartir e intercambiar información.
- Acceso inalámbrico controlado, a la red de la empresa.
- Interconexión entre los computadores de todos los locales de la empresa.
- Servidores que puedan manejar los sistemas de información de la empresa.
- Conectividad de los computadores de los usuarios hacia los servidores de las empresas que manejan aplicaciones internas (bases de datos, ERP, fileserver, etc.).
- Alta disponibilidad de los sistemas de información de la organización (conectividad, servidores, aplicaciones, etc.).
- Publicación páginas Web y aplicaciones online para el negocio de la empresa.
- Navegación controlada de usuarios por Internet.
- Correo corporativo para todos los trabajadores, que este libre de SPAM.
- Centralización de servidores en un site principal, teniendo su contingencia en un site secundario.
- Acceso remoto y seguro (vía Internet) a la red de la organización, para interactuar con los sistemas internos y/o brindar soporte a las plataformas desplegadas.
- Administración continua de todos los elementos que conforman el sistema de información.

Según observamos las organizaciones dependen fuertemente de los sistemas informáticos para llevar a cabo sus actividades diarias, por ende éstas requieren que sus sistemas de información se encuentren siempre disponibles e íntegros.

=> Se requiere calidad, continuidad, ¡sistemas de información seguros!

1.2 Amenazas de red

Actualmente se tienen múltiples amenazas informáticas que atentan contra los sistemas de información de las organizaciones, podemos mencionar como amenazas lo siguiente: la caída de las comunicaciones dentro de la organización, baja performance de las redes, y una serie de malware (código malicioso) tales como viruses, worms, trojans, spyware, amenazas blindadas, bots y ataques de cyber terroristas, spear phishing, root kits, stealth y ataques orientados, así como envío de SPAM que consume recursos del sistema, además de emplear tiempo del personal en revisar esos correos.
Todas estas amenazas pueden tener impacto en la red

Adicional a estas amenazas informáticas, se tiene la manipulación indebida de personas autorizadas y/o no autorizadas de información a la cual ellos puedan acceder.
A continuación se aprecia en la Fig.1.1 un estadístico de amenazas de red que se presentaron de enero a octubre de 2007:

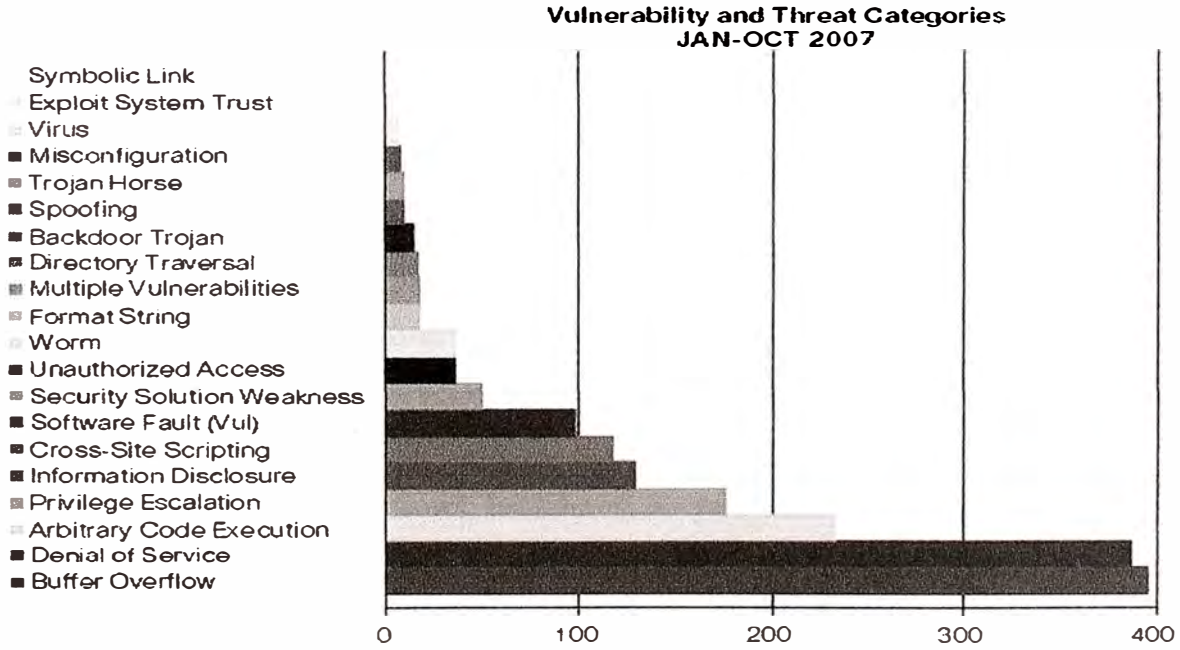
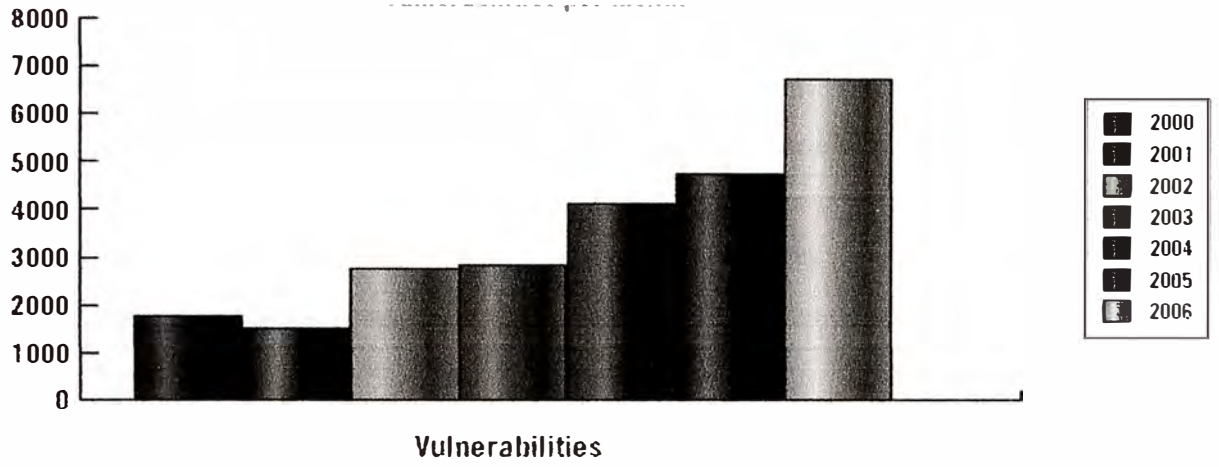


Fig.1.1 Reporte de amenazas de enero a octubre de 2007. Fuente Cisco.

Las AMENZAS explotan las VULNERABILIDADES que puedan existir en el sistema.

1.2.1 Vulnerabilidades

Podemos apreciar que las vulnerabilidades en los sistemas de información se han ido incrementado a lo largo de los años según no muestra la Fig.1.2.



Year	Vulnerabilities	Avg per month	Avg per week	% increase year over year
2000	2007	167	39	
2001	1918	160	37	-4.4%
2002	3210	268	62	67.4%
2003	3156	263	61	-1.7%
2004	4606	384	89	45.9%
2005	5195	433	100	12.8%
2006	7247	604	139	39.5%

Fig.1.2 Reporte de evolución de vulnerabilidades. Fuente IBM-ISS.

Estas vulnerabilidades han sido clasificadas en 3 niveles, dependiendo del posible impacto en una víctima potencial, de la manera siguiente:

- **Alta (high)**: Relacionado a asuntos de seguridad que permiten acceso remoto o local inmediato, o ejecución inmediata de código de línea sin tener privilegios autorizados.

  Ejemplos: Buffer overflows, backdoors, no passwords, pasar por alto el firewalls u otro componente de red.
- **Media (Medium)**: Relacionado a asuntos de seguridad que tienen el potencial de ganar acceso o permitir la ejecución de código vía complejos o largos

procedimientos de "exploits", o problemas de bajo riesgo aplicados a la mayoría de componentes de Internet.

Ejemplos: Cross-site scripting, man-in-the-middle attacks, SQL injection, denegación de servicio de aplicaciones importantes, y denegación de servicio resultante en sistemas de descubrimiento de información.

- **Baja (Low)**: Asuntos de seguridad que deniegan servicio o proveen información; no del sistema, que podría ser usada para formular ataques estructurados sobre un destino, pero no directamente ganan acceso sin autorización.

  Ejemplos: Ataques de fuerza bruta, información no del sistema descubierta (configuraciones, rutas, etc.) y ataques de denegación de servicio.

La Fig.1.3 ilustra esta clasificación.

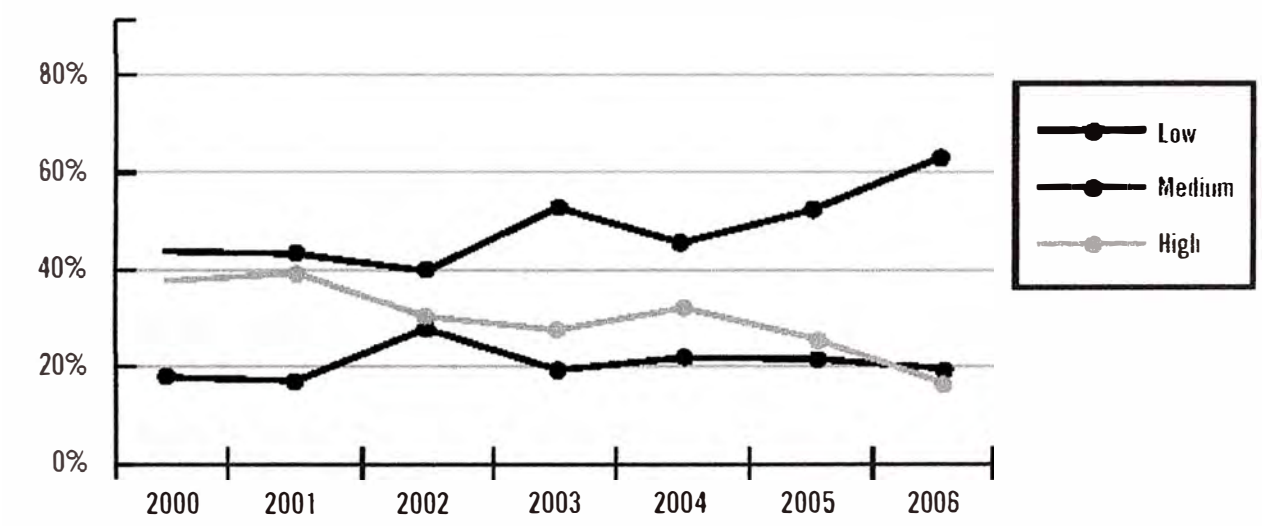


Fig.1.3 Clasificación de vulnerabilidades por año. Fuente IBM-ISS.

Es importante señalar que los criterios para la obtención de estadísticas de vulnerabilidades descubiertas pueden variar dependiendo de la fuente de donde son obtenidas.

Actualmente en el mercado existen diversas compañías en la creciente industria de la seguridad de la información, la cual se asentado con mayor fuerza en los últimos años.

De manera similar a la información previa, la Fig.1.4 nos muestra otra estadística de la evolución de vulnerabilidades en los sistemas de información en los últimos años.

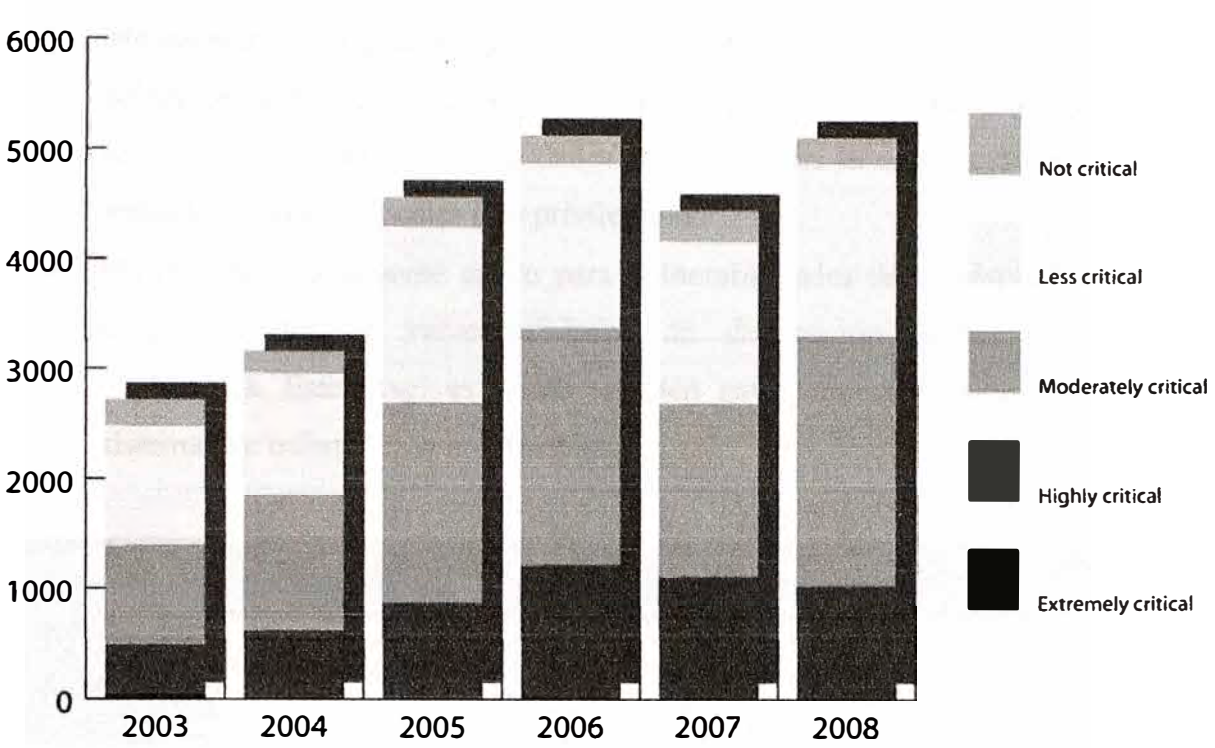


Fig.1.4 Evolución de vulnerabilidades por año. Fuente Secunia.

Esta vez, las vulnerabilidades han sido clasificadas en 5 niveles de criticidad, tal como se muestra en la figura 1.5. Esto en base al siguiente criterio:

- **Extremadamente crítica**: Este nivel es típicamente usado para vulnerabilidades remotamente explotables, que pueden llevar a comprometer el sistema. El éxito de la explotación de la vulnerabilidad no requiere interacción alguna normalmente, y la vulnerabilidad ya está siendo activamente explotada (o los "exploits" están disponibles públicamente).
- **Altamente crítica**: Este nivel es típicamente usado para vulnerabilidades remotamente explotables, que pueden llevar a comprometer el sistema. El éxito de la explotación de la vulnerabilidad no requiere interacción alguna normalmente, pero no hay "exploits" conocidos disponibles en el momento de su divulgación.
- **Moderadamente crítico**: Típicamente usado para vulnerabilidades de denegación de servicio (DoS) remotamente explotables y para vulnerabilidades que permiten comprometer al sistema pero que requieran interacción con el usuario. También usado para vulnerabilidades que permiten comprometer al sistema sobre redes de área local en servicios como SMB, RPC, NFS, LPD, y servicios similares que no se pretende sean usados en Internet.

- **Menos críticos**: Típicamente usado para vulnerabilidades de "cross-site scripting" y vulnerabilidades de escalación de privilegios. Esta clasificación es también acostumbrada para vulnerabilidades que permiten la exposición de información sensible a usuarios locales (sin privilegios).
- **No crítico**: Típicamente usado para vulnerabilidades de escalación de privilegios muy limitados, y vulnerabilidades de denegación de servicio localmente explotables. Este nivel es usado también para vulnerabilidades divulgadas para sistemas de información no sensibles.

Criticality	2003	2004	2005	2006	2007	2008
Extremely critical	55	15	20	24	2	11
Highly critical	438	606	851	1,191	1,149	1,019
Moderately critical	893	1,229	1,817	2,152	1,675	2,275
Less critical	1,093	1,108	1,607	1,511	1,562	1,576
Not critical	237	198	270	250	290	233

Fig.1.5 Clasificación de vulnerabilidades por año. Fuente Secunia.

Según se aprecia en la Fig.1.5 las vulnerabilidades altamente críticas han disminuido, y se ha dado un incremento considerable en las moderadamente críticas al 2008. Esto indica que las vulnerabilidades

1.2.2 Vulnerabilidades "0-day"

Una vulnerabilidad 0-day es aquella que ha sido explotada (aprovechada) en el "mundo salvaje" antes de la divulgación pública de detalles técnicos o parches sobre esta.

Estas vulnerabilidades son de una preocupación particular, porque nadie posee una manera efectiva de protección contra la explotación de esta y por ende todo aquel que opere el software afectado es una víctima potencial.

Las buenas noticias son que este tipo de vulnerabilidades ha decrecido en el 2008, de 20 en el 2007 a 12 reportadas en el 2008.

Según no muestra la Fig.1.6, como en años anteriores, el objetivo primario para los criminales que buscaban estas vulnerabilidades fue software de Microsoft. Un total de 9 vulnerabilidades 0-day afectaron software de Microsoft en el 2008, y las 3 vulnerabilidades restantes afectaron ActiveX (por tanto, el vector fue aun el software de Microsoft).

Este número relativamente bajo de "0-day" indica que un procedimiento de manejo de parches eficiente es capaz de mantener a la mayoría de malos muchachos fuera de nuestra red, desde que relativamente pocos atacantes son realmente conducidos a utilizar "0-day".

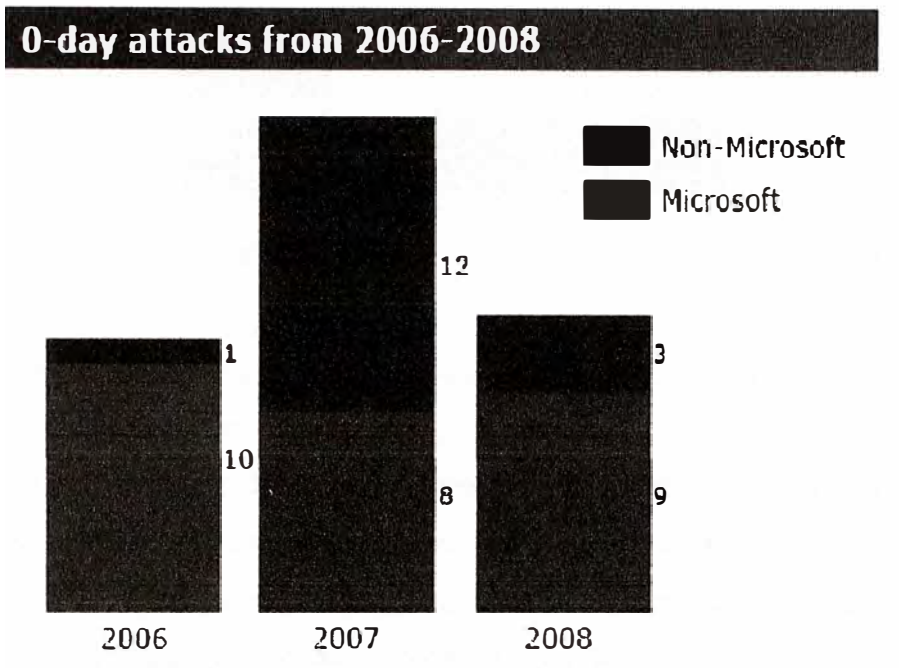


Fig.1.6 Evolución de vulnerabilidades "0-day". Fuente Secunia.

1.2.3 Vulnerabilidades de navegadores web

Siendo el navegador web el mayor contacto entre un usuario de computador y el Internet, es muy importante considerar las vulnerabilidades que se puedan presentar debido a huecos de seguridad en los navegadores web, que son la principal puerta de acceso al Internet.
En el 2008 31 vulnerabilidades fueron reportadas vinculadas al Internet Exploreer (IE 5.x,6.x, y 7), incluyendo aquellas públicamente dejadas al descubierto antes del parche del proveedor como aquellas incluidas en los boletines de seguridad de Microsoft.
En cuanto a los navegadores Safari y Operar cada uno tuvo 32 y 30 vulnerabilidades respectivamente, mientras que 115 vulnerabilidades fueron registradas para Firefox en el 2008.

La Fig.1.7 presenta una revisión de las vulnerabilidades pertenecientes a 4 de los más populares navegadores usados.

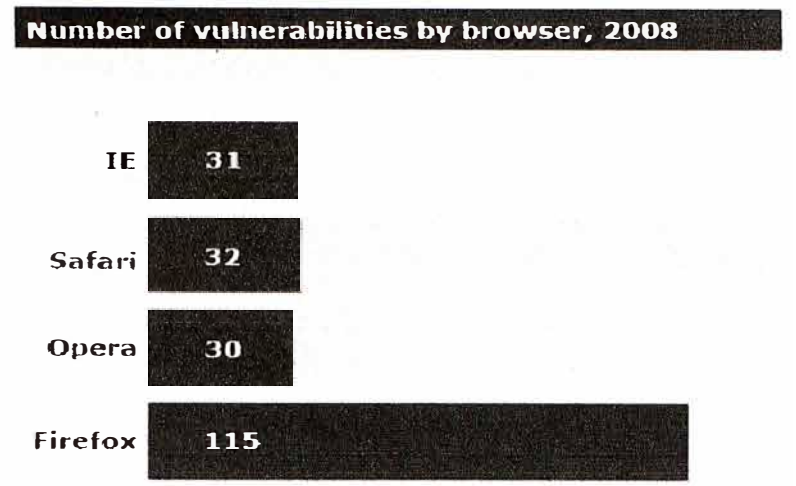


Fig.1.7 Número de vulnerabilidades de los 4 navegadores más populares. Fuente Secunia

No debemos dejar de mencionar a los "Plug-ins", ampliamente utilizados para proveer de cierta función específica a los navegadores bajo demanda.
En cuanto a plug-ins de navegadores, el número de vulnerabilidades en controles ActiveX en el 2008 sigue siendo de lejos el más significativo, llegando a 366.
Los controles ActiveX han siempre sido populares en términos de uso y abuso. Sin embargo, las vulnerabilidades registradas tuvieron un gran salto del 2006; con 45, al 2007 llegando a 339 vulnerabilidades, esto aparentemente se incrementó por eventos tales como "el mes de los controles ActiveX", en mayo de 2007, cuando se presentaron múltiples vulnerabilidades. Otro evento fue el descubrimiento por Secunia, de un componente de ActiveX vulnerable que fue utilizado en unos 40 productos diferentes.

Las noticias del 2008 es que el número de vulnerabilidades ha sido inclusive más alto, posiblemente indicando que los controles están siendo cada vez más atacados por cybercriminales. Sin embargo esto podría también ser un indicio que más vulnerabilidades ActiveX están siendo encontradas usando herramientas de scanning.

La Fig.1.8 contiene un resumen del número de diferentes tipos de componentes de navegadores; plug-ins, que tuvieron vulnerabilidades el 2008.
Mientras los controles ActiveX, widgets, y extensiones Firefox pueden ser desarrolladas para apenas algunas funcionalidades add-on para un navegador, los plug-ins para Java, Flash, y Quicktime plugins son desarrollados y mantenidos por sus respectivos proveedores.

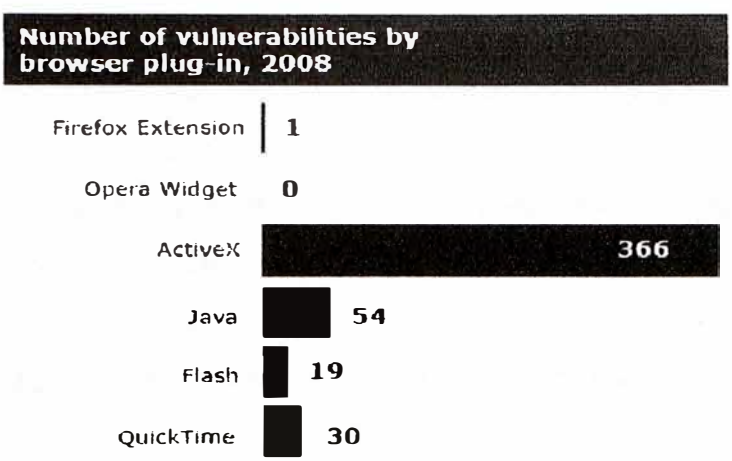


Fig.1.8 Número de vulnerabilidades por plug-in de navegadores. Fuente Secunia.

Ventana de exposición

Es el tiempo en el cual una vulnerabilidad ha sido puesta en descubierta públicamente, y puede ser explotable por alguien. La ventana de exposición de amenazas concernientes a Internet Explorer y Firefox son comparadas en la Fig.1.9. Esta tabla solamente muestra aquellas vulnerabilidades divulgadas públicamente por un reporte antes de la notificación del proveedor. Estos números no incluyen las vulnerabilidades las vulnerabilidades dadas a conocer responsablemente o descubiertas internamente por el vendedor. Mozilla ha desarrollado parches para 3 de los 3 avisos relacionados a Firefox, que son todos concernientes a vulnerabilidades de bajo riesgo.

Microsoft ha desarrollado parches para 3 de los 6 avisos relacionados a Internet Explorer, aunque con varias amenazas serias sin parche por hasta tanto como 110 días después de su divulgación. Tres amenazas de bajo riesgo de Internet Explorer no han sido parchadas durante todo el 2008 ("unpatched").

Secunia Advisory ID for disclosed vulnerabilities	Criticality	Disclosure date	Patching date	Number of days before patch release
Internet Explorer				
SA30857	Moderate	2008-06-26	2008-10-14	110
SA30851	High	2008-06-26	2008-10-14	110
SA30145	Not critical	2008-05-12	Unpatched	233
SA30141	Less critical	2008-05-14	Unpatched	231
SA29453	Less critical	2008-03-24	2008-06-10	78
SA29346	Less critical	2008-03-12	Unpatched	294
Mozilla Firefox				
SA32192	Not critical	2008-10-14	2008-13-11	30
SA32040	Not critical	2008-10-01	2008-12-26	86
SA28622	Less critical	2008-01-24	2008-02-08	15

Fig.1.9 Ventana de explotación de vulnerabilidades públicamente expuestas. F. Secunia.

1.2.4 Vulnerabilidades en páginas web

Las páginas web son las aplicaciones que más abundan en el ciberespacio. Actualmente para toda organización es ya una necesidad tener un portal web que brinde información acerca de la misma, así como para realizar diversas operaciones y transacciones vinculadas a su proceso productivo, servicios, ventas, etc. Pero estas páginas web publicadas en Internet son de libre acceso a todo el mundo, y de no estar sin vulnerabilidades, está latente la amenaza de un ataque que aproveche la vulnerabilidad presente.

A continuación se mostrará el análisis de vulnerabilidades efectuado a 32717 páginas web encontrándose un total de 69476 vulnerabilidades de diferentes grados de severidad. Estudio realizado por el Consorcio de Seguridad de Aplicaciones Web, "Web Application Security Consortium".

Para este análisis se realizó 2 tipos de obtención de resultados:

a) Resultados de pruebas automatizado: consistente en escaneos a los sitios web sin ningún tipo de personalización en la herramienta de escaneo, es decir con un perfil por defecto. Una adicional personalización por un experto en la herramienta de escaneo mejoraría la efectividad de detección de vulnerabilidades automatizadas.
b) Black box & White box: Contiene estadísticas de resultados obtenidos de manera automática y manual. El análisis incluye escaneo con configuraciones (perfil) preliminares seguido por un análisis manual, investigación manual de vulnerabilidades que no puede ser detectado por herramientas de escaneo de manera automática, y análisis de código fuente.
Por lo tanto tendremos 3 datos estadísticos, el caso "a", caso "b" y la estadística global.

El análisis de la Fig.1.10 nos indica que más del 7% de los sitios web analizados pueden ser comprometidos automáticamente. Alrededor del 7.72% de las aplicaciones tuvieron una vulnerabilidad de alta severidad detectada durante el escaneo automático. Mientras que una evaluación detallada manual y automática usando los métodos Black box & White box muestra que la probabilidad para detectar vulnerabilidades de alta severidad alcanza el 96.85%. Así que escaneos automáticos representan información para un promedio de sitios de Internet y los resultados de los métodos Black box & White box hacen referencia a aplicaciones web corporativas interactivas.

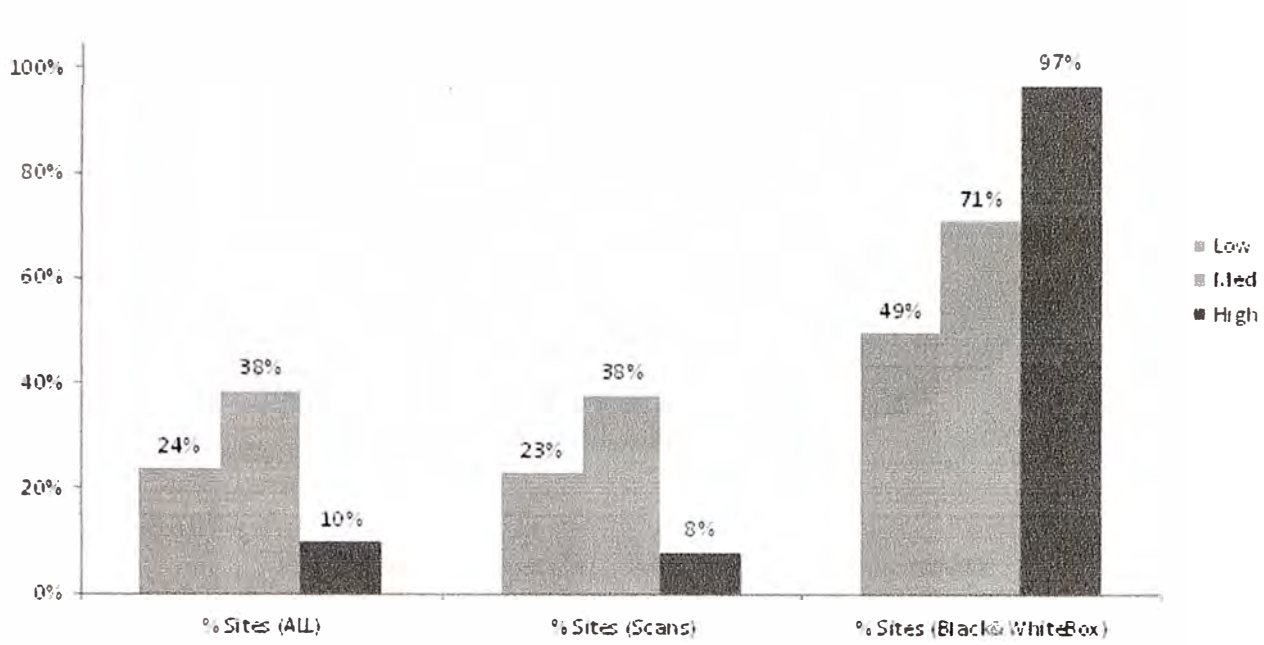


Fig.1.10 Probabilidad para encontrar vulnerabilidades de diferente nivel de riesgo.

Las vulnerabilidades más prevalentes encontradas (ver Fig.1.11 y Fig.1.12) son Cross-Site Scripting, Information Leakage, SQL Injection y Predictable Resource Location.

Como una regla, las vulnerabilidades Cross-Site Scripting y SQL Injection aparecen debido a errores de diseño en el sistema, mientras que Information Leakage y Predictable Resource Location están a menudo vinculadas con una administración del sistema impropia (por ejemplo, debilidades de control de acceso)

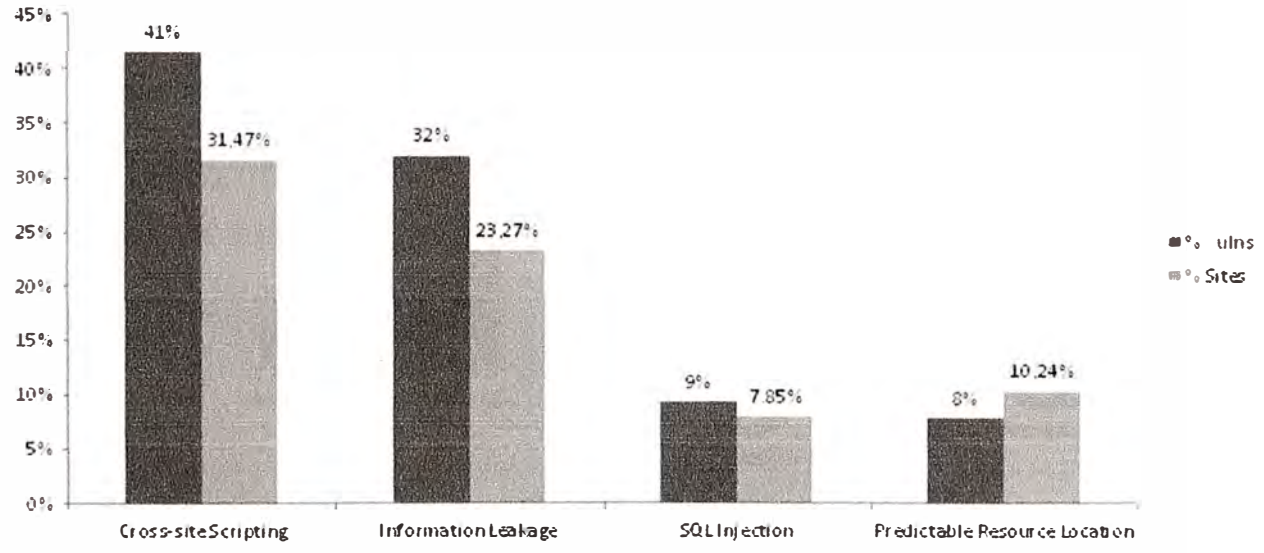


Fig.1.11 Las vulnerabilidades web más encontradas.

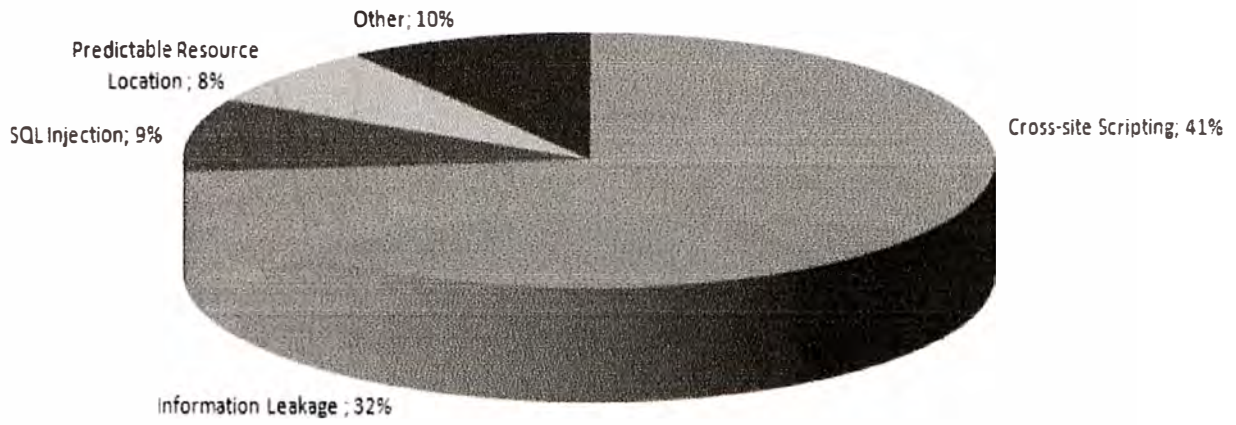


Fig.1.12 Las vulnerabilidades web más encontradas.

Mientras en el análisis de sistemas con los métodos Black & White box, como se muestra en la Fig.1.13 y Fig.1.14, muestran que un apreciable porcentaje de sitios web son vulnerables a Content Spoofing, autorización insuficiente y autenticación insuficiente.
Con ésta evaluación se alcanza una probabilidad de detectar SQL Injection de 25%.

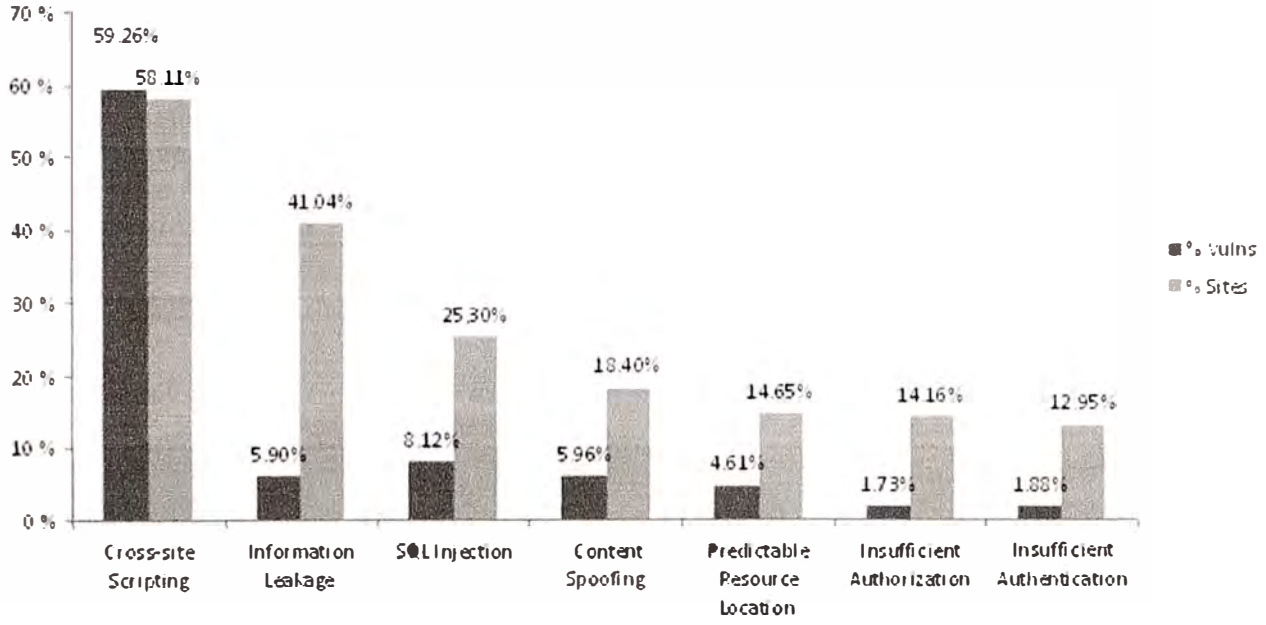


Fig.1.13 Vulnerabilidades web más encontradas (método Black&White box)

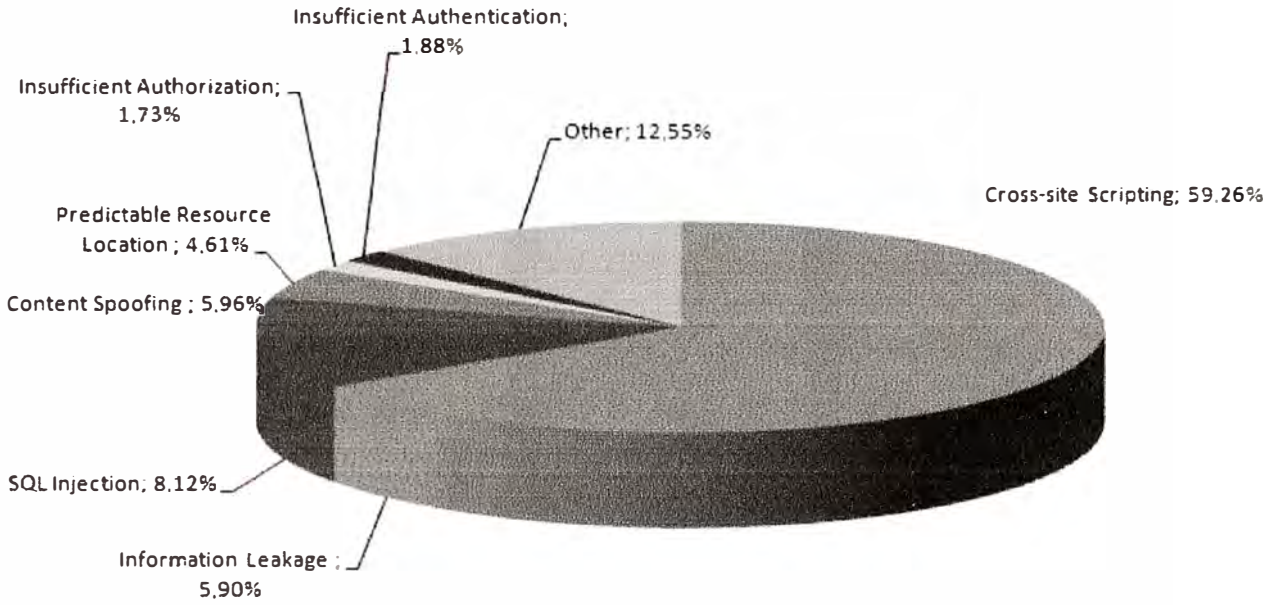


Fig.1.14 Vulnerabilidades web más encontradas (método Black&White box)

En términos del Consorcio de Seguridad de Aplicaciones Web (WASC), las más predominantes clases de vulnerabilidad son Client-side Attacks, Information Disclosure (divulgación de información) y Command Execution (Ejecución de comandos). El análisis detallado muestra la popularidad de las clases Autenticación y Autorización. Ver Tabla 1.1 y Fig. 1.15. y 1.16.

Tabla.1.1 Distribución de la probabilidad de detección de vulnerabilidades según WASC.

	% ALL	% Scans	% Black & WhiteBox
Authentication	1.17%	0.02%	20.82%
Authorization	1.28%	0.07%	19.01%
Client-side Attacks	33.13%	31.17%	69.37%
Command Execution	8.15%	7.32%	27.85%
Information Disclosure	31.78%	30.42%	56.54%
Logical Attacks	0.90%	0.20%	13.92%

Fig.1.15 Distribución de la probabilidad de detección de vulnerabilidades según WASC

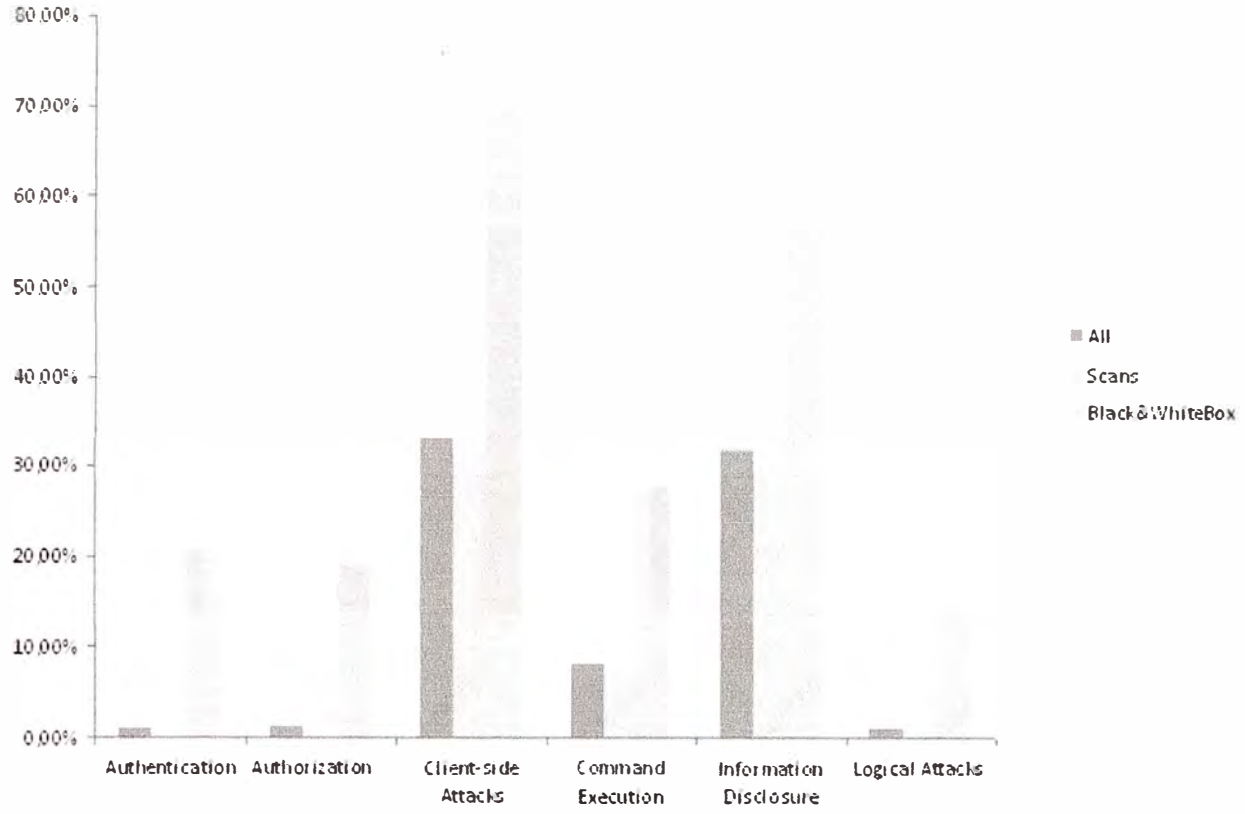


Fig.1.16 Distribución de la probabilidad de detección de vulnerabilidades según WASC

Si comparamos el método de escaneo automático con los métodos detallados Black & White box, es evidentemente claro que un análisis detallado es mucho más efectivo para detectar vulnerabilidades de la clase Autorización y Autenticación y defectos lógicos.
Ver Tabla 1.2 y Fig.1.17.

Tabla.1.2 Diferencia en la probabilidad de detección de vulnerabilidades

Threat Classification	Scans vs Black & WhiteBox
Content Spoofing	18.30%
Insufficient Authorization	14.15%
Insufficient Authentication	12.95%
SQL Injection	8.68%

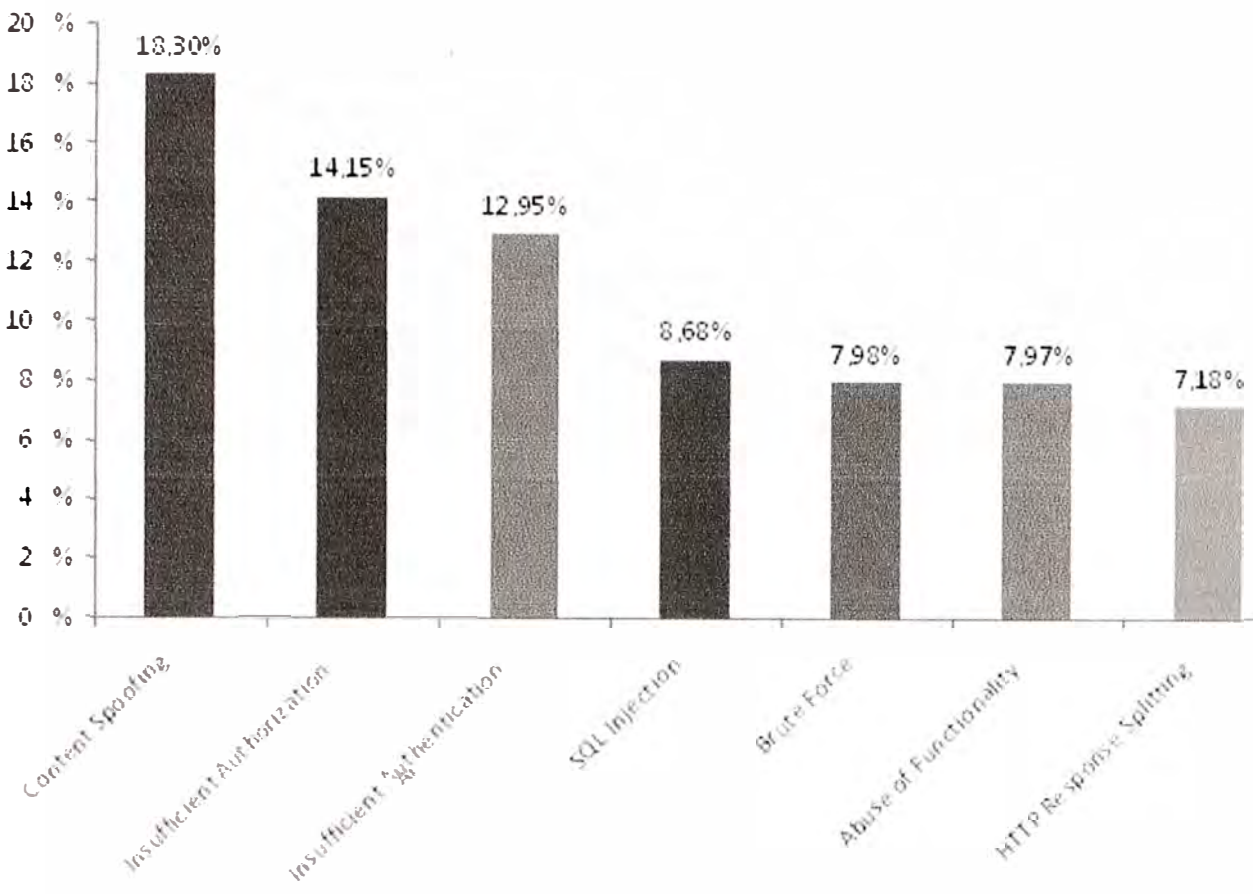


Fig.1.17 Diferencia en la probabilidad de detección de vulnerabilidades

La probabilidad para detectar vulnerabilidades de alto riesgo usando el análisis detallado (Black&White box) es 12.5 veces mayor que usando escaneos automatizados (Scans).

De acuerdo al número de vulnerabilidades detectadas para un sitio (Ver Tabla 1.3 y Fig.1.18), los análisis detallados permiten detectar en promedio 9 vulnerabilidades de alto riesgo por sitio, mientras que los escaneos automatizados permiten detectar solamente 2.3 vulnerabilidades de este rango.

Tabla.1.3 Número de vulnerabilidades por sitio web

	All	Scans	Black&WhiteBox
Low	3.15	2.96	1.11
Med	2.35	2.04	2.65
High	4.22	2.33	8.91
All	2.12	1.61	13.11

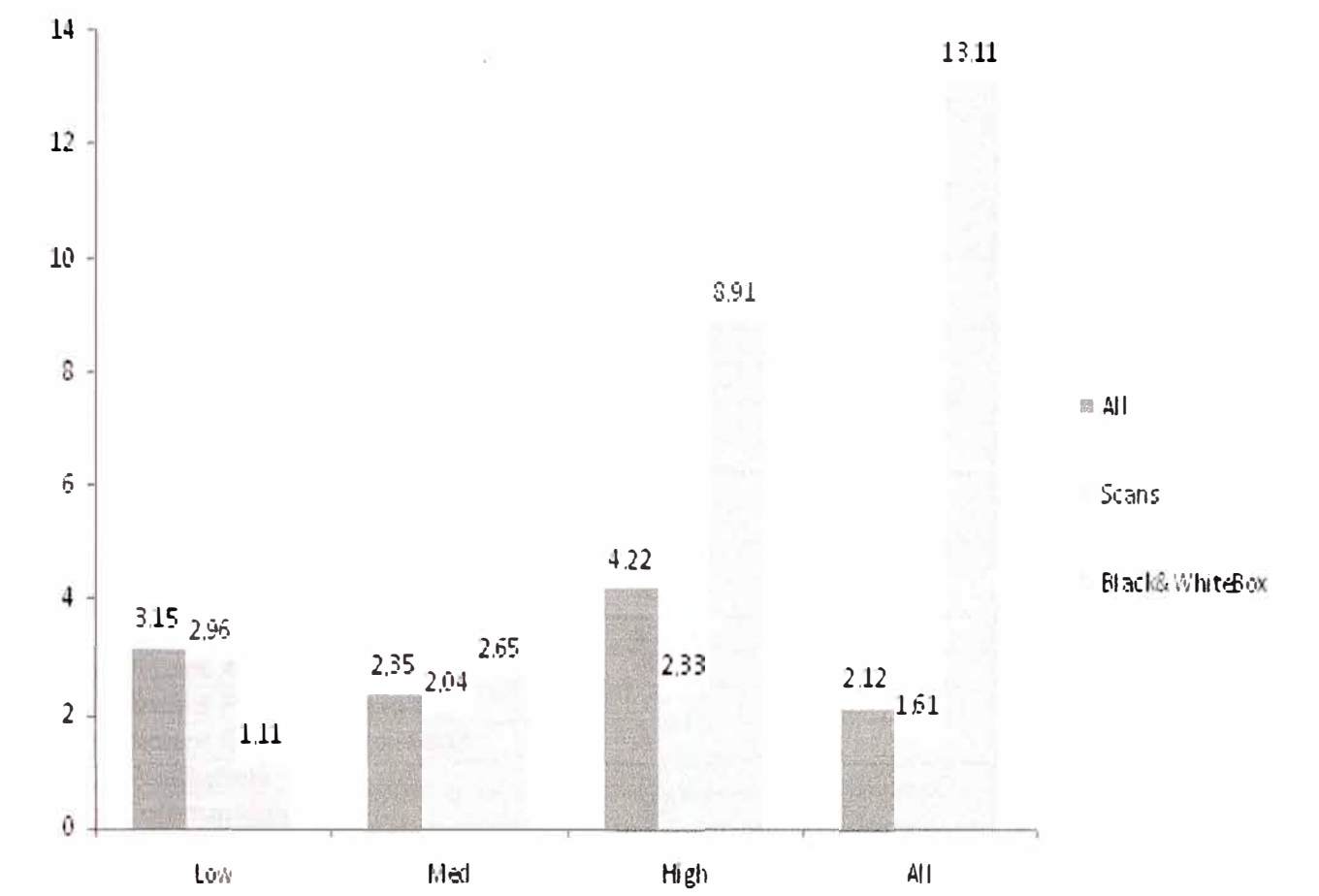


Fig.1.18 Número de vulnerabilidades por sitio web.

En estas estadísticas no se ha incluido vulnerabilidades cuya existencia depende de una plataforma, como por ejemplo, buffer overflow en Apache.

Resultados estadísticos

A continuación se presentaran los resultados estadísticos obtenidos mediante:
a) Escaneos automatizados

Las tablas 1.4, 1.5 y 1.6 nos muestran los resultados estadísticos obtenidos al haber escaneado de manera automatizada (con herramientas de scanning) un total de 31891 páginas web.

Tabla.1.4 Estadística general de escaneo automatizados

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	5	3	0.01%	0.01%
Brute Force	3	3	0.01%	0.01%
Buffer Overflow			0.00%	0.00%
Content Spoofing	33	21	0.06%	0.07%
Credential/Session Prediction	4	4	0.01%	0.01%
Cross-site request forgery	87	53	0.17%	0.17%
Cross-site Scripting	19171	9651	37.29%	30.26%
Denial of Service	30	22	0.06%	0.07%
Directory Indexing	91	12	0.18%	0.04%
Fingerprinting			0.00%	0.00%
Format String Attack			0.00%	0.00%
HTTP Response Splitting	182	161	0.35%	0.50%
Information Leakage	21157	7115	41.16%	22.31%
Insufficient Anti-automation	37	38	0.07%	0.12%
Insufficient Authentication	2	2	0.00%	0.01%
Insufficient Authorization	6	11	0.01%	0.03%
Insufficient Process Validation			0.00%	0.00%
Insufficient Session Expiration	3	3	0.01%	0.01%
LDAP Injection			0.00%	0.00%
OS Commanding	19	3	0.04%	0.01%
Path Traversal	118	116	0.23%	0.36%
Predictable Resource Location	4772	3213	9.28%	10.07%
Session Fixation	3	3	0.01%	0.01%
SQL Injection	5301	2298	10.31%	7.21%
SSI Injection	180	37	0.35%	0.12%
URL Redirectors	195	182	0.38%	0.57%
Weak Password Recovery Validation	1	1	0.00%	0.00%
WSDL Exposure			0.00%	0.00%
XPath Injection	4	1	0.01%	0.00%
Total	51404	31891		

Tabla.1.5 Distribución de vulnerabilidades por riesgo

Threat rank	N of Vulns	N of Sites	% Vulns	% Sites
Low	21736	7352	42.28%	23.05%
Med	24452	12012	47.57%	37.67%
High	5736	2463	11.16%	7.72%

Tabla.1.6 Distribución de vulnerabilidades por clasificación según el WASC

WASC Classes	N of Vulns	N of Sites	% of Vulns	% Sites
Authentication	6	6	0.01%	0.02%
Authorization	16	21	0.03%	0.07%
Client-side Attacks	19668	9941	38.26%	31.17%
Command Execution	5504	2336	10.71%	7.32%
Information Disclosure	26138	9701	50.85%	30.42%
Logical Attacks	72	63	0.14%	0.20%

b) Métodos Black & White box:

Las tablas 1.7, 1.8 y 1.9 nos muestran los resultados estadísticos obtenidos al haber evaluado de manera detallada (metodología Black & White box) un total de 826 páginas web.

Tabla.1.7 Estadística general de análisis Black&White box

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	114	66	1.05%	7.99%
Brute Force	148	66	1.37%	7.99%
Buffer Overflow	1	1	0.01%	0.12%
Content Spoofing	646	152	5.96%	18.40%
Credential/Session Prediction	25	10	0.23%	1.21%
Cross-site request forgery	74	13	0.68%	1.57%
Cross-site Scripting	6418	480	59.26%	58.11%
Denial of Service	25	22	0.23%	2.66%
Directory Indexing	60	39	0.55%	4.72%
Fingerprinting	80	51	0.74%	6.17%
Format String Attack	4	2	0.04%	0.24%
HTTP Response Splitting	447	64	4.13%	7.75%
Information Leakage	639	339	5.90%	41.04%
Insufficient Anti-automation	16	14	0.15%	1.69%
Insufficient Authentication	204	107	1.88%	12.95%
Insufficient Authorization	187	117	1.73%	14.16%
Insufficient Process Validation	77	18	0.71%	2.18%
Insufficient Session Expiration	17	16	0.16%	1.94%
LDAP Injection	1	1	0.01%	0.12%
OS Commanding	6	6	0.06%	0.73%
Path Traversal	60	29	0.55%	3.51%
Predictable Resource Location	499	121	4.61%	14.65%
Session Fixation	120	22	1.11%	2.66%
SQL Injection	879	209	8.12%	25.30%
SSI Injection	5	3	0.05%	0.36%
URL Redirectors	11	11	0.10%	1.33%
Weak Password Recovery Validation	13	10	0.12%	1.21%
WSDL Exposure	0	0	0.00%	0.00%
XPath Injection	55	15	0.51%	1.82%
Total	10831	826		

Tabla.1.8 Distribución de vulnerabilidades por riesgo

Threat rank	N of Vulns	N of Sites	% Vulns	% Sites
Low	452	408	4.17%	49.39%
Med	1549	584	14.30%	70.70%
High	7127	800	65.80%	96.85%

Tabla.1.9 Distribución de vulnerabilidades por clasificación según el WASC.

WASC Classes	N of Vulns	N of Sites	% of Vulns	WASC Classes
Authentication	365	172	3.37%	20.82%
Authorization	349	157	3.22%	19.01%
Client-side Attacks	7596	573	70.13%	69.37%
Command Execution	951	230	8.78%	27.85%
Information Disclosure	1338	467	12.35%	56.54%
Logical Attacks	232	115	2.14%	13.92%

c) Resultados globales:

Las tablas 1.10, 1.11 y 1.12 nos muestran los resultados estadísticos globales del estudio, obtenidos al haber evaluado un total de 32717 páginas web.

Tabla.1.10 Estadística general global

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	169	99	0.24%	0.30%
Brute Force	291	125	0.42%	0.38%
Buffer Overflow	171	19	0.25%	0.06%
Content Spoofing	1399	213	2.01%	0.65%
Credential/Session Prediction	79	46	0.11%	0.14%
Cross-site request forgery	993	126	1.43%	0.39%
Cross-site Scripting	28769	10297	41.41%	31.47%
Denial of Service	55	44	0.08%	0.13%
Directory Indexing	281	87	0.40%	0.27%
Fingerprinting	120	60	0.17%	0.18%
Format String Attack	104	12	0.15%	0.04%
HTTP Response Splitting	749	265	1.08%	0.81%
Information Leakage	22156	7614	31.89%	23.27%
Insufficient Anti-automation	288	115	0.41%	0.35%
Insufficient Authentication	356	229	0.51%	0.70%
Insufficient Authorization	343	218	0.49%	0.67%
Insufficient Process Validation	117	38	0.17%	0.12%
Insufficient Session Expiration	200	91	0.29%	0.28%
LDAP Injection	21	11	0.03%	0.03%
OS Commanding	25	9	0.04%	0.03%
Path Traversal	178	145	0.26%	0.44%
Predictable Resource Location	5331	3349	7.67%	10.24%
Session Fixation	183	65	0.26%	0.20%
SQL Injection	6420	2567	9.24%	7.85%
SSI Injection	185	40	0.27%	0.12%
URL Redirectors	210	195	0.30%	0.60%
Weak Password Recovery Validation	164	31	0.24%	0.09%
WSDL Exposure	60	20	0.09%	0.06%
XPath Injection	59	16	0.08%	0.05%
Total	69476	32717		

Tabla.1.11 Distribución de vulnerabilidades por riesgo

Threat rank	N of Vulns	N of Sites	% Vulns	% Sites
Low	24433	7760	35.17%	23.72%
Med	29575	12596	42.57%	38.50%
High	13765	3263	19.81%	9.97%

Tabla.1.12 Distribución de vulnerabilidades por clasificación según el WASC.

WASC Classes	N of Vulns	N of Sites	% of Vulns	% Sites
Authentication	811	384	1.17%	1.17%
Authorization	805	418	1.16%	1.28%
Client-side Attacks	32120	10840	46.23%	33.13%
Command Execution	6985	2665	10.05%	8.15%
Information Disclosure	28126	10398	40.48%	31.78%
Logical Attacks	629	295	0.91%	0.90%

1.2.5 Desactualización en software y parches

A la par que se encuentran vulnerabilidades en las aplicaciones, sistemas operativos, y software de toda índole, los proveedores continuamente están desarrollando nuevas versiones de software o parches para su software. Diseñados para mejorar el software en cuanto a calidad y uso, solucionando problemas de desperfectos.

Los parches de seguridad son cambios aplicados a un activo para corregir alguna debilidad descrita por una vulnerabilidad en el software. Esta acción correctiva va a prevenir una explotación exitosa y remueve o mitiga la capacidad de una amenaza para explotar una vulnerabilidad específica en un activo. Los parches de seguridad constituyen el método primario para arreglar vulnerabilidades de seguridad en el software. Actualmente Microsoft desarrolla sus parches de seguridad una vez por mes, y en el caso de otros sistemas operativos o proyectos de software tienen equipos de seguridad dedicados a desarrollar los parches de software más confiables tan pronto después que se haya anunciado una posible vulnerabilidad.

Habiéndose mencionado la importancia de las actualizaciones en el software, cabe mencionar que no es muy común que los usuarios mantengan actualizados todos los aplicativos que poseen por diversas razones, por lo que estarán expuestos a vulnerabilidades que son superadas con los últimos parches o actualización de versión de software.

La Fig.1.19 nos muestra información acerca del porcentaje de instalaciones no parchadas de varias aplicaciones populares, información obtenida del último scanning de los usuarios

que poseen la herramienta PSI (Personal Software Inspector) de la empresa Secunia en el 2008.

Software	Number of Installations,	percent
Sun Java JRE 1.6.x/6.x	1,771,802	48%
Adobe Flash Player 9.x	1,462,284	48%
Sun Java JRE 1.5.x/5.x	502,859	96%
Adobe Reader 8.x	410,786	24%
Apple Quicktime 7.x	381,088	38%
Macromedia Flash Player 6.x	368,775	83%
WinRAR 3.x	348,108	38%
Mozilla Firefox 2.0.x	346,614	34%
7-Zip 4.x	295,312	26%
Java Web Start 5.x	250,453	66%

Fig.1.19 Top ten de la mayoría de aplicaciones detectadas sin actualizar durante el 2008.

Es importante recalcar, que esta estadística fue tomada de personas que mostraron interés en mantener su software actualizado y por ello se sometieron a este escaneo. Es de esperar que estas estadísticas sean peores para aquellos que no se someten a este escaneo.

Los números mostrados en la Fig.1.19 muestran un positivo desarrollo, pero ellos también claramente muestran que demasiados usuarios dejan de lado parchar su software cuando la actualización no se da de manera fácil y directa.

Muchos escogen manejar las aplicaciones que son fáciles de parchar, mientras que las aplicaciones que toman mucho tiempo o que son difíciles de parchar son simplemente ignoradas. Cifras como 83% de inseguridad para Flash Player 6.x y 96% para instalaciones Sun Java JRE claramente indica esto.

Los usuarios han sido generalmente bastante voluntariosos para parchar Adobe Reader 8.x; solamente 24% de estas instalaciones son inseguras.

Comparando esto con las cifras para Internet Explorer 7, Microsoft .NET Framework 2.x, y otros parches de Windows agrupados bajo Windows XP Professional, claramente muestra que mientras sea más fácil parchar, más gente realmente terminará haciéndolo, y esto inclusive es válido para gente con relativa conciencia de seguridad.

No obstante, inclusive Microsoft ha tenido problemas en conseguir que los usuarios parchen su software. Algo del 44% de todas las instalaciones de Word 2003 son vulnerables y la razón es obvia. La herramienta de actualización de Microsoft, "Windows

Update" solamente cubre ciertos productos. Para un mejor alcance los usuarios necesitan instalar Microsoft Update.

A continuación se mostrará una segunda estadística sobre actualización de software, que a diferencia del reporte anterior donde solo se considera el resultado del último scanning en los usuarios, aquí se considera todos los resultados de los escaneos hechos a los usuarios desde el primero. Por lo tanto, las cifras obtenidas nos dicen algo acerca del tiempo que toma a los usuarios parchar una aplicación.
En la Fig.1.20, por lo general, podemos decir que a mayor porcentaje, es mayor el tiempo antes que los usuarios realmente parchen. Otra vez, queda claro que los productos Microsoft son parchados muy frecuentemente, solo el 7% de todos los escaneos encontraron instalaciones de Internet Explorer sin parchar y solo en el 1% se encontró Windows Media Player sin parchar.

La diferencia significante puede ser explicada por el hecho que más parches Microsoft incluyeron parches para Internet Explorer que para Windows Media Player.

Software	Number of Installations,	percent insecure
Sun Java JRE 1.6.x/6.x	2,831,001	38%
Adobe Flash Player 9.x	2,389,661	34%
Adobe Reader 8.x	1,836,982	8%
Apple QuickTime 7.x	1,205,226	27%
Mozilla Firefox 2.0.x	544,384	14%
Sun Java JRE 1.5.x/5.x	473,783	97%
Mozilla Firefox 3.0.x	400,721	10%
Macromedia Flash Player 6.x	383,884	81%
iTunes 7.x	357,439	5%
Adobe Reader 7.x	297,827	15%

Fig.1.20 Top ten de la mayoría de aplicaciones detectadas sin actualizar, acumulado.

Aparentemente el software de estos proveedores es demasiado duro de parchar, haciendo que los usuarios se den por vencidos en cuanto a actualizar, por lo que los proveedores tienen trabajo por hacer.

1.2.6 Otras amenazas

Se tienen las conocidas amenazas que atentan contra la seguridad de la información como son los virus, gusanos, troyanos, y todo malware que en algunos casos aprovechan vulnerabilidades en los sistemas.

Otro problema en el Internet es el constante envío de SPAM, o correo electrónico no deseado de manera multitudinal, este envío consume recursos de las redes de manera indeseada. Un alto porcentaje de la información que se cursa por Internet corresponde a tráfico de SPAM. Además de consumir procesamiento de cpu, memoria, etc. en los servidores y computadores personales en las empresas, así como tiempo (horas hombre) de los empleados dedicado a revisar estos correos. La Fig.1.21 nos muestras la procedencia del SPAM a nivel mundial.

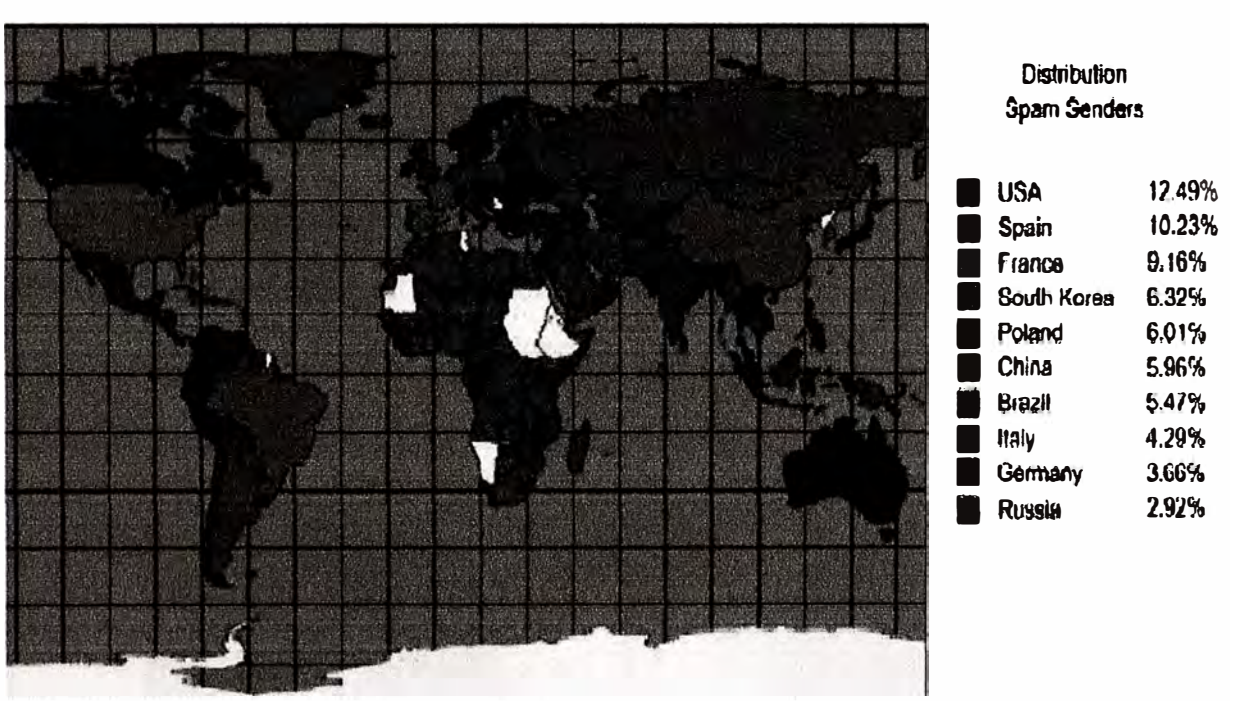


Fig.1.21 Fuentes de SPAM a nivel mundial.

Otro problema en la web es el phishing, en donde aparecen páginas web muy similares y de nombres de dominio también muy similares, que son difundidas generalmente como link dentro de un correo electrónico masivo (SPAM usualmente), para que el usuario al ingresar a esta web que se hace pasar por otra (por ejemplo la del banco de la persona) ingrese información personal, como lo son cuentas de bancos, de correos, etc.

A continuación se mostrarán reportes obtenidos por el Anti-Phishing Working Group correspondientes al segundo semestre del año 2008. En la la Fig.1.22 se muestra un reporte de los casos de Phishing detectados.

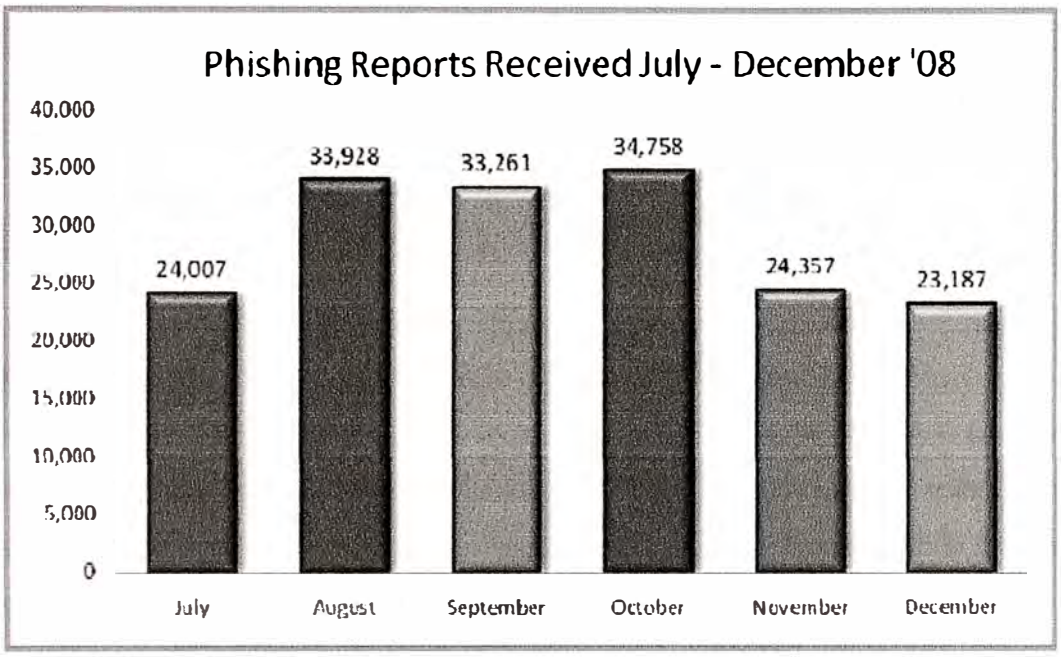


Fig.1.22 Reportes de phishing.

El sector más afectado es el financiero, como se puede apreciar en la Fig.1.23. que nos muestra la estadística de los sectores afectados en los 2 últimos trimestres del 2008.

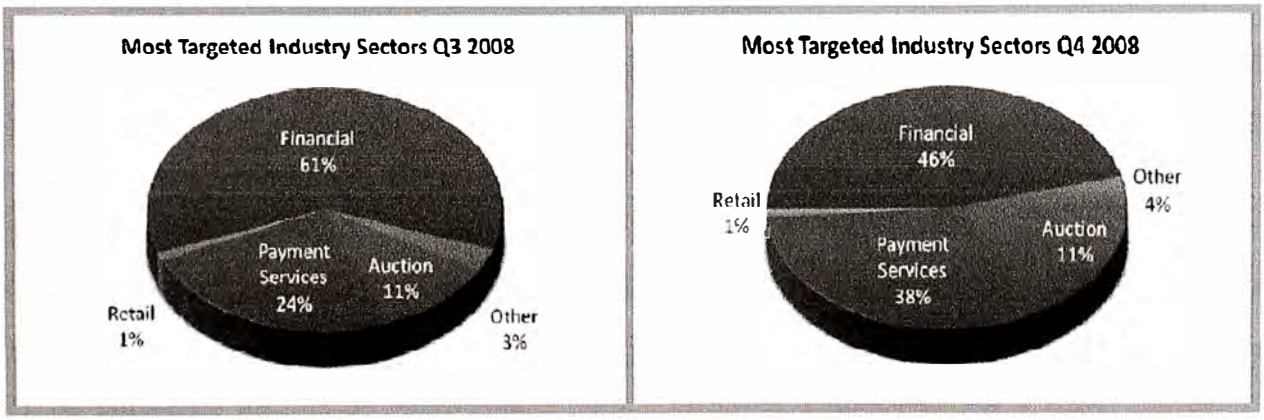


Fig.1.23 Reportes de phishing.

La tabla 1.13 nos muestra una distribución de los países donde se colocaron las páginas web para el phishing.

Tabla.1.13 Países donde se alojó el phishing.

July		August		September		October		November		December	
USA	49.53%	USA	59.37%	Sweden	62.55%	USA	80.08%	USA	51.69%	USA	55.75%
Netherlands	11.44%	Netherlands	6.92%	USA	32.29%	Australia	6.97%	China	22.11%	China	12.32%
Russia	8.83%	Germany	6.79%	Netherlands	1.39%	China	2.65%	Australia	4.68%	Sweden	9.30%
Germany	8.69%	Russia	5.74%	Germany	0.60%	Netherlands	2.62%	Netherlands	3.91%	Germany	4.73%
France	5.35%	France	5.39%	France	0.59%	Canada	1.66%	Germany	3.44%	Canada	4.03%
UK	4.28%	UK	3.62%	Rep. Korea	0.59%	Germany	1.44%	Canada	3.35%	Rep. Korea	3.33%
Canada	3.79%	Sweden	3.30%	Japan	0.56%	Rep. Korea	1.42%	UK	3.13%	France	2.94%
Italy	2.85%	Canada	3.17%	UK	0.52%	France	1.13%	Rep. Korea	3.09%	Russia	2.88%
Rep. Korea	2.79%	China	2.90%	Spain	0.51%	UK	1.09%	Italy	2.39%	UK	2.63%
Luxembour g	2.45%	Rep. Korea	2.81%	Taiwan	0.40%	Malaysia	0.94%	France	2.21%	Netherlands	2.09%

1.3 Importancia de la seguridad de la información en las organizaciones

La evolución del mundo de los negocios ha modificado la manera en la que las compañías se desenvuelven e interactúan entre sí. En este contexto la seguridad de redes es un tema crítico que trasciende las políticas de IT (Tecnologías de la Información) de las empresas, para convertirse en un asunto vital para los negocios.

A continuación se muestran algunos datos interesantes sobre lo que pasa en las empresas cuando son afectadas por ataques:

- **80%** de las compañías siniestradas desaparecen en 5 años.
- **60%** de todas las compañías han sufrido una violación de la seguridad en los últimos dos años.
- El **75%** calificó la violación como **"seria"** y además no habían desarrollado algún plan de contingencia para ocuparse del incidente.
- El **80%** de las violaciones fueron perpetradas por personal propio.

Se verificó que las decisiones gerenciales no eran las convenientes ante un evento grave de servicio, por no contar con adecuados planes de contingencia.

1.3.1 Estudio realizado a Empresas en la Región

Cisco Systems Latinoamérica encomendó a la firma de investigación de mercados Kaagan Research and Associates, la realización de 75 entrevistas en profundidad con Directores de IT de empresas locales de Argentina, Brasil, Colombia, Chile, México y Perú, abarcando una gran variedad de industrias y mercados verticales. Durante las entrevistas, los especialistas fueron consultados sobre diferentes temas de interés para la industria IT, como seguridad, calidad de servicios de Internet, usos de las páginas web corporativas, uso de Internet en ambientes laborales, capacitación y estructuras operativas del área de IT.

Presentamos a continuación los principales resultados del estudio con respecto al tema de seguridad.

a) Antecedentes de ataques de seguridad

Consultados acerca de ataques a la seguridad de los sistemas informáticos de sus compañías ocurridos en los últimos doce meses, se obtuvieron los siguientes resultados:

- Un 43 % afirma haber sido víctima de virus informáticos.
- Las páginas web de un 21 % de las empresas consultadas han sufrido ataques por parte de hackers.
- Un 51 % reconoce haber enfrentado problemas menores, tales como uso inadecuado de los sistemas informáticos, e-mail corporativo o el acceso a Internet para distribución de material inapropiado.

b) Temas que preocupan a los especialistas

La seguridad de la información es el tema que más preocupa al nivel gerencial: 79 por ciento de los consultados consideraron que los máximos directivos de sus compañías consideran este tema "de extrema prioridad" o "muy prioritario". Ver Fig.1.24.

Fig.1.24 Prioridad que asignan los directivos de empresas a la seguridad de sus redes.

Dentro de las amenazas que los directivos de tecnología encuentran para la seguridad de los sistemas informáticos de sus compañías, la posibilidad de ataques por parte de hackers es lo que más les preocupa. 64 % de los directivos consultados dijo estar "muy preocupado" al respecto, mientras que solo un 4 % opinó que el tema no le resultaba preocupante. Ver Fig.1.25.

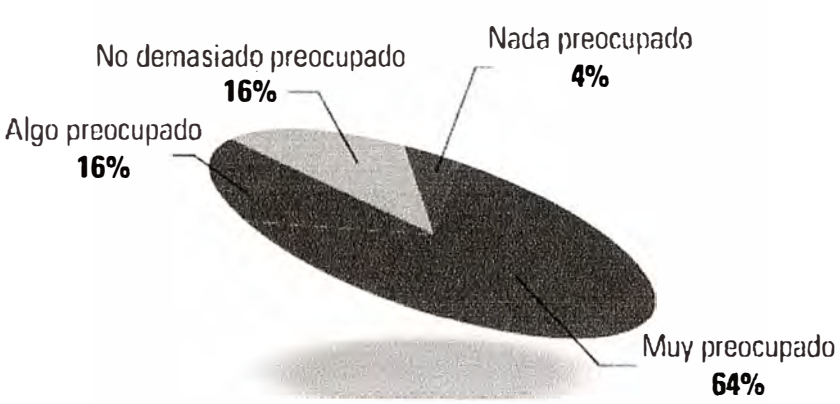


Fig.1.25 Nivel de preocupación por amenazas de seguridad Hackers.

Los directivos de tecnología consideran a los empleados actuales de la compañía como una amenaza de seguridad más importante que los ex-empleados. 64 % de los entrevistados manifiesta estar preocupado por las violaciones de seguridad provocadas por los empleados actuales de la compañía, mientras que 42 % dice estar preocupado cuando se refiere a quienes ya no forman parte de la organización.

En menor medida, los directivos de tecnología también se muestran preocupados por amenazas como terrorismo o crimen organizado.

c) Medidas de seguridad

Ocho de cada diez compañías consultadas cuentan con planes de contingencia para enfrentar posibles ataques de seguridad.

En cuanto a herramientas técnicas de seguridad que actualmente utilizan:

- La totalidad de ellos utilizan software antivirus.
- 93 % refuerzan su seguridad a través de códigos de acceso para sus empleados.
- 92 % cuentan con firewalls para impedir ataques originados en Internet.

Aunque menos comunes, existen además otras medidas "no-técnicas" de seguridad, como:

- Cambios formales en los procedimientos de control de los sistemas informáticos, implementados por un 69 % de los entrevistados.

  Siete de cada 10 de los directivos de tecnología entrevistados aseguran contar con políticas de seguridad claramente documentadas

d) Presupuesto

Un 57 % de los directivos de tecnología consultados accedieron a brindar información sobre los presupuestos del área de IT.

Casi la mitad de ellos destinaron menos del 10 % del total de su presupuesto general de IT a seguridad durante el último año. Ver Fig.1.26.

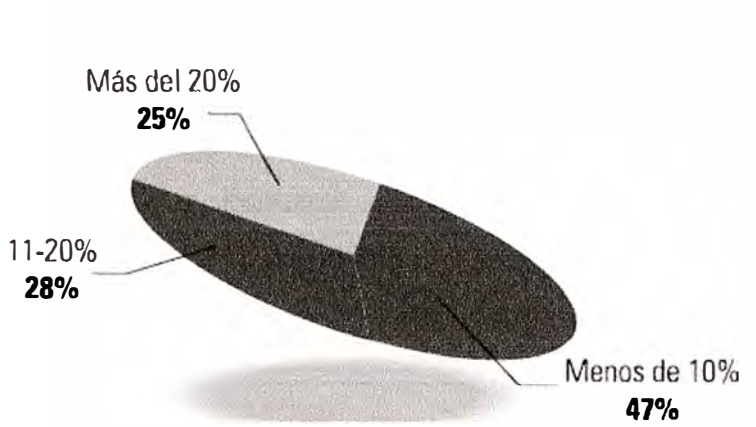


Fig.1.26 Porcentaje estimado del presupuesto general de IT asignado a seguridad.

e) Conclusiones generales del Estudio

- Los hackers son considerados ampliamente como la mayor amenaza para las redes empresariales, superando a otros grupos como empleados y ex empleados, terroristas, crimen organizado y competidores.
- El número de reportes de ataques reales comprobados a las redes corporativas es bajo. Infecciones por virus informáticos y el uso inapropiado de Internet aparecen como problemas más frecuentes.
- A pesar de los altos niveles de preocupación ante posibles ataques a las redes, muchos de los directivos consultados reconocen que sólo se asigna una parte menor del presupuesto general de IT a seguridad.
- En línea con los crecientes niveles de preocupación sobre temas de seguridad, muchas compañías ya cuentan con sistemas de seguridad, que van desde mayores controles de sus procedimientos, hasta soluciones como firewalls, passwords y software antivirus.

1.3.2 Evaluación de la seguridad de la información en América Latina

Cisco Systems realizó el primer Cisco Security Index, una referencia para comprender cómo las empresas de la región evalúan la seguridad de su información clave y cuáles son sus esfuerzos para establecer y mantener estándares que ayuden a conservar segura dicha información. El puntaje del Cisco Security Index va de 0 a 100. Una puntuación perfecta de 100 representa los máximos niveles de implementación y compromiso con las mejores prácticas en lo que se refiere a políticas de seguridad de la información. Por el contrario, un puntaje de 0 refleja una falta total de cumplimiento de prácticas de Seguridad y una posición totalmente alejada de la protección y la defensa contra las amenazas.

Los principales segmentos corporativos entrevistados fueron: Manufactura (40%), Servicios (10%), Finanzas/Seguros/Bienes Raíces (10%), Distribuidores (6%), Energía/Empresas de Servicios Públicos/ Petróleo (5%), Comercio minorista (4%), Transporte (3%), Construcción (3%), Agricultura/ Pesca (3%), Salud (3%).

El puntaje del Índice obtenido por cada país latinoamericano analizado fue el siguiente (Ver Tabla 1.14):

Tabla.1.14 Puntajes obtenidos por países de la Región.

País	Puntaje
México	66
Venezuela	64
Chile	64
Brasil	63
Colombia	62
Argentina	62

De acuerdo con las encuestas realizadas, Argentina es el país con el menor nivel de políticas de Seguridad de la Información aprobadas, con sólo el 68% de las empresas. En Brasil y Colombia, en cambio, esa proporción es del 81%, las más altas de la región.

El 12% de las empresas de Venezuela y México no reportan a la gerencia los problemas de seguridad, mientras que para Argentina el índice llega al 24%. A esto se le suma el hecho de que el 80% de las compañías de Chile y Venezuela cuentan con software de control de acceso y de Argentina el 67%.

Con respecto al uso de passwords y claves de acceso múltiples Brasil está a la cabeza con el 99%, le sigue México con 85% y por último Argentina con 65%.

El 68% de las empresas venezolanas está preocupado por la posibilidad de ataques del tipo phishing/pharming, el 60% de las brasileras y el 40% de las argentinas.

La percepción de amenaza en torno del robo de datos de usuarios es más pronunciada en el Brasil (74% de quienes respondieron la encuesta dijo que es "extremadamente seria" o "muy seria"), seguido por Chile (64%) y Venezuela (57%). Estos tres países son también los que más riesgos ven en los botnets; el phishing / pharming; el acceso no autorizado a los datos por parte de empleados, los ataques a las redes y la pérdida de datos móviles.

Los gerentes de TI del Brasil también mostraron niveles muy elevados de preocupación en torno de la amenaza a la Seguridad de la Información que pueden representar los actuales empleados (el 78% admitió estar "muy preocupado" o "algo preocupado") y también los ex

empleados (63%), mientras que Colombia es el país que tiene el puntaje más alto en lo que se refiere a riesgos para la Seguridad de la Información por parte de los terroristas (48%).

Los peligros para la seguridad provenientes de hackers despiertan altos niveles de preocupación a través de toda la región. Más de las tres cuartas partes de los gerentes de TI (el 78%) están "muy preocupados" o "algo preocupados" por los riesgos a la Seguridad de la Información provocados por los hackers. La mayoría de los sondeados en el Brasil (un 63%) y Chile (56%) dijeron estar "muy preocupados" por dicho tema.

La mayor parte de los representantes de TI de los países encuestados ven a los riesgos procedentes de los ataques de virus como "extremadamente serios" o "muy serios" (70%), con Venezuela (82%) y Chile (80%) a la cabeza de los más países más preocupados. La alta gerencia de las empresas brasileñas son las que más tienen a considerar a la Seguridad de la Información como una muy alta prioridad, mientras que la Seguridad de la Información es menos importante para los altos directivos de la Argentina. Cuando los encuestados consideraron que los riesgos a la Seguridad de la Información aumentaron fuertemente en los últimos años, los temas vinculados a ella tendieron a mostrarse como más prioritarios para la conducciones gerenciales.

El 60% de quienes participaron del sondeo dijeron que la seguridad TI es una "muy alta" o "alta" prioridad para los directores de sus compañías; o Resultados específicos por país: Argentina (46%), Brasil (75%), Chile (60%), Colombia (53%), México (58%) y Venezuela (58%).

Las organizaciones chilenas lideran en cuanto a la medición formal de los costos de seguridad en sus empresas (59%), seguidas por Colombia (50%). En cambio, las compañías brasileñas son las menos inclinadas a incorporar métricas de costos (30%).

De cada cinco firmas, más de cuatro (84%) tienen instalados procesos para cumplir con los requerimientos de seguridad necesarios para mantener la continuidad de los negocios a través de toda la organización. o Resultados específicos por país: Argentina (83%), Brasil (90%), Chile (86%), Colombia (73%), México (85%) y Venezuela (78%).

La mayor parte de las organizaciones en cada nación (en teoría) tienen instalados procedimientos para que los equipos de TI informen posibles vulnerabilidades a la seguridad, y casi la mayoría de los gerentes de TI aseguran tener aplicaciones para gestionar la seguridad, aunque en general no reportan los problemas de seguridad de un modo consistente y periódico. Sólo el 24% de todos los encuestados "siempre" informan los problemas de seguridad TI de manera periódica, mientras que un 39% admite los

reporta "rara vez". Otro 10% admite que "nunca" da a conocer tales problemas. Brasil es el país que más frecuentemente reporta los problemas de Seguridad de la Información a su gerencia, mientras que en Argentina, México y Venezuela la gran mayoría de los sondeados afirmó que "raramente" o "nunca" lo hace.

Conclusiones

Si se analizan los puntajes del Índice basándose en el tamaño de la empresa encuestada, puede advertirse que las organizaciones con menos de 300 empleados tienen puntajes menores que sus contrapartes más grandes. Tales resultados están mostrando que es preciso hacer un trabajo adicional para generar conciencia entre las firmas pequeñas y medianas, con el objetivo de resaltar la importancia de hallar modos efectivos de mantener sus datos e informaciones más sensibles a resguardo.

El Índice, patrocinado por Cisco y realizado por la consultora Kaagan Research Associates, fue creado a partir de las respuestas de más de 600 gerentes de Tecnologías de la Información de los seis principales países latinoamericanos: Argentina, Brasil, Chile, Colombia, México y Venezuela.

A medida que la Seguridad de la Información gana importancia para la organización de la IT en todo el mundo, el Cisco Security Index para América Latina nos ayuda a conocer cuál es la percepción y preparación de las empresas de la región, para establecer puntos de referencia y una guía hacia las mejores prácticas.

CAPITULO II
MARCO CONCEPTUAL

2.1 Antecedentes del problema

2.1.1 Reseña histórica

A medida que los sistemas de información han ido evolucionando, y haciéndose más comunes en la vida cotidiana, también fueron evolucionando las amenazas que se presentaban a los usuarios de los sistemas de información. Esto debido a que había cada vez más aplicaciones para las empresas, usuarios, etc.

Las amenazas fueron evolucionando de la siguiente manera:

a) Amenazas de primera generación:
Amenazas: Virus, gusanos y trojanos, ataques a las redes.
Protección: Los antivirus y los firewall identificaban la mayoría de amenazas pero no todas.

b) Amenazas de segunda generación
Amenazas: SPAM, Spyware, amenazas blindadas, bots y ataques de Cyber terroristas, etc.
Protección: Los antivirus, anti-spyware, y filtro de contenidos intentaban reducir la amenaza, y eliminaban la mayoría de ellas, pero no todas.

c) Amenazas de tercera generación
Amenazas: spear phishing, malware diseñado, root kits, robo y ataques orientados.
Protección: Todos las protecciones legadas intentaron mantenerse protegiendo contra estas amenazas pero no lograron detener muchas de ellas.

La Fig.2.1 nos ilustra las amenazas que se presentan en las redes de datos.

Fig.2.1 Representación de amenazas de red.

- Un alto porcentaje de las vulnerabilidades que se descubren pueden ser explotadas remotamente.
- Europa es la fuente principal de e-mails de phishing. España aporta un gran porcentaje de esta amenaza.
- Casi el 50% de los sitios web para phishing son alojados en USA.
- Un alto porcentaje de las amenazas, categorizadas como malware en el 2007, corresponden a troyanos (28% del total).
- El 80% de las explotaciones basadas en web son ofuscadas, JavaScript es el principal vector de ofuscación.

La Fig.2.2 nos muestra una distribución porcentual del software malicioso, malware, durante el 2007.

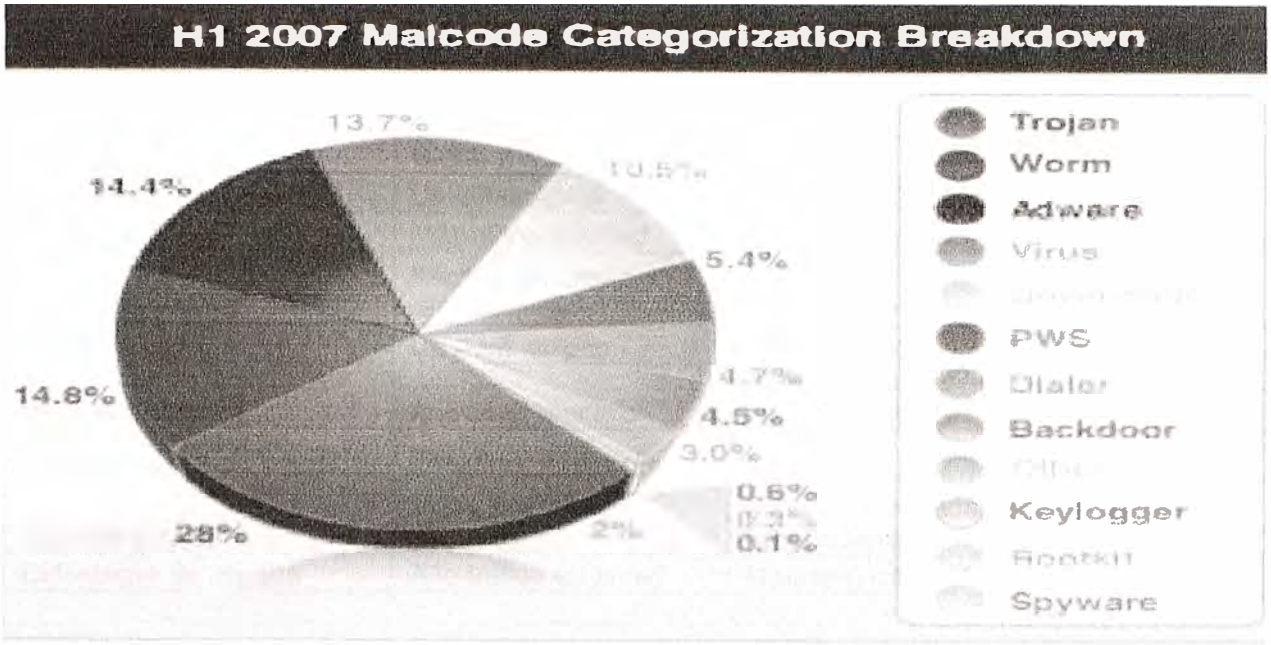


Fig.2.2 Distribución porcentual de Malware en el 2007.

La tabla 2.1 nos muestra información relevante concerniente a las amenazas presentadas en el 2006 y 2007.

Tabla 2.1 Comparación amenazas presentadas.

	2006	2007 (Primer semestre)
Vulnerabilidades	7247, 88% fue explotable remotamente	3273 (bajo 3,3%), 91.4% fue explotable remotamente (subió 3.4%)
Malware	Descargables 22%, gusanos,	Troyanos de boutique (28%), archivos de formato de exploit.
SPAM	Spam basado en imágenes se incrementó dramáticamente	Debuta el spam con pdf.
Phishing	Phishing generalizado hacia grandes objetivos (eBay, PayPal, etc.)	Objetivos bancos y personajes.
Convergencia de amenaza	Malware enviado por spam.	Enlaces Web en spam hacia sitios con malware. Ofuscación basado en navegador.

2.1.2 Evolución de los ataques

La motivación para los atacantes, ha variado con el tiempo conforme los sistemas informáticos también variaron. Cuando recién se iniciaron las redes de computadoras, la gente comenzaba a explorarla y para algunas personas era un reto; en busca de fama, atentar y/o descubrir vulnerabilidades en los sistemas. Actualmente los atacantes no quieren ser descubiertos, y orientan el ataque a algo específico en busca de algo del cual ellos puedan beneficiarse de alguna u otra manera, ideando y/o averiguando métodos complejos de ataque, los cuales están en constante cambio.

La tabla 2.2 nos muestra las características de los ataques de antes y actuales.

Tabla 2.2 Comparación amenazas presentadas.

Características del ataque	Antes	Nueva era
Motivación	Gloria y Fama	Financiero
Complejidad	Unidimensional	Vectores múltiples
Alcance	Máximo/publicidad	El objetivo/ robo
Riesgo primario	Pérdida de servicio, reparaciones	Propiedad intelectual/finaciero
Objetivo	De perfil amplio	Especifico, individuos
Defensa efectiva	Antivirus, reactivo	Multi-tecnologías, proactivo, comportamiento.
Recuperación de servicio	Escanear y remover	No siempre posible.
Tipo de ataque	Virus, gusanos, Spyware	Malware diseñado, root kits, phishing, ransomware.
Estrategia de ataque	Alto tráfico en la red	Malware, robo.

2.1.3 Evolución del Spam

Como sucede en todo tipo de ataque, cuando se encuentra una manera de protegerse de éste, los atacantes buscan formas de poder superar esa protección. Es así, como sucede en la evolución del envío de correo no deseado, como es el Spam.

La figura 2.3 nos muestra los cambios evolutivos ocurridos en los envíos de correo no deseado, spam.

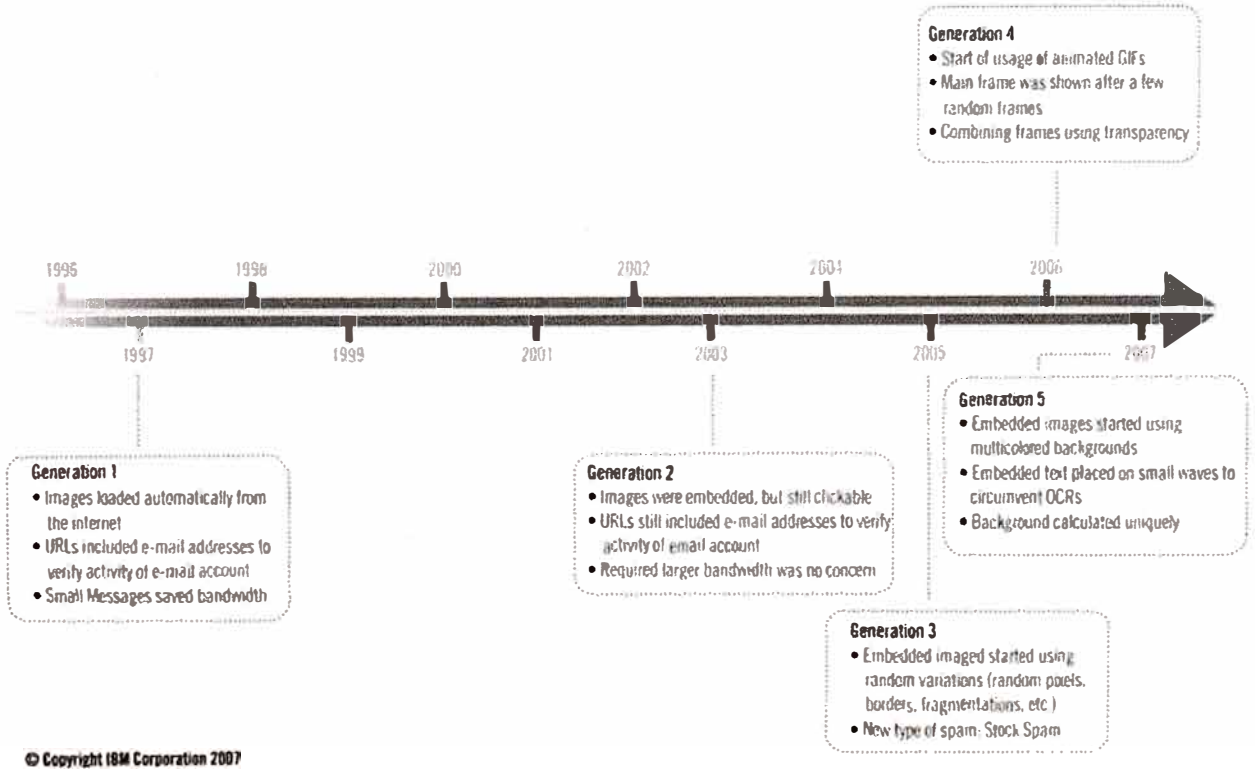


Fig.2.3 Evolución del Spam.

a) Generación 1

Se caracterizaba por:

- Tener imágenes que cargaban automáticamente desde Internet.
- Las URLs incluyeron direcciones e-mail para verificar la actividad de la cuenta de correo objetivo.
- Pequeños mensajes, no ocupaban mucho ancho de banda.

b) Generación 2

Se caracterizaba por:

- Las imágenes venían embebidas en el mail, pero aun eran clickeables.
- Las URLs incluyeron direcciones e-mail para verificar la actividad de la cuenta de correo objetivo.
- El hecho que requerían un mayor ancho de banda no era una preocupación.

c) Generación 3

Se caracterizaba por:

- Las imágenes embebidas en el mail de spam, comenzaron a utilizar variaciones aleatorias (pixeles aleatorios, bordes, fragmentación, etc.).
- Aparece un nuevo tipo de spam, el "Stock Spam".

d) Generación 4

Se caracterizaba por:

- Se inicia el uso de GIF animados.
- El frame principal era mostrado luego de unos pocos frames aleatorios.
- Combinación de frames usando transparencia.

e) Generación 5

Se caracterizaba por:

- Las imágenes embebidas comienzan a usar fondos multicolores.
- El texto embebido se localizó en pequeñas ondas.
- El fondo de pantalla calculado únicamente.

2.1.4 Evolución de los mecanismos de defensa

Frente a la evolución de las amenazas como se vio anteriormente, también fue evolucionando los sistemas de defensa tales como:

a) Firewalls

Evolución de los Firewalls (ver Fig.2.4):

- En 1985 nace la primera generación por filtro de paquete (Packet Filter) en la división de software IOS de Cisco.
- De 1989 a 1990 aparece las segunda generación en los laboratorios Bell de AT&T, firewall a nivel de circuito (circuit level firewall).
- De 1990 a 1991 aparece la tercera generación a nivel de capa de aplicación (application layer). El primer producto comercial fue de Digital Equipment Corporation´SEAL.
- De 1991 a 1992 se da la primera investigación sobre filtrado de paquetes dinámicos (dynamic packet filtering). Pruebas independientes en el USC´s (Information Sciences Institute) generaron los sistemas "Visas".
- En 1994 aparece la cuarta generación, donde Checkpoint desarrollo el primer producto comercial.
- De 1996 a 1997 aparece la quinta generación (arquitectura kernel proxy), Cisco desarrolló un producto en 1997.
- 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007....están aun basados en la misma tecnología.

Pros de los Firewalls:

- Habilidad para controlar las sesiones en las comunicaciones y protocolos.
- Rápido.
- Confiable.
- Entrega control de la comunicación en la red y por ende protección.
- Varias características deseadas (nat, pat, auth, vpn, routing).

Contras de los Firewalls:

- La tecnología se vuelve antigua.
- No puede contra todas las amenazas actuales.
- Carece de inteligencia para implementar una protección compleja de detección de intrusos.

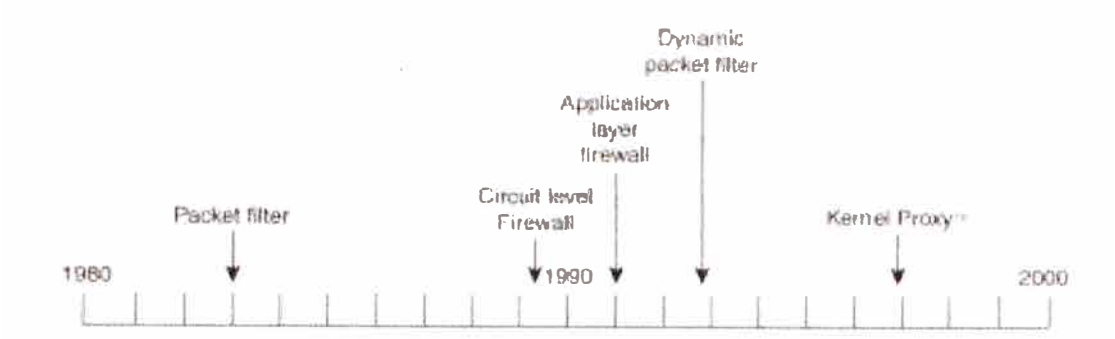


Fig.2.4 Evolución del Firewall

En la actualidad existen cajas "appliance" que no solo son firewall, sino poseen varios módulos de seguridad en un solo producto.

b) Antivirus

Evolución del antivirus:

- En 1949 las teorías sobre autorreplicación de programas son desarrolladas por vez Primera.
- En 1981 aparece virus para apple 1,2,3 encontrados sobre OS II.
- En 1983 Fred Cohen define al virus de computadora.
- En 1986 el primer virus para PC fue creado "Brain".
- El Virus implementa la habilidad para infectar el código del sector de boot y reemplazarlo por su propia rutina de infección.
- Stoned (el primer MBR infector)
- En 1987 el virus Lehigh es un de los primeros.
- El virus Jerusalem apareció en la Universidad de Hebrew en Israel. Fue el primero diseñado para residir en la memoria, también apareció el virus ping-pong.
- En 1990 aparece el antivirus symatecs Norton.
- En 1991 el primer virus polimorfo es nombrado Tequila.
- En 1992 hay 1300 virus (420% más que 1990). DAME y VCL son creados.
- En 1995 "Word concept" es exparcido a través de los documentos word.
- En 1996 Baza, Laroux y Staog infectaron windows 95, excel and linux.
- En 1998 StrangeBrew es el primer virus que infecta Java.
- El virus Melissa se exparce , BubbleBoy es el primer gusano no dependiente de que el recipiente esté abierto para infectar.
- El 2000 aparece I LOVEYOU
- El 2003 el virus SLAMMER (saphire) infecta 75.000 máquinas en 10 minutos, doblando su número cada 8.5 segundos de infección en el primer minuto.

Pros de los Antivirus:

- Precisa la forma de detectar amenazas de virus conocidos.
- Eficiente respuesta de borrado, bloqueo y cuarentena.
- Puede ser desplegado en perímetros y local hosts.

Contras de los Antivirus:

- Aunque todos tengan instalados Antivirus, el desencadenamiento de virus aun podría ocurrir.
- Las firmas de escaneo no reconocen nuevos virus y gusanos hasta que es demasiado tarde. Hasta 2000 gusanos de rápida replicación podrían infectar entre actualizaciones semanales.
- Las firmas de los escaneos reconocen solamente aquellos virus en los cuales hay una muestra en la base de datos de firmas.
- Virus y gusanos paquetizados no están reconocidos.
- Las bases de datos de firmas crecen grandemente y lentamente.

c) IDS e IPS

- En 1980 nace el IDS como documento.
- En 1983 se convirtió en un proyecto.
- En 1987 se convirtió en un modelo.
- El primer IDS comercial salió a la luz en 1997 (ISS Real Secure Network Sensor).
- En el 2001 el primer IPS comercial es creado por ISS (Real Secure Guard).

Pros de los IDS:

- Suficientemente inteligentes para detectar la presencia de ataques en el tráfico de red.
- Lo suficientemente rápido.
- Entrega visibilidad y protección.

Contras de los IDS:

- Proclive a falsos positivos.
- Algo reactivo (desplegado como dispositivo pasivo)
- Comparando con los Firewall tienen poco mecanismo de bloqueo.
- Alto volumen de logs.

Los IPS (Intrusion Prevention System) es un dispositivo de seguridad (computador) que ejerce control de acceso para proteger los computadores de explotación (ingreso de

intrusos). Es considerado como una extensión de la tecnología del IDS (Intrusion Detection System), pero es realmente otra forma de control de acceso, como un firewall a nivel de la capa de aplicación.

2.2 Definición de términos

A continuación se define una serie de amenazas informáticas:

Malware: (del inglés ***malicious software***, también llamado **badware**, **software malicioso** o **software malintencionado**) es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware. Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red.

Virus informáticos: Los virus informáticos utilizan una variedad de portadores. Los blancos comunes son los archivos ejecutables que son parte de las aplicaciones, los documentos que contienen macros (Virus de macro), y los sectores de arranque de los discos de 3 1/2 pulgadas y discos duros (Virus de boot, o de arranque). En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al primero el código del virus. Normalmente la aplicación infectada funciona correctamente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado van de una computadora a otra y es ejecutado.

Cuando un software produce pérdidas económicas en el usuario del equipo, también se clasifica como **software criminal o Crimeware**, término dado por Peter Cassidy, para diferenciarlo de los otros tipos de software malignos, en que estos programas son encaminados al aspecto financiero, la suplantación de personalidad y el espionaje, al identificar las pulsaciones en el teclado o los movimientos del ratón o creando falsas páginas de bancos o empresas de contratación y empleo para con ello conseguir el número de cuenta e identificaciones, registros oficiales y datos personales con el objetivo de hacer fraudes o mal uso de la información. También es utilizando la llamada Ingeniería social, que consiste en conseguir la información confidencial del propio usuario mediante engaños, como por ejemplo, mediante un correo en donde mediante engaños se solicita al usuario enviar información privada o entrar a una página falsificada de Internet para hacerlo.

Adware: Este software muestra o baja anuncios publicitarios que aparecen inesperadamente en el equipo, pudiendo hacerlo simultáneamente a cuando se está utilizando la conexión a una página Web o después de que se ha instalado en la memoria de la computadora.

Algunas empresas ofrecen software "gratuito" a cambio de publicitarse en su pantalla,[5] otras al instalar el programa, se instalan junto con Spyware sin que lo note.

También existen algunos programas "a prueba" (shareware), que mientras no son pagados, no permiten algunas opciones como puede ser imprimir o guardar y además en ocasiones cuentan con patrocinios temporales que al recibir la clave libera de tales mensajes publicitarios y complementan al programa.

El adware es una aplicación que muestra publicidad y que suele acompañar a otros programas. Si bien esto puede hacerse, en algunas oportunidades, bajo el conocimiento del usuario, el problema radica en los casos en los cuales se recoge información sin consultar.

También pueden ser fuente de avisos engañosos. Por lo general los programas adware tiene la capacidad de conectarse a servidores en línea para obtener publicidades y enviar la información obtenida. Cabe aclarar que no toda aplicación que muestra algún tipo de publicidad incluye adware y esto, en muchos casos, se ha transformado en una controversia para determinar cuando un elemento se encuadra dentro de estas características.

Backdoor: Una puerta trasera (también conocidos como *Backdoor*) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación o facilita la entrada a la información de un usuario sin su permiso o conocimiento. Como es el caso de e-mail, que aparentan ser enlaces a actualizaciones y que al pulsarla nos conecta a páginas similares a las originales, descargando archivos backdoor que al instalarlos, abrirá un puerto del equipo, dejándolo a expensas del autor del malware o para poder descargar otros códigos maliciosos.

Según como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras.

El primer grupo se asemeja a los Caballos de Troya, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infecta al sistema para poder ser instalado permanentemente.

El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.

Badware Alcalinos: Este es un tipo de Malware mitad spyware, mitad backdoor, suele residir en las ventanas del sistema observando incesantemente hasta que se lanza al acecho de un usuario.

Bomba fork: Programa que se autorreplica velozmente para ocupar toda la memoria y capacidad de proceso del ordenador donde se ejecutan, debido a que su forma de ataque es del tipo denegación de servicio (DoS) que es un ataque al servidor o a la red de computadoras para producir la no conectividad a una red debido a que consume el ancho de banda atacado, al crear programas y procesos simultáneos muy rápidamente, saturando el espacio disponible e impidiendo que se creen procesos reales del usuario.

Bots: Es un programa robot que se encarga de realizar funciones rutinarias, pero que también pueden ser usados para, por ejemplo, crear cuentas en los diferentes sitios que otorgan e-mail gratuitos, para con estas cuentas realizar daños. En algunos casos este bot, puede encargarse de fingir ser un humano dando contestación a preguntas como es el caso de supuestos adivinos que dan el futuro a aquellos que pagan por este servicio o fingir ser una mujer u hombre con quien se esta teniendo una candente conversación, pero también pueden ser juegos de Internet programados para jugar contra supuestamente una serie de contrincantes que lo son en forma virtual, pudiendo pedir cantidades de dinero para poder participar y con ello además poder tener datos de cuentas de tarjetas de crédito. También son programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de la víctima, es decir convirtiéndola en un "Zombi".

Bug: Es todo error en la programación que impide funcionar bien a los equipos de cómputo. Se le llama así por la entrada de una polilla encontrada atrapada entre los puntos en el relé # 70, panel F, de la Mark II , Construida por Aiken, cuando era probada en la Universidad de Harvard, el 9 de septiembre de 1945.

Caballo de Troya: Un programa caballo de Troya (también llamado Troyano) cuyo nombre está relacionado con la conocida historia del Caballo de Troya, es un intruso informático, software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador y contaminar a los equipos por medio del engaño, usando un programa funcional para encubrirse y permanecer dentro del computador. Se considera que el primer troyano aparece a finales de los años 1980, pero eran poco comunes al ser necesario que el programa se distribuyera casi manualmente, fue hasta que se generalizo la comunicación por Internet, que se hizo más común y peligroso al entrar ocultos e instalarse

cuidadosamente sin que se percatara el usuario del equipo, con lo que sean considerados una de las más temibles invasiones ilegales en las estaciones de trabajo, servidores y computadoras personales.

Cookies: La cookie es el tipo de almacenamiento de información guardado en el propio equipo que puede hacer normalmente el seguimiento de las preferencias en Internet dándole una clave que su creador podrá identificar para con ello tener una referencia de visitas con la finalidad de medir preferencias de mercado. Pero también por lo mismo puede ser usada por hackers para analizar qué páginas consulta un usuario regularmente, quitándole privacidad. Estos cookies se pueden aceptar o evitar en nuestros equipos, por medio de la configuración de privacidad de las opciones del navegador de Internet.

Crackers: Son programas que monitorean las contraseñas en las aplicaciones de la máquina. Además de referirse a hackers con malas intenciones, a los que se les conocen también como ladrones de contraseñas, se considera que lo hacen para demostrar su habilidad y satisfacer su vanidad, dañando la relativa seguridad del cifrado, en algunos casos dejando hasta su rubrica, para hacer más palpable su osadía.

Cryptovirus, Ransomware o Secuestradores: Es el programa que entra a la computadora y se instala, registra su estancia en dispositivos de almacenamiento extraíble (flash disks, pendrives, etc.) buscando y cifrando los archivos del registro del disco infectado, después borran los originales en forma inadvertidamente para el usuario, haciéndolos inaccesibles para el dueño y cuando se intenta abrir algún documento, a través de un archivo de texto que forma parte de este malware informa, como en el AIDS.exe: *"Si quiere obtener una clave para liberar el documento, ingrese 378 dólares a la cuenta en la ciudad de Panamá número X"*,[2] o también se le solicita que se envíe el pago vía Internet (rescate), para obtener la clave de dicha codificación (la liberación del rehén). o bien simplemente impide el ingreso del usuario a su unidad de almacenamiento extraíble ocasionando el bloqueo temporal del sistema hasta la desconexión del dispositivo de la PC. Como en el "Cn911.exe" (aplicación encubierta como ejecutable que se instala en el registro de usuario y lo modifica.) La codificación es de claves simétricas simples, es decir son aquellas que utilizan la misma clave para cifrar y descifrar un documento lo que ocasiona la reducción de la capacidad de almacenamiento del disco extraíble, sin embargo algunos usuarios con conocimientos informáticos avanzados, descifran, cuales son dichas claves y pueden llegar a recuperar la capacidad real del dispositivo, trucada por el malware.

Dialers: Los dialers son programas que llaman a un número telefónico de larga distancia, o de tarifas especiales, para, a través del módem, entrar de forma automática y oculta para el usuario y sin su consentimiento, principalmente a páginas de juegos, adivinación o pornográficas, que van a redituar en beneficio económico a los creadores del malware, pero que además al usuario le crean la obligación de pagar grandes tarifas por el servicio telefónico. Actualmente las conexiones por medio de banda ancha, han evitado estos problemas.

Exploit: Un exploit es aquel software que ataca una vulnerabilidad particular de un sistema operativo. Los exploits no son necesariamente maliciosos –son generalmente creados por investigadores de seguridad informática para demostrar que existe una vulnerabilidad. Y por esto son componentes comunes de los programas maliciosos como los gusanos informáticos.

Falso antivirus: Hacen creer que es un antivirus gratuito y que la computadora ha sido detectada infectada, pero que para deshacerse de la infección deberá comprar la versión completa, y si trata de eliminar esta instalación del supuesto antivirus le informan que debe tener la clave de desinstalación, la cual deberá comprar.

Hijacker: Programa que realiza cambios en la configuración de la página de inicio del navegador, que lo redirige a otras páginas de características indeseables como son las pornográficas y más peligrosamente a copias casi fieles de las bancarias.

Hoaxes, Jokes o Bulos: Son bromas que semejan ser virus, pero que, ciertamente no los son. Normalmente una persona conocida nuestra recibe una "alarma" de un supuesto virus y nos "hace el favor" de notificarnos para que tomemos precauciones en nuestro equipo.

Keystroke o keyloggers: Son programas espías, que toman el control de los equipos, para espiar y robar información, monitorea el sistema, registrando las pulsaciones del teclado, para robar las claves, tanto de páginas financieras y correos electrónicos como cualquier información introducida por teclado, en el equipo utilizado para saber lo que la víctima ha realizado como conversaciones que la misma tuvo, saber donde ha entrado, qué ha ejecutado, qué ha movido, etc. Pueden ser también aparatos o dispositivos electrónicos colocados intencionalmente en equipos, que se intercalan entre el dispositivo y el computador.

Ladilla virtual: Conocido como (virtual crab). Este tipo de programa maligno que, como analogía al parásito de transmisión sexual, entra en una computadora a través del sexo

virtual, sitios pornográficos o cualquier aplicación relacionada. Los sitios web pornográficos suelen ser un gran caldo de cultivo para estos Malware virtuales.

Leapfrog: Las ranas como también se conocen en español son programas que entran a los equipos para conocer las claves de acceso y las cuentas de correo almacenadas en la libreta de direcciones para ser utilizadas en la replicación de estos, a través de enviar copias del gusano.

Parásito Informático: Este tipo de malware es el que se adhieren a archivos (especialmente ejecutables), como lo haría un parásito. Ese archivo ejecutable es denominado portador (o Host) y el parásito lo utiliza para propagarse. Si el programa es ejecutado, lo primero que se ejecuta es el parásito informático, y luego, para no levantar sospechas, se ejecuta el programa original. Muchas veces es aquí donde los parásitos fallan, porque hay programas que detectan estas modificaciones y lanzan errores (incluso errores de advertencias de presencia de malware).

Pharming: Es el software maligno que suplanta el DNS, en el archivo host local, para conducirnos a una página Web falsa, con lo cual, al intentar entrar a un determinado nombre de dominio en nuestro navegador nos redirecciona al que el cracker, ha cambiado.

Phishings: Del inglés "fishing" (pescando), se utiliza para identificar la acción fraudulenta de conseguir información confidencial, vía correo electrónico o página web, con el propósito de que los usuarios de cuentas bancarias lo contesten, o entren a páginas aparentemente iguales a la del banco o de los portales con ingreso por contraseña. El phishing se basa en el envío por parte de un estafador de un mensaje electrónico o enlace de una empresa supuestamente respetable. Éstas a menudo conducen a una página Web falsificada que han creado, y engañan al usuario para que introduzca su contraseña y su información personal. Así lo convierten en un blanco fácil del robo de información personal o financiera de manera electrónica utilizando el nombre de un tercero (banco) y últimamente las páginas del acceso a e-mails de compañías como Yahoo!.

Pornware: Describe programas que usan el Módem de la computadora para conectarse a servicios de pago por evento pornográfico o para bajar contenidos pornográficos de la Web. Es un caso particular de Dialers. Primero se descarga desde algún sitio que ofrece todo absolutamente gratis un pequeño programa ejecutable, que coloca en el escritorio de la PC un llamativo ícono para que cualquier incauto con un simple click haga el enlace mencionado, aparecen insistentes mensajes sugiriendo de que todo es completamente gratis y sin límite de tiempo.

Rabbit o conejos: Reciben este nombre algunos gusanos informáticos, cuyos códigos malignos llenan el disco duro con sus reproducciones en muy poco tiempo y que también pueden saturar el ancho de banda de una red rápidamente además de poder mandar un número infinito de impresiones del mismo archivo, colapsando la memoria de la impresora al saturarla.

Riskware: Programas originales, como las herramientas de administración remota, que contienen agujeros usados por los crackers para realizar acciones dañinas.

Rootkit: Los rootkits son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Los rootkit generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante. Los rootkit pueden incluir puertas traseras, permitiendo al atacante obtener de nuevo acceso al sistema o también pueden incluir exploits para atacar otros sistemas y evitan ser desinstalados o eliminados a toda costa, pues cuenta con protección para no permitirlo, con lo cual se convierte en un programa indeseable y molesto. Los rootkit se volvieron famosos a partir de uno que estaba incluido en un mecanismo anticopia en algunos CD de música de la empresa Sony.

Scumware o escoria: Es cualquier software que hace cambios significativos en la apariencia y funciones de las páginas Web sin permiso del Administrador (Webmaster) o propietarios. Por ejemplo, un número de productos sobreponen la publicidad de los banners con otros anuncios, a veces para los productos de la competencia. El Scumware puede agregar hyperlinks desautorizados a la sección opinión de una página Web - a veces usar de un usuario acoplamientos a los sitios posiblemente desagradables. Tales programas pueden interferir con hipervínculos (hyperlinks) existentes agregando otros destinos a los previstos. A veces, el Scumware es conocido como thiefware.

Spam: Se le llama spam a los e-mailes basura, que son enviados masivamente a direcciones electrónicas compradas por empresas con la finalidad de vender sus productos. Se calcula que alrededor del 75% del correo electrónico que circula en la red son spam,

Spyware: Programas espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instalados ("husmean" la información que está en nuestro equipo) para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad en algunos casos lo hacen para obtener direcciones de e-mail. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar programas de terceros, por lo que rara vez el usuario es consciente de ello. Estos agentes espía, pueden ingresar a la

PC por medio de otras aplicaciones. Normalmente trabajan y contaminan sistemas como lo hacen los Caballos de Troya.

Ventanas emergentes/POP-UPS: Son, generalmente, ventanas muy molestas que aparecen al navegar y muestran publicidad o información que es difícil de eliminar y que aparece constantemente. Son una forma en línea de publicidad en el World Wide Web, que aumentan el tráfico de la red o que son también usadas para capturar direcciones de e-mail. Trabaja cuando ciertos sitios abren una ventana del buscador para exhibir los anuncios. La ventana pop-up que contiene un anuncio es generada normalmente por JavaScript, pero se puede generar por otros medios también.

Worms o gusanos: Los gusanos informáticos son similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades del objetivo o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar.

CAPITULO III
METODOLOGIA PARA LA SOLUCION DEL PROBLEMA

3.1 Alternativas de solución, tecnologías existentes

3.1.1 Firewall

- Sistema que previene el uso y el acceso desautorizados a ordenadores, elementos de red.
- Los firewall (cortafuegos) pueden ser software, hardware, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios desautorizados de Internet tengan acceso a las redes privadas conectadas con Internet, especialmente intranets.
- Todos los mensajes que entran o salen de la Intranet pasan a través del firewall, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados.
- Es importante recordar que **un firewall no elimina problemas de virus u otro tipo de malware del ordenador**, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, etc. añadirá cierta seguridad y protección adicionales para tu ordenador o red.

Tipos de técnicas usadas en firewall:

- **Packet filter:** mira cada paquete que entra o sale de la red y lo acepta o rechaza basándose en reglas definidas por el usario. La filtración del paquete es bastante eficaz y transparente a los usuarios, pero es difícil de configurar. Además, es susceptible al IP spoofing.
- **Application gateway:** Aplica mecanismos de seguridad a ciertas aplicaciones, tales como servidores ftp y servidores telnet. Esto es muy eficaz, pero puede producir una disminución de las prestaciones.

- **Circuit-level gateway:** Aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se haya hecho la conexión, los paquetes pueden fluir entre los anfitriones sin más comprobaciones.
- **Proxy server:** Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta con eficacia las direcciones de red verdaderas.

3.1.2 IPS (Intrusion Prevention System)

Un IPS es un dispositivo de seguridad de red que monitorea la red y/o la actividad en los sistemas buscando malicioso o comportamientos no deseados y puede reaccionar, en tiempo real, para bloquear y prevenirla de aquellas actividades.

Un IPS basado en red, por ejemplo, operará en línea para monitorear todo el tráfico de red para descubrir código malicioso o ataques. Cuando un ataque es detectado, éste puede descartar (dropear) los paquetes de la ofensiva mientras aun pueda pasar el resto de tráfico válido. La tecnología de prevención de intrusos es considerada como una extensión de la tecnología de detección de intrusos (IDS).

Los IPS evolucionaron a finales de los 90 para resolver ambigüedades en el monitoreo de redes pasivas mediante la localización de sistemas de detección en linea. En sus inicios los IPS eran IDS que eran capaces de implementar comandos de prevención a los firewalls y cambios en los controles de acceso de los routers. Esta técnica quedó corta operacionalmente porque creó una competencia entre el IDS y el exploit que pasó por el mecanismo de control. IPS en línea pueden ser vistos como una mejora por encima de las tecnologías de firewall.

Los IPS pueden tomar decisiones de control de acceso basados en el contenido de la aplicación, en vez de la dirección ip y los puertos como los firewall tradicionales. Sin embargo, para mejorar el rendimiento y exactitud de la clasificación, la mayoría de IPS usan puerto destino en el formato de sus firmas.

Los IPS pueden también servir en segundo término a nivel de host para denegar actividad maliciosa potencial. Hay ventajas y desventajas para los IPS basados en hosts comparados con los IPS basados en la red. En muchos casos, las tecnologías son planeadas para ser complementarias.

Un IPS debe también ser un sistema muy bueno en detección de intrusos para tener una baja cantidad de falsos positivos. Algunos IPS pueden también prevenir ataques de descubiertos, tales como aquellos causados por Buffer overflow.

El IPS trabaja mediante una profunda inspección del tráfico de la red. Puede identificar y analizar más de 100 redes y protocolos de capa de aplicación y formatos de archivos de datos.

Los IPS previenen contra gusanos, Spyware, P2P, DoS/DDoS, Cross-site Scripting, SQL Injection, Phishing, Buffer Overflow, etc.

3.1.3 Protección de correo - Antispam y Antivirus

Son aplicaciones o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados. Algunos antivirus y firewalls (cortafuegos) poseen incorporadas herramientas antispam. El principal objetivo de una herramienta antispam, es lograr un buen porcentaje de filtrado de correo no deseado. Pero tampoco deben identificar al correo deseado como no deseado, pues eso traería peores consecuencias que "olvidar" filtrar algún spam. Las herramientas antispam utilizan múltiples técnicas para detectar el correo no deseado. Algunas utilizan técnicas locales. Por ejemplo, emplean un diccionario propio para detectar palabras que suelen aparecer en estos correos. Ese diccionario puede ser "armado" con palabras que el propio usuario identifica como spam manualmente, o armado de forma inteligente por la aplicación, cuando el usuario selecciona qué es deseado y qué es no deseado de su bandeja de entrada. Otra técnica local es el uso de una lista de amigos y una lista de enemigos. El programa o el propio usuario manualmente identifican las direcciones y nombres que son considerados amigos y de los cuales no recibirán correos no deseados. Lo mismo para la lista de enemigos. Una técnica no local, la utilizan las herramientas que se conectan a servidores remotos, que se encargan de analizar cada uno de los emails que llegan al usuario, para identificar si son o no spam. Esos servidores remotos utilizan grandes bases de datos con información (direcciones IP, nombres, textos, etc.) para identificar el correo no deseado. Similares técnicas utilizan los servicios antispam online que prestan algunas empresas para sus usuarios como Gmail de Google, Hotmail de Microsoft y Yahoo! Mail de Yahoo!.

3.1.4 Servidor Proxy

El servidor proxy web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc. También existen proxies para otros protocolos, como el proxy de FTP.

Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos

descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Ventajas

En general (no sólo en informática), los proxies hacen posibles varias cosas nuevas:

- **Control**. Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Ahorro**. Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro

usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- **Abuso**. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- **Carga**. Un proxy ha de hacer el trabajo de muchos usuarios.
- **Intromisión**. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
- **Incoherencia**. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.
- **Irregularidad**. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

3.1.5 Filtro de contenidos

El filtro de contenido refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web. El filtro de contenido determina qué contenido estará disponible en una máquina o red particular. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable. Cuando se impone sin el consentimiento del usuario, puede constituir censura. Los usos comunes de estos programas incluyen padres que desean limitar los sitios que sus hijos ven en sus computadoras

domésticas, escuelas con el mismo objetivo, empleadores para restringir qué contenidos pueden ver los empleados en el trabajo.

3.1.6 Terminador de túneles - VPN

Son dispositivos que sirven para que un usuario remoto, pueda establecer una sesión virtual, segura y encriptada entre ellos, y un cliente remoto. De manera que nadie que interceptase la comunicación pueda interpretar la información que se está cursando.

Generalmente son utilizados para que usuarios con acceso a Internet, puedan realizar conexiones seguras contra sus empresas, y así poder accesar a información solo disponible dentro de su empresa que no puede ser vista de manera pública.

La encriptación que suelen utilizar estos equipos es SSL (la misma usada por las URL https) , en este caso, al cliente remoto solo deberá abrir una página web específica, ingresar su usuario y clave, y logrará que su pc obtenga una dirección ip virtual que le permitirá acceder a la red de su empresa.

También son utilizada las conexiones por túneles "ipsec" , en este caso el usuario remoto necesita tener instalado un software cliente para conectarse al terminador de túneles de su empresa.

3.1.7 Solución Token

Un token de seguridad (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Los *tokens* electrónicos tienen un tamaño pequeño que permiten ser cómodamente llevados en el bolsillo o la cartera y son normalmente diseñados para atarlos a un llavero. Los *tokens* electrónicos se usan para almacenar claves criptográficas como firmas digitales, o datos biométricos como las huellas digitales. Algunos diseños se hacen a prueba de alteraciones, otro pueden incluir teclados para la entrada de un PIN.

Existe más de una clase de *token* de autenticación, tenemos los bien conocidos generadores de contraseñas dinámicas "OTP" y la que comúnmente denominamos *tokens* USB, los cuales no solo permiten almacenar passwords y certificados, sino que permiten llevar la identidad digital de la persona.

Estos dispositivos token, muestran claves que al desear un usuario autenticarse, ésta es validada por un servidor Token.

3.2 Solución del problema para una empresa

3.2.1 Topología diseñada

En la figura 3.1 se propone una primera topología de red para una empresa que desee minimizar los diversos tipos de riesgos y amenazas presentes en las redes informáticas tanto dentro de sus organizaciones como fuera, esto es en Internet, y que además desee garantizar la disponibilidad de la información y por tanto la disponibilidad del servicio de red para la seguridad de la información.

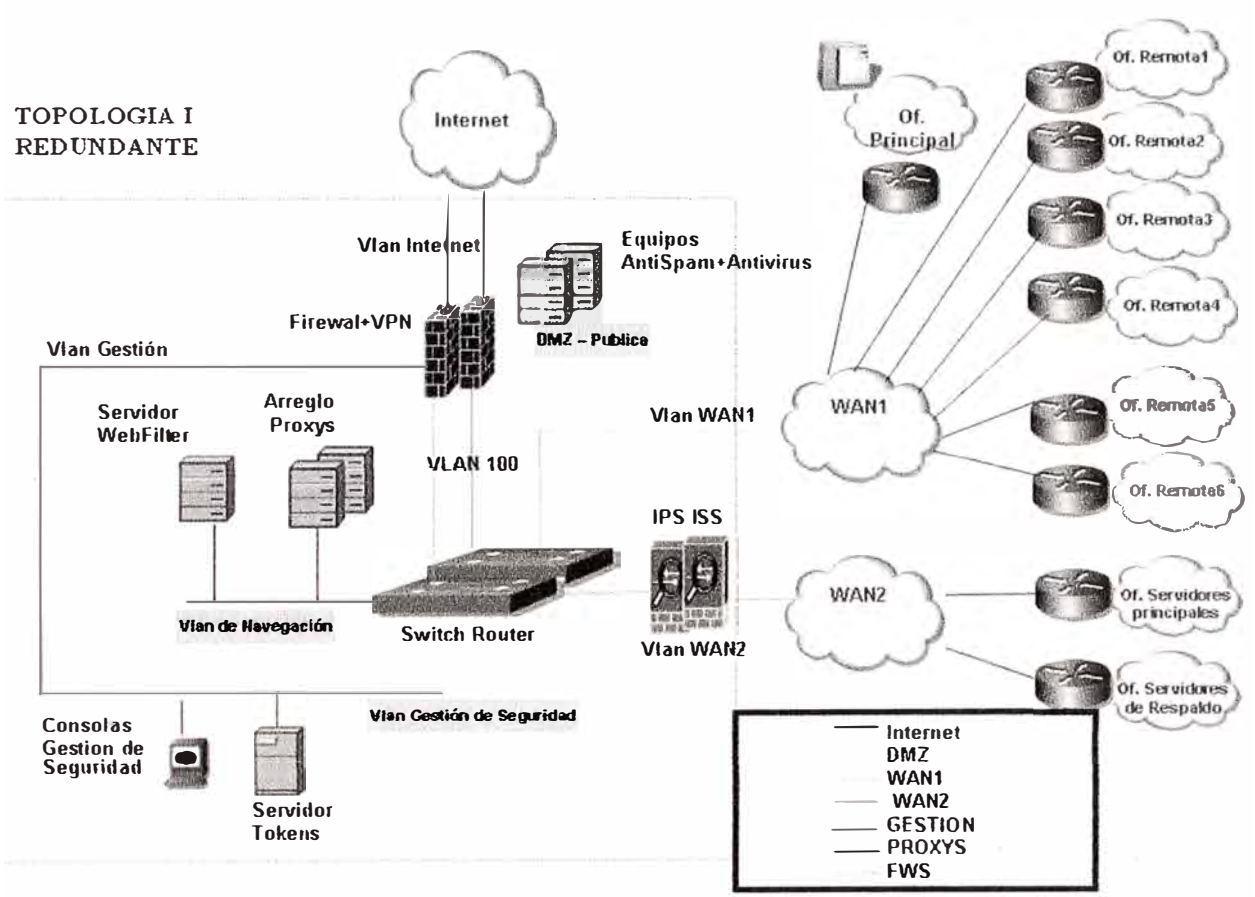


Fig. 3.1 Topología I: Solución redundante

Se ha diseñado una solución de seguridad (para una organización) que puede estar localizada en cualquier locación; como un centro de datos fuera de la empresa, para brindar una mayor autonomía y flexibilidad.

Se está considerando una red WAN1 para tráfico desde las sedes remotas de la organización hacia Internet, o a sus servidores de aplicaciones u otras sedes remotas, y una red WAN2 para tráfico dirigido desde las sedes remotas o Internet hacia las sedes de los servidores, la principal y la sede de respaldo de darse el caso.

Para que la WAN1 pueda comunicarse con Internet, el tráfico primero deberá ser analizado el Proxy, WebFilter, Firewall/IPS Perimetral y solución antispam/antivirus. En caso que el la WAN1 desee comunicarse con los servidores de aplicaciones ubicados en la WAN2, el tráfico será analizado primero por el IPS de ISS; alternativamente, algún tráfico desde la WAN1 hacia la WAN2 podría bien pasar también por el Firewall perimetral de ser necesario. Es importante notar que el tráfico que se da en la red interna de la organización o intranet suele ser mayor al tráfico cursante entre la organización e Internet, por tal motivo se ha dimensionado unos firewalls perimetrales que soportarían sin ningún inconveniente tráfico entre Internet y la organización en ambos sentidos, pero que dependiendo del volumen del tráfico de las aplicaciones internas que maneja la organización, si todo ese tráfico pasase por estos firewall podría llegar a saturarse. Por tal motivo se opta en colocar una solución IPS exclusivamente para proteger la WAN2 de los servidores, debido a la criticidad y volumen de tráfico que estos recibirán.
En caso que el tráfico provenga de Internet hacia los servidores de aplicaciones en la WAN2, éste será analizado primero por el Firewall/IPS perimetral y por la solución IPS de ISS asegurando la zona de red más importante de la organización.
Desde Internet se podrán establecer túneles VPN para usuarios, así como túneles VPN contra sedes remotas (por ejemplo con otro país), de manera que estos puntos remotas puedan tener un acceso seguro (sesiones encriptadas) hacia las redes y aplicaciones de la organización protegida. De esta manera también se protege la red de la organización al restringir el acceso desde Internet solo mediante una conexión VPN permitida, hacia redes u aplicaciones que no deben ser publicadas en Internet, pero que empleados en ubicaciones remotos así lo requieran para llevar a cabo sus actividades laborales.

En ésta solución se está considerando el equipamiento necesario para poder mitigar las diversas amenazas a la información, expuestas en el presente trabajo. Sin embargo, estas tecnologías no garantizan; como ninguna tecnología lo hace, una plena seguridad de las redes informáticas para la organización a proteger.

A sabiendas que los costos son un factor decisivo, alternativamente, se presenta en la figura 3.2 una solución que ofrece las mismas características y seguridad en la red, empero no ofrece la redundancia mostrada en la solución 1.

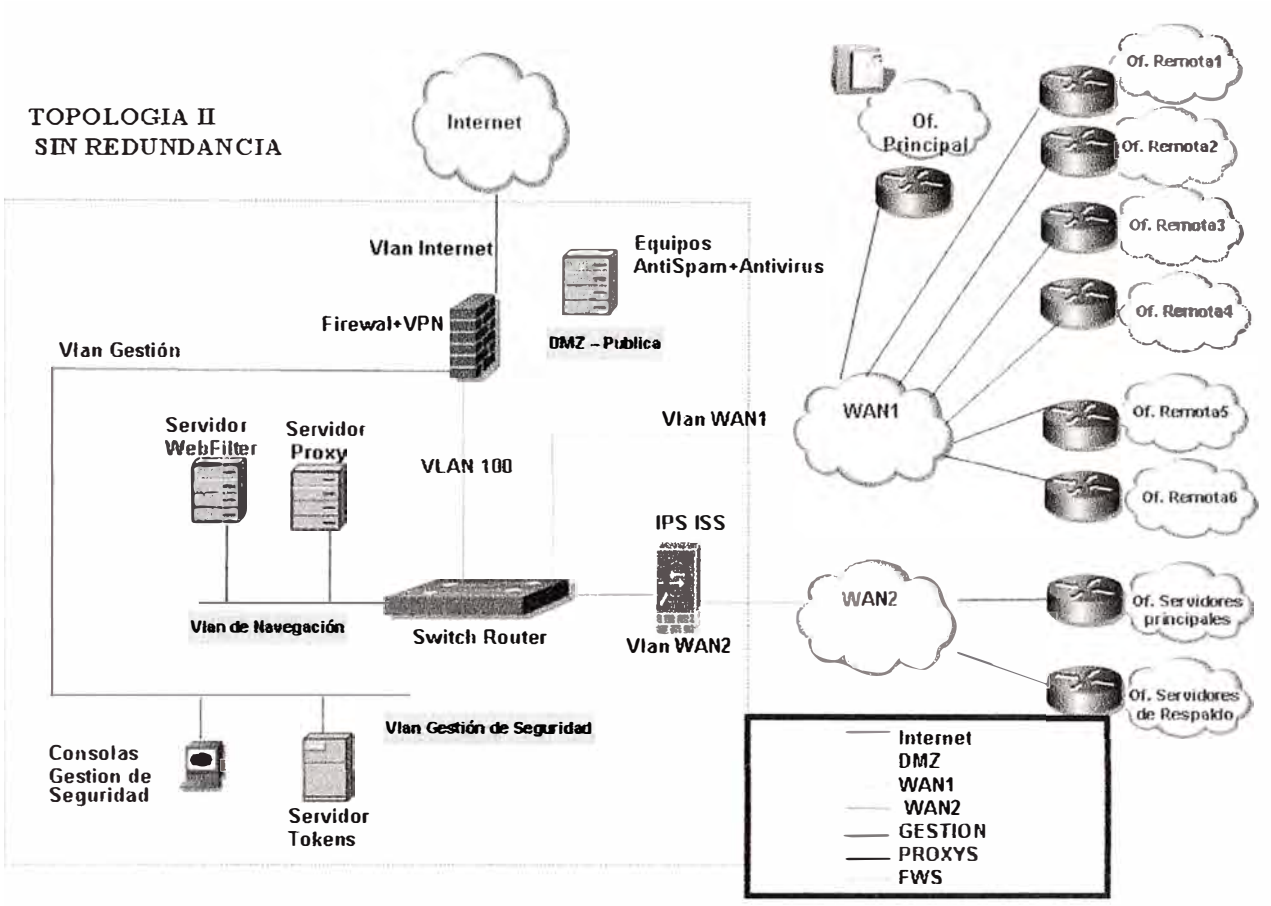


Fig. 3.2 Topología II: Solución no redundante

Esta solución sin redundancia posee únicos puntos de falla no redundantes, a diferencia de la solución 1 que podrían dejar sin servicio ciertas necesidades de la organización.
Por ejemplo, en caso de caída del Firewall Perimetral, toda comunicación contra Internet se vería afectada. Por otro lado, en caso de falla del equipo IPS de ISS, éste dejaría pasar el tráfico, comportándose como si se tratase de un "cable", permitiendo así la comunicación entre la WAN1 y la WAN2, pero esta vez sin ser inspeccionado.

3.2.2 Alcance de la solución

La solución redundante planteada comprende lo siguiente:

- Firewall en arreglo de alta disponibilidad para el manejo de una (1) zona DMZ, compuesta por dos equipos appliances CheckPoint UTM-1 Modelo 1050.

- Servicio de Proxy con "caché", compuesta por:
    - Software, dos (02) licencias de ISA Server version 2006 de Microsoft y
    - Hardware, dos (02) servidores HP modelo DL360.
- Servicio de detección de virus en correos (anti-virus) y Servicio de detección de correos no deseados (anti-spam). Ambos servicios estarán compuestas por: Hardware, dos (02) equipo appliance Ironport modelo C100
- Servicio de filtro de contenido (WEB filtering) compuesta por:
    - Software, Proventia Web Filter de ISS con licencia para 1500 usuarios.
    - Hardware, un (01) servidor HP modelo DL360.
- Servicio de acceso remoto seguro (VPN) que use protocolo SSL, cual con el uso de perfiles da acceso a los usuarios de manera que se puede permitir las conexiones hasta el nivel de aplicación, este servicio esta incorporado en los dos (02) equipos appliances CheckPoint UTM-1 Modelo 1050 que brindan el servicio de firewall con el modulo adicional CheckPoint SSL Network Extender para Windows para 50 usuarios.
- Servicio de IPS perimetral en arreglo de alta disponibilidad, este servicio esta incorporado en los dos (02) equipos appliances CheckPoint UTM-1 Modelo 1050 que brindan el servicio de firewall, con el modulo SmartDefense.
- Equipo IPS interno que concentra el tráfico de datos de todas las oficinas, validando la calidad del tráfico y evitando la propagación de virus, ataques, etc. Se trata de un (01) equipo de la marca ISS modelo Proventia Network IPS GX4004-C, que tiene la capacidad de pasar a modo transparente (bridge) ante la ocurrencia de una falla y de un (01) servidor HP modelo ML 110G4 para la gestión, administración y monitoreo del IPS.
- Para la conexión al servicio de VPN modalidad VPNSSL a la red de datos, se sustenta en un mecanismo de autenticación de un nivel suficientemente seguro y robusto como el uso de dispositivos "Token" que refuercen la identificación de los usuarios. La autenticación robusta está compuesta por doscientos tokens Digipass Go 3 y el software VM Radius 3.0 con licencia para doscientos usuarios. Ambos componentes de la marca VASCO.

Con todo lo mencionado, se puede esperar una disponibilidad de la plataforma de seguridad de 99%.

Para el caso de la solución 2 sin redundancia, solo se considera un equipo del mismo modelo que el propuesto en la solución 1, en cada ítem.

3.2.3 Entregables

Con toda esta tecnología usada en el diseño, se puede obtener los siguientes reportes mensuales, que sirven como feedback para controlar, dimensionar, y tomar alguna acción necesaria para así poder optimizar y asegurar la red. Los posibles reportes mensuales son:

Firewall:

- Consumo de ancho de banda por IP (interna y externa)
- Consumo de ancho de banda por servicio (puerto tcp, udp,etc.)
- Registro de actividades por dirección IP origen e IP destino, servicio, acción realizada, cantidad de bytes, tiempo y fecha
- Registro de actividades por servicio
- Reporte de alertas, ataques recibidos y bloqueados
- Reporte de reglas establecidas.

Proxy:

- Reporte de acceso a páginas Web (por url)
- Reporte de los tiempos de conexión de cada usuario
- Reporte de consumo de ancho de banda por IP y por usuario.
- Reporte de los accesos atendidos y denegados de los usuarios.

VPN:

- Reporte histórico de acceso atendidos por IP y por usuario, indicando fecha y hora
- Reporte de los accesos atendidos y denegados de los usuarios
- Reporte detallado de los accesos que no fueron atendidos, indicando las razones
- Registro (log) de las operaciones que efectúe cada usuario según la demanda
- Reporte de los usuarios conectados por días y horas

AntiSpam

- Reportes de correos bloqueados, en cuarentena y válidos, tanto de entrada como de salida
- Reporte de correos bloqueados, en cuarentena y válidos por categorías, tanto en entrada como en salida
- Reporte de correos en cuarentena por RBL indicando los remitentes y destinatarios

- Reporte de remitentes y destinatarios de los correos por volumen.

Filtro de contenido (Web Filter)

- Reporte de páginas WEB por usuario, por IP, por fecha y hora, pr categorías.
- Reporte de páginas WEB más visitadas y los usuarios "TOP"
- Reporte de intentos de accesos acertados y fallidos
- Reportes de accesos por categorías.

Antivirus para correo

- Reporte de correos infectados usando la cuarentena de correos infectados.
- Reporte de tabla estadistica por dominio.
- Reporte de ranking de virus detectados por el sistema

3.3 Recursos requeridos para la solución

3.3.1 Equipamiento y Costos

El equipamiento a utilizar en cualquiera de las soluciones es mostrado en la tabla 3.1.

Tabla 3.1 Equipamiento a utilizar en la solución.

Servicio	Hardware	Software
Firewall	Checkpoint - UTM Modelo 1050	-
Proxy	Servidor HP Modelo DL360	Microsoft ISA Server 2006
VPN SSL	Checkpoint - UTM Modelo 1050	Checkpoint SSL Network
Antispam/antivirus Correo	Ironport C100	
Web Filter	Servidor HP Modelo DL360	ISS Proventia WebFilter
IPS Perimetral	Checkpoint - UTM Modelo 1050	Checkpoint SmartDefense
IPS Interno	Proventia Network IPS GX4004-C	
Tokens	Servidor HP Modelo ML110 / VASOC - 200 Digipass Go3	Vasco - VM Radius

Al utilizar equipos redundantes en la solución 1 a diferencia de la solución 2 se da una diferencia de costos considerable.

Teniendo en cuenta que los equipos requieren contratos de soporte y mantenimiento para garantizar la correcta operación y actualización durante el tiempo que se utilicen en la empresa a proteger, se considerará un presupuesto en base a 5 años de operación.

La tabla 3.2 nos muestra el presupuesto de la solución de seguridad con alta redundancia.

Tabla 3.2 Presupuesto en solución redundante a 5 años.

Función	Modelo	Cantidad	P. Unidad	Subtotal
Firewalls	Firewall UTM-1 1050	2	28207	56414
SmartCenter y Reporter	HP ML110 G4 (1 GB RAM)	1	1447	1447
Consola IPS – SiteProtector	HP ML110 G4 (1 GB RAM)	1	1447	1447
IPS	IPS ISS	2	26512	53024
Switch L3	Switch Cisco 3560	2	3000	6000
Servidor Proxy	HP DL360 G5 (2 GB RAM-RAID5)	2	7146	14293
AntiSpam/antivirus correo	IRONPORT C100 (1500 users)	2	29602	59204
Servidor WebFilter	HP DL360 G5 (2 GB RAM-RAID5)	1	7146	7146
Servidor Tokens	HP ML110 G4 (1 GB RAM)	1	1447	1447
Software WebFilter	Software WebFilter	1	26250	26250
Software Tokens	Software Tokens	1	16872	16872
			TOTAL $	243 543

La tabla 3.3 nos muestra el presupuesto de la solución de seguridad sin redundancia.

Tabla 3.3 Presupuesto en solución no redundante a 5 años.

Función	Modelo	Cantidad	P. Unidad	Subtotal
Firewalls	Firewall UTM-1 1050	1	28207	28207
SmartCenter y Reporter	HP ML110 G4 (1 GB RAM)	1	1447	1447
Consola IPS – SiteProtector	HP ML110 G4 (1 GB RAM)	1	1447	1447
IPS	IPS ISS	1	26512	26512
Switch L3	Switch Cisco 3560	1	3000	3000
Servidor Proxy	HP DL360 G5 (2 GB RAM-RAID5)	1	7146	7146
AntiSpam/antivirus correo	IRONPORT C100 (1500 users)	1	29602	29602
Servidor WebFilter	HP DL360 G5 (2 GB RAM-RAID5)	1	7146	7146
Servidor Tokens	HP ML110 G4 (1 GB RAM)	1	1447	1447
Software WebFilter	Software WebFilter	1	26250	26250
Software Tokens	Software Tokens	1	16872	16872
			TOTAL $	149 076

Los precios mostrados incluyen contratos de soporte y mantenimiento con los fabricantes.

Se aprecia que la solución redundante es 63% más costosa.

3.3.2 Recursos humanos

Se requiere de al menos un ingeniero de seguridad especialista responsable de administrar toda esta plataforma, realizando las tareas de mantenimiento, actualizando versiones de firmware, software, hardware de los equipos involucrados en cada uno de los servicios ofrecidos (Firewall, Proxy, VPN, AntiSpam, Web Filter, Antivirus para Correo, etc.).

Es importante considerar además que estas tecnologías de seguridad requieren un monitoreo continúo del tráfico analizado para detectar posibles anomalías y/o ataques en la red, y de esta manera poder tomar las acciones necesarias para preservar los sistemas "limpios".

También se requiere que el personal de operaciones de la empresa, se encarguen de monitorear estos servicios los siete días de la semana, las 24 horas del día para garantizar que el servicio se encuentre disponible y tomar las acciones correctivas rápidamente en caso de incidencia.

CONCLUSIONES

Las necesidades tecnológicas de las organizaciones en cuanto a comunicaciones y sistemas informáticos son casi comunes para todas ellas, y muchas de ellas imperativas para poder ser eficientes y subsistir en el mercado.

Las vulnerabilidades y amenazas a los sistemas de información han ido evolucionando a lo largo del tiempo, y por esta razón se requiere que los responsables de seguridad de las organizaciones estén en constante actualización para hacerles frente.

Las técnicas y tecnologías utilizadas para hacerle frente a estas amenazas también han ido evolucionando, y con el pasar de los años cada vez más empresas han ido adquiriendo estas tecnologías.

El hecho que una empresa posea muchas tecnologías para asegurar sus redes minimiza pero no garantiza que no haya problemas en los sistemas de información. Es necesario un adecuado y constante monitoreo, gestión, actualización y administración de éstas tecnologías, que siempre son administradas por el hombre.

Es importante mantener los sistemas operativos, firmwares, aplicaciones, y todo tipo de software actualizado, tanto en las computadoras personales, como en los servidores, equipos de comunicaciones y de seguridad. Dado que estas actualizaciones, incluyen parches de seguridad que libran de vulnerabilidades a los sistemas.

Los diseños de solución de seguridad presentados, han sido realizados considerando las múltiples amenazas expuestas en el presente trabajo, y con estos se logra el objetivo de hacerles frente a todas ellas, cubriendo las expectativas de aseguramiento a una posible empresa que cursa información crítica por sus redes.

Los diseños presentados fueron realizados considerando soluciones y equipamiento de marcas reconocidas en su campo, que puedan brindar flexibilidad, granularidad y el adecuado desempeño y rendimiento necesario para cubrir las expectativas de una empresa que valore bastante su información.

Es claramente notable, que en la medida que una empresa quiera asegurar en un mayor grado su información cada vez, mayor será la inversión que deberá realizar, y deberá considerar tecnologías líderes en el mercado, además de tener redundancia a lo largo de toda la solución de seguridad garantizando así la disponibilidad de la información.

El desembolso de dinero que una empresa despliega en aseguramiento de la información, se debería considerar como una inversión y no un gasto, pues de ocurrir un incidente, este podría propiciar cuantiosas pérdidas para la compañía, hasta el extremo del cierre.

Es importante considerar mejores prácticas en todos los procesos de la organización para preservar su información, teniendo como referencia; por ejemplo, a la ISO27000, relacionada a la seguridad de la información en las organizaciones, que no solo cubre la seguridad lógica, sino también una serie de buenas prácticas para preservar la confidencialidad, disponibilidad, integridad, etc. de la información, que se encuentra en almacenada de manera lógica en gran parte.

BIBLIOGRAFÍA

1. http://www.deloitte.com
2. http://www.ciscoredaccionvirtual.com/redaccion/multimedia/descargar.asp?archivo=822
3. http://www.webappsec.org/
4. http://www.antiphishing.org/
5. http://www.secunia.com
6. http://www.openware.biz/novedades/el_security_index_para_america_latina_dio_resultados_desalentadores
7. http://www.iss.net
8. http://cve.mitre.org
9. http://www.sans.org/top20/
10. http://support.microsoft.com/kb/824684
11. http://www.wikipedia.org