UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

SEGURIDAD INFORMÁTICA EN LOS SITIOS DE CAFÉ INTERNET EN LA CIUDAD DE MÉXICO

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N

ACOSTA CASTILLO RUBÉN

PACHECO CÁMARA SERGIO ALFREDO

DIRECTORA: M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS.

CIUDAD UNIVERSITARIA, NOVIEMBRE 2009.

AGRADECIMIENTOS

A ti mi Padre Dios por permitirme llegar hasta este día ayudándome a vencer los obstáculos que muchas veces parecieron inquebrantables. Hoy me siento dichoso de saber que siempre he contado con tu amor y bendición, los cuales han sido suficientes para lograr culminar esta tan importante etapa de mi vida que lejos de ti nunca hubiera sido posible concluir. No encuentro palabras para expresar la felicidad que embarga mi corazón, sólo quiero ofrecerte mi más sincero reconocimiento como mi Dios y mi Padre, pues por tu gracia soy lo que soy y tu gracia no ha sido en vano para conmigo. Pero antes de ser un profesionista quiero ser siempre tu hijo, ya que es el mayor privilegio que puedo tener, más valioso que todos los títulos de la tierra.

A ti Señor Jesús, por haberme visto con ojos de amor y misericordia regalándome a través de tu sacrificio y muerte la vida que hoy a tu lado disfruto y valoro. Te pido siempre guíes mi vida con tu poder y me ayudes a reconocer que todo lo que tengo y lo que soy es gracias a ti. Gracias por este momento tan significativo, pero más gracias por ser mi Salvador.

A ti Espíritu Santo por ser mi compañero en los momentos alegres y tristes, y aún los más difíciles. Gracias por consolarme y darme de tu unción para seguir siempre adelante. Este logro sin duda es por ti y para ti.

Con profundo agradecimiento a ti mamá, por ser mi inspiración para alcanzar mis metas, por guiarme desde pequeño y por todo tu apoyo. Gracias por tu paciencia, tu tolerancia, tu amor y aún por tu sufrimiento. Gracias por siempre confiar en mí. Tu esfuerzo se convirtió en tu triunfo y el mío, TE AMO. Mamá, todo mi trabajo va dedicado a ti, esperando que te llene de tanto gozo y satisfacción como a mí.

A ti papá por darme la estabilidad emocional, económica y sentimental, para poder llegar a este logro, que definitivamente no hubiese podido ser realidad sin ti, por ser el proveedor durante todos estos años que he vivido bajo tu techo, gracias por tus consejos y por preocuparte por el desarrollo de esta tesis. Gracias por siempre confiar en mí y apoyarme en los momentos más críticos de mi vida.

A mi querida Universidad, a mi facultad, a mis amigos(as) quienes siempre tendrán un espacio especial en mi corazón y a todos aquéllos profesores que compartieron conmigo sus conocimientos y sus experiencias, las cuales sin duda han sido valiosas y me han ayudado a llegar al final de la meta.

A la M.C. Jaquelina López Barrientos por haber compartido todo su conocimiento y experiencia con nosotros apoyándonos y motivándonos a concluir nuestra carrera universitaria. Gracias por sus consejos, su dirección, su tiempo brindado, su paciencia, pero más aún gracias por haber aceptado ser parte de este proyecto que hoy nos pertenece a los tres, y que es el impulso hacia las nuevas metas y retos que nos esperan en nuestro ejercicio profesional.

A ti Sergio, por haber sido la pareja perfecta en la realización de este trabajo, gracias por compartir conmigo los tiempos de angustia, pero también de alegría. Quizás después de este trabajo, no coincidamos más en otro proyecto pero estoy seguro que el haber trabajado juntos ha dejado una gran experiencia y una gran amistad que espero podamos conservar a lo largo de los años.

No puedo dejar de nombrar a la mujer que Dios envío a mi vida y que ha sido mi pilar en esta última etapa. Gracias Yadira, mi esposa amada, la mitad de lo que soy, la persona que Dios escogió para mi, con todos los atributos de la única compañera que posee todo lo que a mi me falta. Gracias por amarme a pesar de cómo soy y porque desde que te conocí supe que eres la compañera perfecta, junto a ti me han pasado las cosas más increíbles, lo único que te puedo decir es que TE AMO. Gracias por ser mi apoyo y mi ayuda en todos los proyectos. Somos un gran equipo para Dios. Gracias por aguantar las noches de desvelo y trabajo, en donde siempre me acompañaste y

peleaste codo a codo conmigo. Gracias linda por estar conmigo y dejar salir lo mejor de mí. Por ti y para ti es este trabajo, deseando que esta nueva etapa en nuestra vida pueda ayudarnos a progresar bajo el cuidado y la dirección de nuestro Dios. Gracias por siempre creer en mí, por tus palabras de aliento, por tu confianza depositada en mi persona, por tu tolerancia, pero sobre todo por ser la madre de los dos hermosos luceros que han alumbrado mi vida desde que Dios unió nuestras vidas: Michelle y Rubén.

No puedo concluir mis agradecimientos, sin mencionar a las dos personas más importantes que me ha dado la vida y quienes fueron el motor principal para poder terminar esta tesis. Me refiero en primer lugar, a ti mi niña Michelle quien con tu amor y con tu manera de ser conmigo te has ganado mi corazón. Te doy gracias por siempre creer en mí y motivarme a seguir aún en contra de todo. Gracias por tus besos, por tus abrazos, por tu sonrisa. Gracias por hacerme el hombre más feliz con tu existencia. Gracias por infundirme el coraje de superarme y por la dicha enorme de ser tu padre.

A ti mi niño Benbenuto quien llegaste a mi vida cuando más necesitaba recordar la tarea tan importante que Dios me había encomendado. Gracias por llenar mi vida de tanta felicidad con tu sola presencia en mi vida, hoy no logro imaginarme la vida sin ti pues tú eres mi vida y por ti es que me he esforzado y me seguiré esforzando para que con la ayuda de Dios siempre pueda ser tu apoyo, tu padre, pero sobre todo tu amigo en quien puedas confiar.

A ti Dios Padre por el camino que has puesto enfrente de mí y por permitirme completar cada proyecto de mi vida, como este trabajo el cual no hubiera sido posible de no estar conmigo y ponerme a todas las personas que me ayudaron de una y otra forma.

A ti mamá, te agradezco por esta vida que me has dado, por todo tu amor, apoyo y cariño, por estar conmigo en todo momento y alentarme para seguir adelante.

A ti papá, por cuidarme y enseñarme que no hay límites para lo que puedo hacer.

A mis hermanos, Mary y Chris, por todos esos momentos felices y tristes que hemos tenido y los que faltan por venir, para seguir juntos en este camino.

A ti Rubén, por acompañarme en esta travesía de la tesis y ser constante hasta el final, por demostrarme que la esperanza nunca muere.

A la maestra Jaquelina, por creer en nosotros y en nuestro trabajo, por ser la guía en este proyecto y el apoyo que necesitamos para completarlo.

A todos mis amigos, de la facultad y del trabajo, por enseñarme que siempre hay algo nuevo por conocer y siempre una sonrisa va a mejorar el día.

ÍNDICE

PÁGINA

INTRODUCCIÓN

Actualmente los sistemas computacionales representan un avance muy importante para las actividades del ser humano y poco a poco a través de los años se han ido involucrando en todos los ámbitos pensables; desde generar un trabajo escolar, hasta controlar grandes equipos industriales.

Desafortunadamente todos estos avances que dejan de manifiesto la dependencia del hombre hacia las computadoras han ocasionado problemas de seguridad en los sistemas de información; que van desde el descontrol de procesos como movimientos bancarios, robos de información de usuarios hasta fraudes en compañías.

Es por eso que los llamados virus, han mutado en elementos que ya no necesitan ser ejecutados por el usuario para infectar una computadora, los llamados malwares, se encargan de “tocar la puerta” hacia equipos con poca seguridad, para infiltrarse e iniciar la fuga de información hacia servidores específicos.

No se hable de los llamados “Café Internet”, los cuales requieren de manera importante de la seguridad informática debido al flujo de usuarios que llegan por día, y que realizan un sin fin de actividades, todas, de diferente giro y por ende, vulnerando la seguridad.

El problema surge porque los Café Internet son un centro de actividades computacionales a los que asisten todo tipo de clientes, existen los clientes quienes en sus oficinas no pueden hacer lo que quieren porque su empresa tiene acceso restringido a Internet, los jóvenes que no pueden chatear desde su casa, el aprendiz de hacker que no desea que sus huellas puedan ser rastreadas haciendo sus maldades desde estos sitios públicos, etc.

Entre los diferentes problemas que se pueden suscitar están: a raíz de este tránsito indiscriminado, puede recaer, en usuarios molestos por un “mal servicio” al verse afectados por intrusos o por daños a su información, suspensión o baja definitiva del servicio de Internet por parte del proveedor de la conexión, por argumentos de seguridad a sus servidores.

Es por ello que se realiza el presente proyecto, con la finalidad de analizar los niveles de seguridad informática que actualmente existen en los sitios de Café Internet en la Ciudad de México, para posteriormente, desarrollar un sistema de apoyo que permita generar políticas y mecanismos adecuados de seguridad con la finalidad de que los administradores o dueños de estos sitios mantengan un nivel de seguridad adecuado.

La relevancia más importante de la tesis es el aportar políticas y mecanismos mínimos para una mejora en la seguridad de los sitios de café internet, basándose en un sistema de apoyo que pueda ser usado por los dueños de estos sitios públicos en el DF para protegerse ellos mismos y para "garantizar" la seguridad de la información y de sus recursos informáticos.

En la realización de este proyecto y con el afán de alcanzar los objetivos planteados; en el Capítulo 1 titulado "Historia de los sitios de Café Internet", se hace una investigación del inicio de éstos sitios de manera mundial, para posteriormente enfatizar su surgimiento en México y en especial en el Distrito Federal, por ser éste el campo de estudio propuesto; asimismo se presenta de forma detallada la definición de éstos sitios explicando su estructura, así como su situación actual en México. Dado que no se puede hablar de los Café Internet, sin hablar a su vez de Internet y la manera en que interconectan los equipos de cómputo, en éste capítulo se incluyen los tipos de Redes, así como las capas del modelo OSI concluyendo con los protocolos de red más importantes en el mercado de la tecnología de información.

El Capítulo 2 titulado "Análisis de la Seguridad Informática actual en los sitios de Café Internet en la Ciudad de México", define el concepto de Seguridad Informática haciendo énfasis en su importancia en estos sitios, recopilando las principales amenazas y riesgos en Internet, como son: virus, spyware, phishing, hackers, dialers, spam, entre otros. Hacia el final de éste capítulo se muestra la metodología seguida para conocer el nivel de seguridad que guardan los sitios de Café Internet en la ciudad de México; la cual consiste en la aplicación de dos cuestionarios, uno para administradores y otro para usuarios en las 16 delegaciones del Distrito Federal.

En el Capítulo 3 titulado "Propuestas de políticas y mecanismos de seguridad indispensables en los sitios de Café Internet", se explican algunos conceptos de

importancia, tales como: análisis de riesgos, política de seguridad y mecanismo de seguridad; los cuales deben ser considerados siempre que existe la necesidad de salvaguardar información confidencial y proteger cualquier recurso informático de las amenazas cada vez mayores en el Internet. En la parte final de este capítulo se proponen, con base en los datos obtenidos de la investigación de campo realizada en el capítulo anterior, las políticas y mecanismos de seguridad básicos y principales con los que a criterio deben contar los sitios de Café Internet para ofrecer un nivel de seguridad óptimo a sus clientes.

El Capítulo 4 titulado “Diseño y desarrollo del sistema de apoyo para mejorar el nivel de seguridad en los sitios de Café Internet” contiene la información de cómo se elaboró dicho sistema que se espera sea de gran utilidad a quien lo utilice, así mismo se explica el algoritmo de solución empleado y la explicación de motivos de la selección de las herramientas de programación seleccionadas en este proyecto.

El Capítulo 5 titulado “Pruebas y liberación del sistema” se encuentra compuesto por diversas pruebas a la aplicación desarrollada, desde su interoperabilidad con sistemas operativos Windows, hasta su eficiencia con respecto a aplicaciones ya existentes.

Capítulo 1

Historia de los sitios de Café Internet

1.1 Surgimiento de los sitios de Café Internet

En las últimas dos décadas uno de los acontecimientos más sobresalientes en el mundo, en cuestión de flujo de información, ha sido el crecimiento explosivo de la red de redes: **Internet**.

La aparición de Internet trajo consigo posibilidades hasta entonces desconocidas para la creatividad humana, el acceso a la información y la comunicación internacional. A pocos años de su aparición, Internet ha evolucionado de una manera impresionante, logrando con ello, inmiscuirse en la vida del ser humano, reduciendo el tiempo y la distancia en el desarrollo de nuestras actividades; siendo su principal función hasta el momento la búsqueda de la información, de ahí que también se le conozca como la **"supercarretera de la información".**

Una de las principales virtudes de Internet en la actualidad es la eliminación de las diferencias de tiempo, que nos permite incluso la comunicación en tiempo real.

El crecimiento tan acelerado de Internet, así como sus distintos usos que en la actualidad ofrece al ser humano, es precisamente lo que desencadenó el origen de los sitios de Café Internet. Estos sitios se han expandido rápidamente alrededor del mundo y se espera que sigan creciendo en forma exponencial.

El Café Internet nació en el año de 1984, al parecer el primer proyecto desarrollado en este ámbito fue realizado por Electronic Café International, en Santa Mónica California, USA. El Café Electrónico Internacional es el padre de todos, refiriéndonos a la definición conocida de cibercafé=café+Internet. Instalado como parte del festival de las artes de las Olimpiadas de L.A., estuvo en funcionamiento durante 7 semanas. Entre sus principales atractivos se encuentra la conjunción de la realidad del propio local con su realidad virtual, ofreciendo encuentros comunes a través de videoconferencias, o grandes fiestas, todo ello amenizado con los mejores DJ's del momento. Más adelante surgieron diferentes locales en otras partes del mundo. Los pioneros de los cibercafé se muestran en la tabla 1.1

En Europa	BerZyber (Berzelius Highschool), Linköping, Suecia Bytes, Belfast, Irlanda del Norte. Cyberia, Londres, Inglaterra MySTER 2000, Ámsterdam, Holanda Peak Art Cyber Café, Stockport, Inglaterra
En Norte América	Café Renaissance, San Diego Texas Café Liberty, Cambridge, Massachusetts Internet Café, Seattle, Washington Internet Café – Scranton, Pennsylvania ICON-Byte Bar&Grill, San Francisco, California Paper Moon Espresso Café – Ashland, Oregon The Light Café – Atlanta, Georgia CyberPerk, Ottawa, Ontario The Internet Café, Prince George, British Columbia Yaletown Benny's Bagels, Vancouver, British Columbia.
En Asia	Cyber Café Club, Hong Kong.

Tabla 1.1 Pioneros de los cibercafé

Otra vertiente asegura que el primer cibercafé fue el Café Cyberia, arriba mencionado que abrió sus puertas en septiembre de 1994. Su fundadora, Eva Pascoe, dice que la idea se le vino a la cabeza a principios de los años 90. Era de las pocas personas que tenía acceso a una cuenta de correo electrónico, servicio puramente académico por aquellos días; pero al no tener nadie más en su familia una dirección de correo electrónico, debía gastar cantidades considerables de dinero en cuentas telefónicas.

Un día, sentada en un café cerca de su universidad, pensó que podría ser divertido poder ir a ese establecimiento con su ordenador portátil y enviar correos mientras se tomaba un descanso en su rutina habitual. Echó un vistazo alrededor y pudo reconocer algunos amigos de los que sabía que tenían conexión a Internet desde sus casas.

Después, hablando con ellos, pensaron en cómo sería tener conexión permanente a Internet desde un café y pagar una pequeña tarifa para poder intercambiar mensajes con sus amigos y familiares, enviar correo y tener mensajería instantánea. Tres meses después, en septiembre, abrieron el primer café Internet en Londres.

Este trabajo se enfoca al estudio de la seguridad en los sitios de Café Internet en México y en específico en el Distrito Federal, por lo que conviene hablar sobre la historia de estos sitios en nuestra ciudad.

Es difícil precisar cuál fue el primer Café Internet en México, debido a la expansión acelerada de estos sitios en diversas ciudades del país y casi de manera simultáneamente, después de análisis detallados se cree que el más antiguo y por consiguiente el primer cibercafé en México es “La Noria” ubicado en Puebla, Puebla. Este cibercafé fue abierto en diciembre de 1995 por el visionario Ing. Eduardo López Nissivocia.

A continuación se presentan algunos de los cibercafés con mayor tiempo operando en el área metropolitana de la ciudad de México. Véase tabla 1.2.

Interlomas Cybercafé	Plaza Interlomas
Club Internet	Echegaray, Estado de México
Ragnatela	Santa Fe

Tabla 1.2 Cibercafés más antiguos de la Ciudad de México

Otros que tuvieron mucho éxito y que desaparecieron por la competencia desatada a su alrededor fueron los que se muestran en la tabla 1.3.

Ciberpuerto,	Colonia Condesa
Novanet	Colonia Condesa

Tabla 1.3 Cibercafés de la ciudad de México desaparecidos por la competencia

Otros que han podido sobrevivir por adaptarse a los cambios del mercado y por elegir puntos geográficos estratégicos, son los que se muestran en la tabla 1.4:

Nombre	Fecha de fundación	Ubicación
- Bits café y canela	abril de 1998	Zona Rosa
- Javachat Café	mayo de 1998	Zona Rosa
- PC Works	mayo de1997	Naucalpan, Estado de México
- Internet Station	1998	Polanco

Tabla 1.4 Cibercafés sobrevivientes de la ciudad de México por su ubicación

1.2 Los sitios de Café Internet

Un cibercafé, café Internet, ciberlocal o simplemente “ciber” es un lugar comercial que permite, por medio de una tarifa determinada, obtener por un tiempo establecido acceso a la navegación en Internet y a otros servicios de la red como chat, correo electrónico, video conferencia, juegos en red, teleconferencia, entre otros. Además puede hacerse uso de aplicaciones de oficina a través de distintos programas. También es común contar con servicios de impresión de documentos, escáner, grabación de CDs o DVDs., lectores de memorias para cámaras fotográficas, entre otros.

Los sitios de Café Internet, también son un lugar de interacción, aprendizaje, de alfabetización para la sociedad y un sitio de reunión comunitaria, sobre todo entre los más jóvenes.

El Cibercafé llegó para quedarse. Es un negocio insertado en la mente del consumidor, que ha crecido exponencialmente en el período 2000-2008.

1.3 Estructura básica de un sitio de Café Internet

Los componentes básicos con los cuales debe contar cualquier Café Internet para poder ofrecer un buen servicio a sus clientes y/o usuarios y además ser competitivo en el mercado se enuncian en la tabla 1.5:

Componentes	Fundamentos
Equipos de cómputo (CPU, monitores, teclados, ratones) Hubs para redes y conectores	*Actualizados o por lo menos de una generación atrás de la actual*
Impresoras	*De dos tipos, inyección de tinta para trabajos de calidad y láser para trabajos de alto volumen*
Scanners Licencias de software (servicio y administración del negocio)	*Digitalización de documentos de los usuarios instalar equipos sin problemas legales en materia de derechos de autor*
No-brakes Reguladores de corriente	*Evitar pérdida inesperada de energía con posibles descontentos por los usuarios* *Evitar descargas eléctricas en los equipos*
Sistema de iluminación de emergencia Sistema contra incendios Sistema de seguridad con videocámaras	*Seguridad de todas las personas que se encuentren en el local*
Aire acondicionado	*Evitar sobrecalentamiento en los equipos*
Sillas Escritorios Teléfono Equipo de sonido Cafeteras	*Permitir una estancia cómoda a los usuarios*
Papelería en general Estantería	*Como parte del valor agregado y en caso de que los usuarios necesiten algún producto*

Tabla 1.5 Componentes básicos de un cibercafé

De entre los cuales en términos de la Tecnología de la Información destacan:

a) Equipos de cómputo (CPU, monitores, teclados, ratones)
b) Hubs para redes y conectores
c) Impresoras
d) Scanners
e) Licencias de software (servicio y administración del negocio)

La figura 1.1 muestra la apariencia de un Café Internet.

Fig. 1.1 Apariencia de un Café Internet

1.4 Tipo de Redes Ethernet

En 1972 comenzó el desarrollo de una tecnología de redes conocida como Ethernet Experimental- El sistema Ethernet desarrollado, conocido en ese entonces como red ALTO ALOHA, fue la primera red de área local (LAN) para computadoras personales (PCs). Esta red funcionó por primera vez en mayo de 1973 a una velocidad de 2.94Mb/s.

Las redes Ethernet están formadas por un cable común en el que conectamos todos los equipos, y cualquiera de éstos es capaz de monitorear todo el tráfico que circula por ella.

Una red del tipo Ethernet, es una red de transmisión de paquetes basadas en bus común. Al bus común se conectan todos los equipos informáticos de la red. La siguiente figura 1.2 ilustra una red Ethernet.

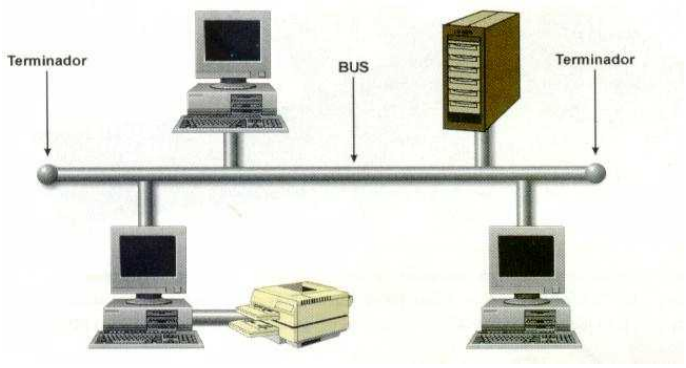


Figura 1.2 Red Ethernet

En el apéndice A se puede observar la evolución de las redes Ethernet en el transcurso de casi 25 años.

Las especificaciones formales de Ethernet de 10 Mb/s fueron desarrolladas en conjunto por las corporaciones Xerox, Digital (DEC) e Intel, y se publicó en el año 1980. Estas especificaciones son conocidas como el estándar DEC-Intel-Xerox (DIX), el libro azul de Ethernet. Este documento hizo de Ethernet experimental operando a 10 Mb/s un estándar abierto.

La tecnología Ethernet fue adoptada para su estandarización por el comité de redes locales (LAN) de la IEEE como IEEE 802.3. El estándar IEEE 802.3 fue publicado por primera vez en 1985.

El estándar IEEE 802.3 provee un sistema tipo Ethernet basado, pero no idéntico, al estándar DIX original. El nombre correcto para esta tecnología es IEEE 802.3 CSMA/CD, pero casi siempre es referido como Ethernet.

IEEE 802.3 Ethernet fue adoptado por la organización internacional de estandarización (ISO), haciendo de el un estándar de redes internacional.

Ethernet continuó evolucionando en respuesta a los cambios en tecnología y necesidades de los usuarios. Desde 1985, el estándar IEEE 802.3 se actualizó para incluir

nuevas tecnologías. Por ejemplo, el estándar 10BASE-T fue aprobado en 1990, el estándar 100BASE-T fue aprobado en 1995 y Gigabit Ethernet sobre fibra fue aprobado en 1998.

La arquitectura Ethernet provee detección de errores pero no corrección de los mismos. Tampoco posee una unidad de control central, todos los mensajes son transmitidos a través de la red a cada dispositivo conectado. Cada dispositivo es responsable de reconocer su propia dirección y aceptar los mensajes dirigidos a ella. El acceso al canal de comunicación es controlado individualmente por cada dispositivo utilizando un método de acceso probabilístico conocido como disputa (contention).

Los modos de funcionamiento de las redes Ethernet son definidos por la frase *acceso múltiple sensible a la portadora, con detección de colisiones (carrier sensing, multiple access with collision detection,* CSMA/CD) y pertenecen a la clase de redes de contienda en bus. Los métodos de contienda utilizan un medio de transmisión único para enlazar todos los hosts.

El protocolo que gestiona el acceso al medio se llama protocolo de control de acceso al medio *(médium access control, MAC).* Dado que un único enlace conecta todos los hosts, el protocolo MAC combina en una única capa las funciones de un protocolo de enlace de datos (responsable de la transmisión de paquetes sobre los enlaces de comunicación) y de un protocolo de red (responsable de la entrega de los paquetes a los **hosts)**.

Formato de la trama de Ethernet

Trama de Ethernet

Preámbulo	SOF	Destino	Origen	Tipo	Datos	FCS
7 bytes	1 byte	6 bytes	6bytes	2 bytes	46 a 1500 bytes	4 bytes

Preámbulo

Campo de 7 bytes (56 bits) que contiene una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

Estos bits se transmiten en orden de izquierda a derecha y en la ***codificación Manchester*** representan una forma de onda periódica.

SOF (Start Of Frame) Inicio de Trama

Campo de 1 byte (8 bits) que contiene un patrón de 1 y 0 alternados, y que termina con dos 1 consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de ***dirección MAC*** de destino.

Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

Dirección de destino

Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo ***multicast*** o la dirección de ***broadcast*** de la red. Cada estación examina este campo para determinar si debe aceptar el paquete.

Dirección de origen

Campo de 6 bytes (48 bits) que especifica la ***dirección MAC*** de tipo EUI-48 desde la que se envía la trama. La estación que deba aceptar el paquete conoce a través de este campo la dirección de la estación origen con la cual intercambiar datos.

Tipo

Campo de 2 bytes (16 bits) que identifica el ***protocolo de red*** de alto nivel asociado con el paquete, o en su defecto la longitud del campo de datos. Es interpretado en la capa de enlace de datos.

Datos

Campo de 46 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del ***nivel de red*** (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

FCS (Frame Check Sequence - Secuencia de Verificación de Trama)

Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC ***(control de redundancia cíclica)*** Este CRC se calcula por el emisor sobre todo el contenido de la trama, y se vuelve a calcular por el receptor para compararlo con el recibido y verificar la integridad de la trama.

1.5 Capas del Modelo OSI

Es un hecho que ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas. Sin embargo, se desarrollaron utilizando implementaciones de hardware y software diferentes. Como resultado, muchas de las redes eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre sí.

Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, tomando como punto de partida el protocolo TCP/IP elaboraron el modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) en 1984.

Los estándares aseguran mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnologías de red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un

marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.), hasta otro programa de aplicación ubicado en otro computador de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de red.

En el modelo de referencia OSI, hay siete capas numeradas (véase figura 1.3), cada una de las cuales ilustra una función de red específica. Esta división de las funciones de networking se denomina división en capas. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

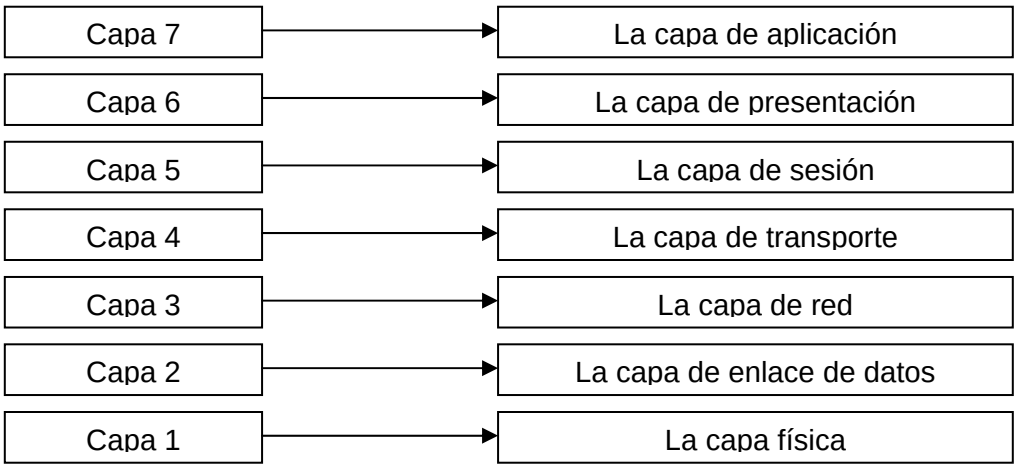


Figura 1.3 Capas del modelo OSI

Funciones de cada capa

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, presentamos una breve descripción de cada capa del modelo de referencia OSI tal como aparece en la figura 1.4.

Figura 1.4 Descripción de cada capa del modelo OSI

Capa 7: La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. Algunos ejemplos de aplicaciones son los programas de hojas de cálculo, de procesamiento de texto y los de las terminales bancarias. La capa de aplicación establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. Si desea recordar a la Capa 7 en la menor cantidad de palabras posible, piense en los navegadores de Web.

Capa 6: La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. Si desea recordar la Capa 6 en la menor cantidad de palabras posible, piense en un formato de datos común.

Capa 5: La capa de sesión Como su nombre lo indica, administra, mantiene y finaliza las sesiones entre dos hosts que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación. Si desea recordar la Capa 5 en la menor cantidad de palabras posible, piense en diálogos y conversaciones.

Capa 4: La capa de transporte segmenta los datos originados en el host emisor y los re-ensambla en una corriente de datos dentro del sistema del host receptor. El límite entre la capa de transporte y la capa de sesión puede imaginarse como el límite entre los protocolos de aplicación y los protocolos de flujo de datos. Mientras que las capas de aplicación, presentación y sesión están relacionadas con asuntos de aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.

La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte. Si desea recordar a la Capa 4 en la menor cantidad de palabras posible, piense en calidad de servicio y confiabilidad.

Capa 3: La capa de red La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Si desea recordar la Capa 3 en la menor cantidad de palabras posible, piense en selección de ruta, direccionamiento y enrutamiento es decir en donde se realizan tareas de control, de flujo y de congestionamiento.

Capa 2: La capa de enlace de datos proporciona tránsito de datos confiable, esto es, que el intercambio de datos se convierta en una comunicación efectiva a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de

errores, entrega ordenada de tramas y control de flujo. Si desea recordar la Capa 2 en la menor cantidad de palabras posible, piense en tramas y control de acceso al medio.

Capa 1: La capa física La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares son definidas por las especificaciones de la capa física. Si desea recordar la Capa 1 en la menor cantidad de palabras posible, piense en señales y medios.

1.6 Protocolos

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente.

Una definición técnica de un protocolo de comunicaciones de datos es: un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos. La capa n de un computador se comunica con la capa n de otro computador. Las normas y convenciones que se utilizan en esta comunicación se denominan colectivamente protocolo de la capa n.

En la tabla 1.6 se muestra la pila TCP/IP y otros protocolos relacionados con el modelo OSI original:

7	Aplicación	HTTP, DNS, SMTP, SNMP, FTP, Telnet, SSH y SCP, NFS, RTSP, Feed, Webcal
6	Presentación	XDR, ASN.1, SMB, AFP
5	Sesión	TLS, SSH, ISO 8327 / CCITTX.225, RPC, NetBIOS
4	Transporte	TCP, UDP, RTP, SCTP, SPX
3	Red	IP, ICMP, IGMP, X.25, CLNP, ARP, RARP, BGP, OSPF, RIP, IGRP, EIGRP, IPX, DDP
2	Enlace de datos	Ethernet, Token Ring, PPP, HDLC, Frame Relay, RDSI, ATM, IEEE 802.11, FDDI
1	Físico	cable, radio, fibra óptica

Tabla 1.6 Pila TCP/IP y otros protocolos relacionados con el modelo OSI original

Capítulo 2

Análisis de la Seguridad Informática Actual en los Sitios de Café Internet en la Ciudad de México

Concepto de seguridad informática y su importancia en los sitios de Café Internet

Debido a que Internet se ha convertido en una herramienta indispensable para el desarrollo de distintas actividades del ser humano, como son: búsqueda de información, correo electrónico, chat, educación, entre otros; las empresas, así como las personas tienen la necesidad de proteger su información, ya que si bien es cierto que Internet desde sus orígenes ha ofrecido muchas ventajas al hombre que le facilitan su vida, también le han provocado riesgos y amenazas importantes a su información por **ser un foco de información sin censura de ninguna clase**.

Los riesgos y amenazas que afectan a todos los que hacen uso de Internet se potencian cuando, por motivos personales tienen que recurrir al uso de sitios públicos como los Café Internet en donde exponen su información a personas ajenas a la información, también conocidas como piratas informáticos, quienes buscan tener acceso a la información para modificar, sustraer o borrar datos, porque la gran mayoría de estos sitios no ofrecen ningún nivel de seguridad a sus clientes. Además al checar su cuenta de mail o acceder a cualquier otra página utilizando una contraseña, puede resultar arriesgado o peligroso ya que hay computadoras que cuentan con programas que guardan automáticamente las contraseñas. Éstos no son caros, exclusivos o difíciles de conseguir. Por tal motivo es importante el tema de la seguridad informática en dichos sitios, y es justamente el término de seguridad informática lo que se procede a definir en este capítulo.

En términos generales la seguridad informática puede entenderse como aquellas reglas, técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

La seguridad informática consiste entonces en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que la información que se considera importante no sea fácil de acceder por cualquier persona que no se encuentre acreditada.

Para comprender con más claridad el concepto de seguridad informática y sus alcances conviene mencionar sus activos, es decir, los elementos que la seguridad informática tiene como objetivo proteger. Son tres los elementos que conforman los activos y se muestran en la tabla 2.1.

Activos de la seguridad informática	
Información	Es el objeto de mayor valor para una persona u organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.
Equipos que la soportan	Software, hardware y organización.
Usuarios	Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

Tabla 2.1 Activos de la seguridad informática

Para la mayoría de los expertos o especialistas el concepto de seguridad informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debemos de dotar de cuatro características al mismo:

- **Integridad:** La información no puede ser modificada por quien no está autorizado.
- **Confidencialidad:** La información sólo puede ser legible para los autorizados.
- **Disponibilidad:** La información debe estar disponible cuando se necesita.
- **Irrefutabilidad (no-Rechazo):** Que no se puede negar la autoría.

Dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad lógica y seguridad física.

2.1.1 Seguridad física

Es muy importante ser consciente que por más que una empresa sea la más segura desde el punto de vista de ataques externos: hackers, virus, keyloggers, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático, lo que puede derivar que para un atacante sea más fácil lograr tomar y copiar una cinta de alguna sala, que intentar acceder vía lógica a la misma.

Así, la *Seguridad física* consiste en "la aplicación de barreras tangibles y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos."

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza, del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

a) Desastres naturales, incendios accidentales, tormentas e inundaciones.
b) Amenazas ocasionadas por el hombre.
c) Disturbios, sabotajes internos y externos deliberados.

En el caso de los Café Internet la seguridad física es un punto importante a considerar, ya que los equipos informáticos son muy sensibles al fuego y al humo. Se debe considerar la instalación de detectores de humo, extinguidores automáticos de incendios y sistemas de alarmas.

El polvo es abrasivo y acorta la vida útil de los medios magnéticos y de las unidades ópticas y de cintas. El polvo puede acumularse en los sistemas de ventilación y bloquear el flujo de aire, impidiendo que este se regenere.

La tabla 2.2 contiene algunas sugerencias para mejorar la seguridad física de la instalación en los cibercafés.

Medidas para mejorar la seguridad física de la instalación de un Cibercafé
1. No deje el sistema, las unidades de cinta, las terminales o las estaciones de trabajo sin vigilancia durante largos períodos de tiempo. Conviene establecer algunas restricciones de acceso en los lugares donde se encuentren estos dispositivos.
2. No deje la consola del sistema u otros dispositivos de terminal conectados como raíz y sin supervisión alguna.
3. Sensibilice a los usuarios de los equipos informáticos sobre los riesgos que amenazan la seguridad física del equipo.
4. Guarde las copias de seguridad en una zona segura y limite el acceso a dicha zona.

Tabla 2.2 Sugerencias para mejorar la seguridad física de la instalación en los cibercafés

2.1.2 Seguridad lógica

Luego de ver como nuestro sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada.

Debido a que en un centro de cómputo el activo más importante que posee es la información, deben existir técnicas, más allá de la seguridad física, que la aseguren. Éstas técnicas las brinda la seguridad lógica.

La seguridad lógica, se refiere a la seguridad de uso de software, a la protección de datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido”, y esto es lo que debe asegurar la seguridad lógica.

Los objetivos que se plantean son los mostrados en la tabla 2.3.

Objetivos principales de la seguridad lógica
1. Restringir el acceso a los programas y archivos. 2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar ni los programas ni los archivos que no correspondan. 3. Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto. 4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro. 5. Que la información recibida sea la misma que ha sido transmitida. 6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. 7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Tabla 2.3 Objetivos principales de la seguridad lógica

Controles de acceso

Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standards and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

a) Identificación y autentificación
b) Roles
c) Transacciones
d) Limitaciones a los servicios
e) Modalidad de acceso
f) Ubicación y horario
g) Control de Acceso Interno
h) Control de Acceso Externo
i) Administración

a) Identificación y autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina **Identificación** al momento en que el usuario se da a conocer en el sistema; y **Autenticación** a la verificación que realiza el sistema sobre esta identificación.

Existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona posee: por ejemplo una tarjeta magnética.
- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
- Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
- Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
- Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar

funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

b) Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc.

En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

c) Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

d) Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

e) Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
- Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
- Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- Creación: permite al usuario crear nuevos archivos, registros o campos.
- Búsqueda: permite listar los archivos de un directorio determinado.

f) Ubicación y horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

g) Control de acceso interno

Dentro de un entorno cambiante y en un mercado altamente competitivo y globalizado como el que enfrentan actualmente las organizaciones, los riesgos amenazan día a día el logro de los objetivos, por esta razón las entidades se han visto en la necesidad de crear mecanismos que les permitan mitigar dichos riesgos y brindar una seguridad razonable al cumplimiento de sus objetivos; y es en ese punto en el que el control interno juega un papel importante pues provee de técnicas y herramientas que facilitan el monitoreo constante tanto del ambiente que la rodea como el desarrollo de operaciones al interior de las empresas. A continuación se enlistan y explican algunas de las técnicas más usadas para tener control de acceso interno.

Palabras Claves (Passwords)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

- Sincronización de passwords: consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún

mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

- Caducidad y control: este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

Cifrado de información

La información cifrada solamente puede ser descifrada por quienes posean la clave apropiada. El cifrado de información puede proveer de una potente medida de control de acceso.

Listas de Control de Accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios previamente dados de alta por el administrador que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

Límites sobre la Interfase de Usuario

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

Etiquetas de Seguridad

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

h) Control de Acceso Externo.

El control de acceso externo es un concepto de ordenador en red y conjunto de protocolos para definir como asegurar los nodos de la red antes de que estos accedan a la red. Su objetivo implica el control de acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y los dispositivos y que pueden hacer en ella. Algunas de las técnicas de control de acceso externo más utilizadas se encuentran las siguientes:

Dispositivos de Control de Puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

Firewalls o Puertas de Seguridad

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

Acceso de Personal Contratado o Consultores

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

Accesos Públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

i) Administración

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa específico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

Administración del Personal y Usuarios - Organización del Personal

Este proceso lleva generalmente cuatro pasos:

- Definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
- Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
- Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea

efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

2.2 Niveles de seguridad informática

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de **niveles de seguridad**. La seguridad absoluta no es posible, por eso solamente debemos entender que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos. Además, la seguridad informática precisa de un nivel organizativo, por lo que diremos que:

Sistema de Seguridad = TECNOLOGÍA + ORGANIZACIÓN

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commision) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La numeración actual de las Normas de la serie ISO/IEC 27000 es la que se muestra en la tabla 2.4.

ISO/IEC 27000	Fundamentos y vocabulario.
ISO/IEC 27001	Norma que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de procesos.
ISO/IEC 27002	(Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799): Código de buenas prácticas para la gestión de Seguridad de la Información.
ISO/IEC 27003	Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO/IEC 27001.
ISO/IEC 27004	Métricas para la gestión de Seguridad de la Información. Es la que proporciona recomendaciones de quién, cómo y cuándo realizar mediciones de seguridad de la información.
ISO/IEC 27005	Gestión de riesgos de la Seguridad de la Información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.
ISO IEC 27006: 27007	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la Seguridad de la Información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC/TR 27008	Proporcionará una guía para auditar los controles de seguridad de la norma ISO 27002:27005.
ISO/ IEC 270010	Proporcionará una guía específica para el sector de las comunicaciones y sistemas de interconexión de redes de industrias y administraciones, a través de un conjunto de normas más detalladas que comenzarán a partir de la ISO/IEC 27011.
ISO/IEC 27011	Será una guía para la gestión de la seguridad en telecomunicaciones (conocida también como X.1051)
ISO/IEC 27031	Estará centrada en la continuidad de negocio.
ISO/IEC 27032	Será una guía para la cyberseguridad.
ISO/IEC 27033	Sustituirá a la ISO/IEC 18028, norma sobre la seguridad en redes de comunicaciones.
ISO/IEC 27034	Proporcionará guías para la seguridad en el desarrollo de aplicaciones.
ISO/IEC 27799	No será estrictamente una parte de la serie ISO 27000, aunque proporcionará una guía para el desarrollo de SGSI para el sector específico de la salud.

Tabla 2.4 Numeración actual de las normas de la serie ISO/IEC 27000

2.3 Principales riesgos o amenazas de seguridad informática en Internet

En el lenguaje informático, se denomina *amenaza* a la violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo), que podría efectuar una persona ó máquina, dada una oportunidad. Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes (Ver figura 2.1):

- **Interrupción:** Es un ataque contra un recurso del sistema que es destruido o deshabilitado temporalmente. Por ejemplo, destruir un disco duro, cortar una línea de comunicación o deshabilitar un sistema de consulta.
- **Intercepción:** Este es un ataque de una entidad que consigue acceso a un recurso no autorizado. Dicha entidad podría ser una persona, un programa o una computadora. Ejemplos de este tipo de ataque son interceptar una línea para obtener información y copiar ilegalmente archivos o programas que circulen por la red, o bien la lectura de las cabeceras de mensajes para descubrir la identidad de uno o más de los usuarios involucrados en una comunicación que es interceptada ilegalmente.
- **Modificación:** Este es un ataque de una entidad no autorizada que consigue acceder a un recurso y es capaz de modificarlo. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación:** Este es un ataque de una entidad no autorizada que añade mensajes, archivos u otros objetos extraños en el sistema. Ejemplos de este ataque son insertar mensajes no deseados en una red o añadir registros a un archivo.

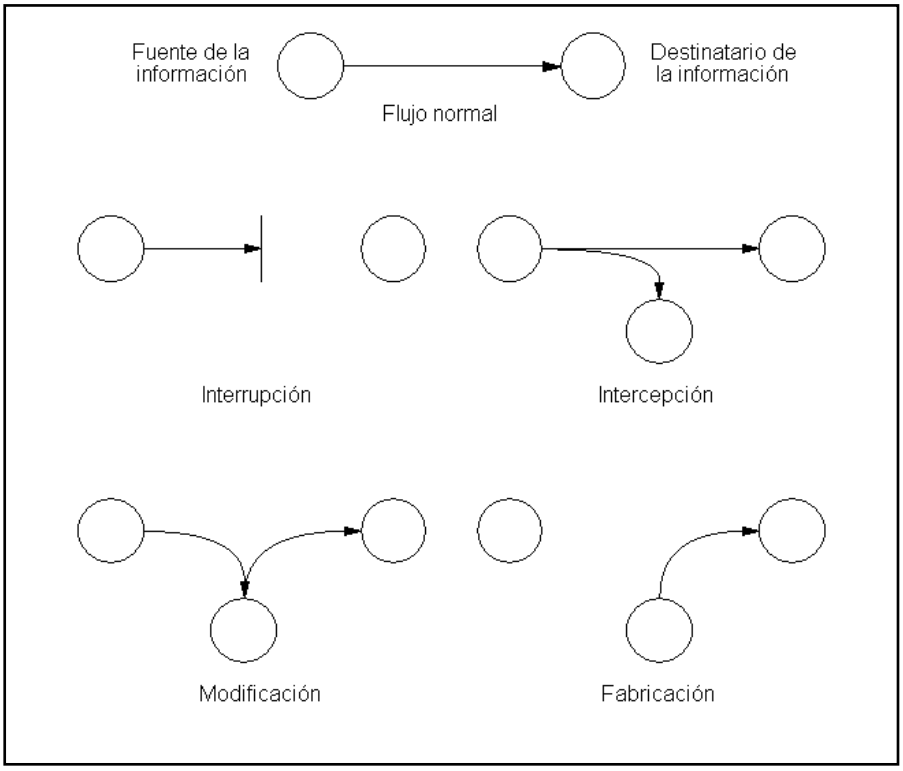


Fig. 2.1 Principales tipos de amenazas

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

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la observa, con el fin de obtener la información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más útil para obtener información de la comunicación, que puede consistir en:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los mensajes interceptados.
- **Control del volumen de tráfico** intercambiado entre las entidades interceptadas, obteniendo así información acerca de actividad o inactividad inusuales.
- **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los periodos de actividad.

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

Ataques activos

Estos ataques implican algún tipo de modificación en el proceso de transmisión de información a través de la red o la creación de un falso proceso de transmisión, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- **Re-actuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces a una cuenta dada.
- **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje “Ingresa diez mil dólares en la cuenta A” podría ser modificado para decir “Ingresa diez mil dólares en la cuenta B”
- **Degradación fraudulenta del servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes no deseados. Entre estos ataques se encuentran los de *denegación de servicio,* consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Internet fue diseñado para ser sencillo y cómodo, pero no para ser seguro. El hecho de que no existan fronteras en Internet representa ciertos riesgos, como son:

- La aprobación indebida de datos
- La presencia de algún virus (intencionada o no)

El mayor peligro para el usuario es que un pirata cibernético que vigile el tráfico de la información a través de una PC pueda apropiarse de información sensible y realizar transacciones comerciales en su provecho.

Existen varias posturas frente a esta realidad:

- Los que defienden que la información es de todos y que ésta debe circular libremente.
- Los gobiernos (como el de EU) que defienden la garantía legislativa de un buen uso.
- Los que defienden el derecho a la intimidad opinan que los mensajes electrónicos deben estar protegidos por un sistema que garantice que sólo van a leerlo sus destinatarios.

2.4 Clasificación de los diferentes problemas de seguridad en Internet (Café Internet)

Actualmente los Café Internet son el punto ideal para cometer cualquier delito informático porque la gran mayoría no cuentan ni con políticas ni con mecanismos de seguridad adecuados que permitan darle confianza a sus clientes, a esto se añade que el Internet en sí mismo es altamente inseguro.

En la tabla 2.5 se enlistan las amenazas más comunes que se encuentran latentes en el Internet y por consecuencia en los Café Internet, asimismo se da una breve explicación de los riesgos que representan y que conllevan para los usuarios de la supercarretera de la información.

Posteriormente se profundizará en ellos, con el objeto de aclarar que la palabra virus informático, ha dejado de ser la amenaza por excelencia y es solo uno de los muchos tipos de riesgos que hoy por hoy conviven con el ser humano en el cyber-espacio.

a) Malware	Es la abreviatura de "Malicious Software" (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento.
b) Spyware	Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o consentimiento del ordenador.
c) Phishing	Es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjetas de crédito, identidades, etc.
d) Virus	Es un malware que tiene por objetivo alterar el normal funcionamiento de la computadora sin el permiso o conocimiento del usuario.
e) Dialers	Se trata de un programa que marca un número de tarificación nacional (NTA) usando el módem, éstos NTA son números cuyo costo es superior al de una llamada nacional.
f) Hackers	Experto técnico en comunicaciones o seguridad, que gusta de introducirse en sistemas ajenos con el fin de conocer la profundidad de su funcionamiento interno, estudiar sus funciones o demostrar fallas en los sistemas de protección.
g) Crackers	Experto que entra en los sistemas informáticos de forma furtiva y con malas intenciones. Suele contar con tecnologías avanzadas para cometer sus acciones y es capaz de deteriorar complejos sistemas.
h) Spam	Son mensajes no solicitados y enviados comúnmente en cantidades masivas sin el permiso explícito de los receptores y frecuentemente contiene varios trucos para esquivar los filtros de spam.

Tabla 2.5 Principales amenazas en los Café Internet

A continuación se explica a detalle las características de cada una de estas amenazas.

a) Malware

Malware (del inglés **mal**icious soft**ware** también llamado **badware**) es software que tiene como objetivo infiltrarse en o dañar un ordenador sin el consentimiento informado de su dueño. Existen muchos tipos de malware, aunque algunos de los más comunes son los **virus informáticos,** los **gusanos**, los **troyanos**, los programas de **spyware / adaware** o incluso los **bots**.

Dos tipos comunes de malware son los *virus* y los *gusanos* informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismo que en algunas ocasiones ya han mutado, la diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.

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, y los sectores de arranque de los discos de 3,1/2 pulgadas. En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al mismo tiempo el código del virus. Normalmente la aplicación infectada funciona normalmente. 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.

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.

Un **programa caballo de Troya** es una pieza de 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 o puede contaminar a los equipos por medio del engaño.

Una puerta trasera(o bien Backdoor) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación. De acuerdo en 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.

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.

Los rootkit, 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.

b) Spyware

Los **programas espía** o **spyware** son un tipo del Malware cuyo concepto es un programa, que tiene la finalidad de causar perjuicios a los usuarios de sistemas informáticos. Como su nombre lo indica, son aplicaciones cuyos diseños fueron creados para espiar el comportamiento de los usuarios cuando se encuentran navegando por Internet. Este tipo

de programas recopilan información sobre una persona u organización sin su consentimiento, para distribuirla a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software.

Hay que aclarar que, aunque evidentemente tienen cierta similitud con los programas Troyanos, los Spyware no representan un peligro de manipulación ajena del sistema, ni de daños a nuestro ordenador por parte de terceros. Sus efectos son, simple y llanamente, la violación de nuestros derechos de confidencialidad de nuestros datos, así como una navegación más lenta.

Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.

Los spyware monitorean y capturan información de las actividades de los usuarios, hacia servidores donde almacenarán los datos recolectados para fines, por lo general comerciales o hasta delincuenciales y esta información es vendida a ciertos proveedores de productos o servicios que posteriormente bombardearán los buzones de correo ofreciendo equipos de cómputo, periféricos, consumibles, viajes, turísticos, pornografía, etc. Pueden tener acceso por ejemplo a: el correo electrónico y el password; dirección IP y DNS; teléfono, país; páginas que se visitan, qué tiempo se está en ellas y con qué frecuencia se regresa; qué software está instalado en el equipo y cuál se descarga; qué compras se hacen por Internet; tarjeta de crédito y cuentas de banco.

Los **Spyware** pueden contener rutinas que capturan las teclas digitadas por el usuario denominadas **keyloggers**, tales como nombres de usuario, contraseñas, números de tarjetas de crédito, fecha de expiración y hasta sus códigos secretos las cuales son almacenadas en archivos de tipo "log" para posteriormente ser enviadas al intruso vía cualquier servicio de Internet.

Principales síntomas de infección de spyware

Entre los indicadores que pueden señalar que una computadora tiene instalado spyware se encuentran los siguientes:

- Un bombardeo de anuncios de tipo pop-up.
- Cambio de la página de inicio, la de error y búsqueda del navegador.
- Barras de búsquedas de sitios como la de *Alexa, Tovar, MyWebSearch, FunWeb, etc.* que no se pueden eliminar.
- Aplicación de íconos nuevos en la bandeja de sistema (system tray) ubicada en la parte inferior de la pantalla de su computadora.
- Aparición de mensajes de error fortuitos.
- Modificación de valores de registro
- Lentitud en iniciar el computador debido a la carga de cantidad de software espía.
- La navegación por la red se hace cada día más lenta y con más problemas.
- Teclas que no funcionan (por ejemplo, cuando se trata de saltar de un casillero a otro al completar un formulario Web, la tecla “Tab” no funciona)

Pasos para disminuir el riesgo de las infecciones de spyware y/o eliminarlas

- Actualización del sistema operativo y programa de navegación de Internet.
- Descarga de programas gratuitos únicamente ofrecidos por sitios Web conocidos y confiables.
- Elegir **no** cuando sean hechas preguntas inesperadas.
- No seguir los link de e-mail que dicen ofrecer software anti-spyware.
- Ajustar las preferencias del browser para limitar el uso de ventanas pop-up y cookies.
- Instalar un programa firewall personal para evitar que los usuarios indeseados tengan acceso a su computadora.

Para poder eliminar el spyware de una computadora, se recomiendan los siguientes puntos:

- Realizar una exploración completa en la computadora con un software antivirus.

- Ejecutar programas anti-espía legítimos específicamente diseñados para remover spyware.

La siguiente tabla 2.6 muestra los programas anti-espía más comunes.

Programas anti-espía más comunes
✓ Adaware de LavaSoft
✓ Spysweeper de Webroot
✓ PestPatrol
✓ Spybot Search and Destroy

Tabla 2.6 Programas anti-espía más comunes

c) Phishing

El término **phishing** proviene de la palabra en inglés *"fishing" (pesca)* haciendo alusión al acto de pescar usuarios mediante formas cada vez más sofisticadas, y de este modo obtener información financiera y contraseñas. También se dice que el término es la contracción de *"password harvesting fishing" (cosecha y pesca de contraseñas)*.

La primera mención del término *phishing* data de enero de 1996 en grupo de noticias de hackers, aunque el término apareció tempranamente en la edición impresa del boletín de noticias hacker *"2600 Magazine"*. Este término fue adoptado por *crackers* que intentaban "pescar" cuentas de miembros de AOL; *ph* es comúnmente utilizado por hackers para sustituir la *f*, como raíz de la antigua forma de hacking conocida como "phone phreaking"

Es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

Quienes comenzaron a hacer phishing en AOL durante los **años 1990** solían obtener cuentas para usar los servicios de esa compañía a través de números de tarjetas de crédito válidos, generados utilizando **algoritmos** para tal efecto. Estas cuentas de acceso a AOL podían durar semanas e incluso meses. En 1995 AOL tomó medidas para prevenir este uso fraudulento de sus servicios, de modo que los crackers recurrieron al phishing para obtener cuentas legítimas en AOL.

El phishing en AOL estaba estrechamente relacionado con la comunidad de **warez** que intercambiaba **software pirateado**. Un cracker se hacía pasar como un empleado de AOL y enviaba un mensaje instantáneo a una víctima potencial. Para poder engañar a la víctima de modo que diera información confidencial, el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura". Una vez que el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y utilizarla para varios propósitos criminales, incluyendo el **spam**. Tanto el phishing como el warezing en AOL requerían generalmente el uso de programas escritos por crackers, como el **AOLHell.**

En 1997 AOL reforzó su política respecto al phishing y los warez fueron terminantemente expulsados de los servidores de AOL. Durante ese tiempo el phishing era tan frecuente en AOL que decidieron añadir en su sistema de mensajería instantánea, una línea de texto que indicaba: *"no one working at AOL will ask for your password or billing information"* ("nadie que trabaje en AOL le pedirá a usted su contraseña o información de facturación"). Simultáneamente AOL desarrolló un sistema que desactivaba de forma automática una cuenta involucrada en phishing, normalmente antes de que la víctima pudiera responder. Los phishers se trasladaron de forma temporal al sistema de mensajería instantáneo de AOL (AIM), debido a que no podían ser expulsados del servidor de AIM. El cierre obligado de la escena de warez en AOL causó que muchos phishers dejaran el servicio, y en consecuencia la práctica.

Funcionamiento del phishing

El usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de

crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos.

Para que estos mensajes parezcan aún más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estos sitios se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Entre las técnicas o métodos de phishing más comunes actualmente se encuentran:

- Engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor.
- URLs mal escritas o el uso de subdominios, como por ejemplo esta URL (http://www.nombredetubanco.com.ejemplo.com).
- Disfrazar enlaces Utilizando direcciones que contengan el carácter arroba @, para posteriormente preguntar el nombre de usuario y la contraseña. Por ejemplo, el enlace http://www.google.com@members.tripod.com/ puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los navegadores de **Mozilla** e **Internet Explorer.**
- Utilizar programas en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL legítima.
- Utilizar contra la víctima el propio código del programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta muy problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. Este ataque es conocido como

Cross Site Scripting. los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Comparación entre una página original y una página clonada con la técnica phishing

La página original cuenta con un cifrado de alta seguridad que se muestra en la propia dirección electrónica, que empieza con HTTPS. (Véase Fig. 2.2)

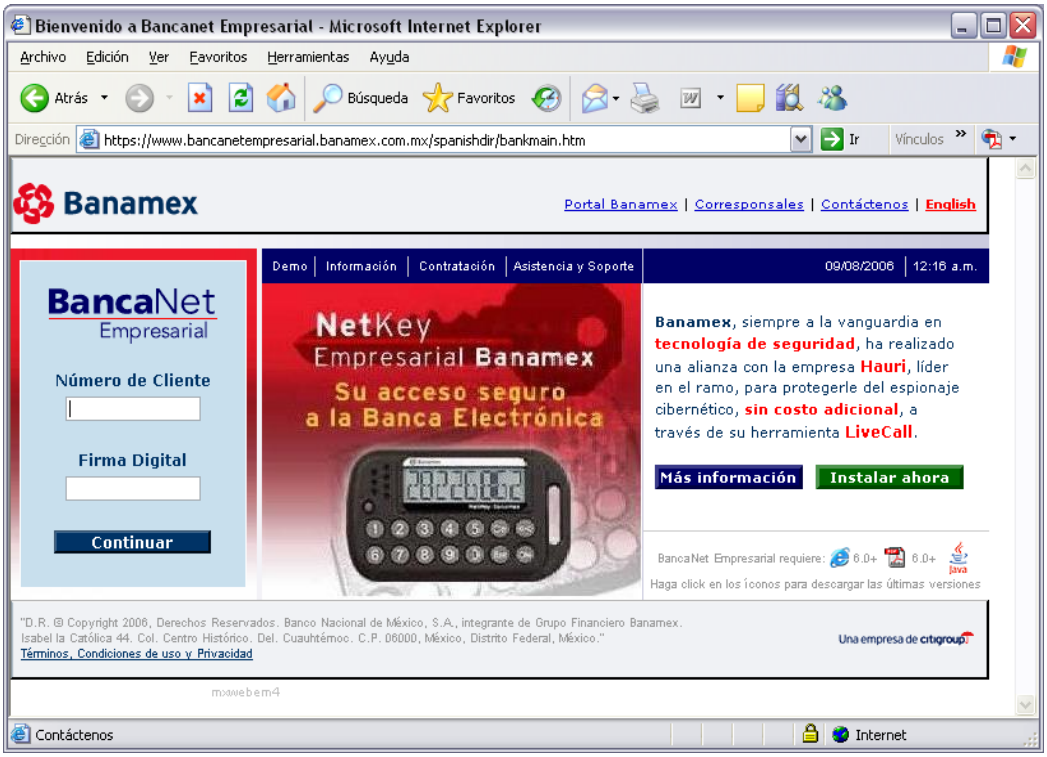


Fig. 2.2 Sitio Web Seguro (HTTPS) de BancaNet Banamex

Además, muestra su estado de seguridad mostrando un candado en la parte inferior derecha, tal como se muestra en la figura 2.3.

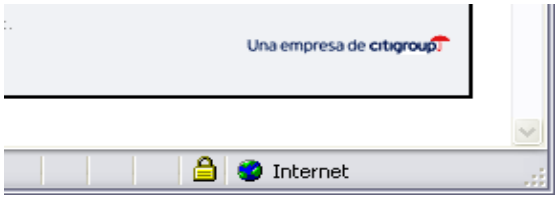


Fig. 2.3 Candado de seguridad en el sitio Web seguro

La página clonada no muestra que sea una página con cifrado de seguridad, además de ciertas irregularidades en la dirección electrónica, el **.ene.cl**, que sigue al .com.mx. Véase la figura 2.4.

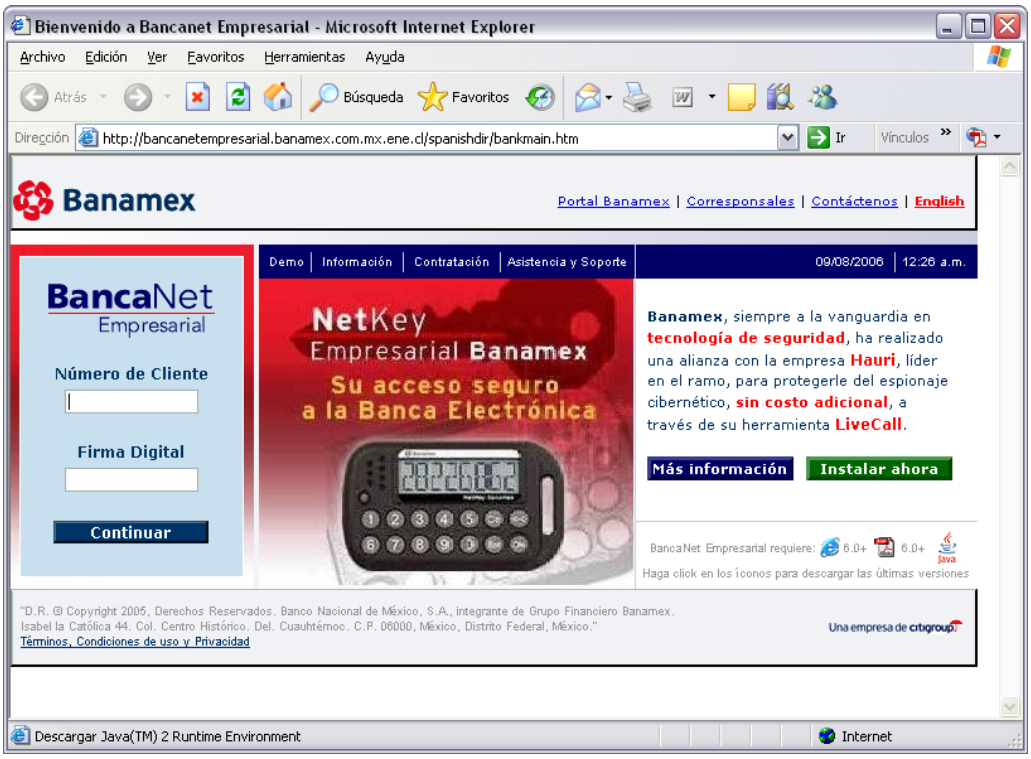


Fig. 2.4 Página clonada de BancaNet Banamex

Otra muestra es que no presenta el candado que indica que viene con el cifrado de alta seguridad, tal como se aprecia en la figura 2.5.

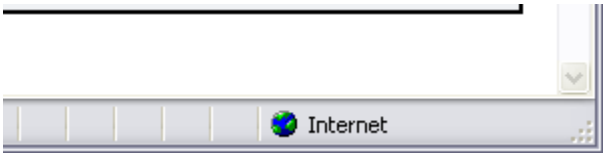


Fig. 2.5 Ausencia del candado de seguridad

Procedimientos para protegerse del phishing

Al igual que en el mundo físico, los estafadores continúan desarrollando nuevas y más siniestras formas de engañar a través de Internet. La tabla 2.7 muestra algunos sencillos pero útiles pasos para proteger y preservar la privacidad de nuestra información.

Pasos para protegerse del phishing.
i. Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje.
ii. Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones.
iii. Asegúrese de que el sitio Web utiliza cifrado.
iv. Consulte frecuentemente los saldos bancarios y de sus tarjetas de crédito desde sitios seguros y nunca públicos.
v. Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

Tabla 2.7 Pasos para protegerse del phishing.

Intentos recientes de phishing

Los intentos más recientes de phishing han tomado como objetivo a **clientes de bancos** y **servicios de pago en línea**. Estudios recientes muestran que los phishers en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un **e-mail**, falseado apropiadamente, a la posible víctima. En términos generales, esta variante hacia objetivos específicos en el phishing se ha denominado *spear phishing* (literalmente *phishing con lanza*). Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el **robo de identidad**. Algunos experimentos han otorgado una tasa de éxito de un 70% en ataques phishing en redes sociales. A finales del 2006 un **gusano informático** se apropió de algunas páginas del sitio web **MySpace** logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.

d) Virus

La tabla 2.8 muestra algunas definiciones de lo que son los virus por personas relacionadas al área de seguridad. Como se puede apreciar todas las definiciones son correctas, aún así la mejor definición sería una mezcla entre todas las expuestas.

Algunas definiciones de virus.
➢ Es un segmento de código de programación que se implanta a si mismo en un archivo ejecutable y se multiplica sistemáticamente de un archivo a otro.
➢ Pequeño segmento de código ejecutable escrito en ensamblador o lenguaje de macro, capaz de tomar el control de la máquina o aplicación en algún momento y auto replicarse, alojándose en un soporte diferente al que se encontraba originalmente.
➢ Programa que puede modificar otros programas modificándolos para incluir una versión de sí mismo.
➢ Son programas de ordenador. Su principal cualidad es la de poder auto replicarse o auto reproducirse. Intentan ocultar su presencia hasta el momento de su explosión y alteran el comportamiento y rendimiento del ordenador.
➢ Los virus tienen la misión que le ha encomendado su programador, con lo que sería difícil decir que los virus tienen una misión común. Lo único que tienen de parecido es que deben pasar desapercibidos el máximo tiempo posible para cumplir su misión. Si son detectados, el usuario puede eliminar el virus con algún programa antivirus y controlar el contagio.

Tabla 2.8 Algunas definiciones de virus informáticos

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el consentimiento del usuario. Los virus son programas que se replican y se ejecutan por si mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de éste.

Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina (playload) con distintos

objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando de, manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en un disco, con lo cual el proceso de replicado se completa.

Clasificación de los virus

Los virus se clasifican según lo infectado y según su comportamiento.

Según lo infectado

Según algunos autores existen, fundamentalmente dos tipos de virus:

a) Aquellos que infectan archivos. A su vez éstos se clasifican en:

   - Virus de acción directa. En el momento en el que se ejecutan, infectan a otros programas.
   - Virus residentes. Al ser ejecutados, se instalan en la memoria de la computadora. Infectan a los demás programas a medida que se accede a ellos. Por ejemplo, al ser ejecutados.

b) Los que infectan al sector de arranque. Recordemos que el sector de arranque es lo primero que lee el ordenador cuando es encendido.

c) Los multipartite. Corresponde a los virus que infectan archivos y al sector de arranque, por lo que se puede decir que es la suma de las dos categorías anteriores.

Para otros autores, la clasificación de los virus también se divide en dos categorías, pero el criterio de clasificación es distinto:

- ✓ Virus de archivos, que modifican archivos o entradas de las tablas que indican el lugar donde se guardan los directorios o los archivos.
- ✓ Virus de sistema operativo, cuyo objetivo consiste en infectar aquellos archivos que gobiernan la computadora.

Existe una tercera clasificación, promovida por CARO (Computer Antivirus Research Organisation), para unificar la forma de nombrar los virus. En esta clasificación se atiende a la plataforma en la que actúa el virus y a algunas de sus características más importantes.

Por ejemplo, el W32/Hybris.A-mm es un virus que funciona en la plataforma win32 en su variante A (primera) que tiene capacidad *mass mailing* o de envío masivo de correo electrónico infectado.

Tipos de virus

- Worms o gusanos: Se registran para correr cuando inicia el sistema operativo ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables. Utilizan medios masivos como el correo electrónico para esparcirse de manera global.

- Troyanos: Suelen ser los más peligrosos, ya que no hay muchas maneras de eliminarlos son capaces de mostrar pantallas con palabras. Funcionan igual que el caballo de troya, ayudan al atacante a entrar al sistema infectado, haciéndose parecer como contenido genuino (salvapantallas, juegos, música). En ocasiones descargan otros virus para agravar la condición del equipo.

- Jokes o virus broma: Son virus que crean mensajes de broma en la pantalla. También pueden ejecutar el lector de CD/DVD abriéndolo y cerrándolo, o controlar el propio ratón incluso el teclado, siempre con un fin de diversión y nunca de destrucción o daño para el contenido del ordenador aunque a veces pueden llegar a ser molestos.

- Hoaxes o falsos virus: Son mensajes con una información falsa, normalmente son difundidos mediante el correo electrónico, a veces con fin de crear confusión entre la gente que recibe este tipo de mensajes o con un fin aun peor en el que quieren perjudicar a alguien o atacar al ordenador mediante ingeniería social, mensajes como *borre este archivo del equipo* es un virus muy potente pudiendo ser archivos del sistema necesarios para el arranque u otras partes importante de este.

Según su comportamiento

Los grupos principales (y más simples) de virus informáticos son:

- **Kluggers:** Aquellos virus que al entrar en los sistemas de otro ordenador se reproducen o bien se cifran de manera que tan sólo se les puede detectar con algún tipo de patrones.

- **Viddbers:** Aquellos virus que lo que hacen es modificar los programas del sistema del ordenador en el cual entran.

Además hay otros subgrupos de los anteriores grupos:

- *Virus uniformes*, que producen una replicación idéntica a sí mismos.
- *Virus cifrados*, que cifran parte de su código para que sea más complicado su análisis. A su vez pueden emplear:
    - *Cifrado fijo*, empleando la misma clave.
    - *Cifrado variable*, haciendo que cada copia de sí mismo esté cifrada con una clave distinta. De esta forma reducen el tamaño del código fijo empleado para su detección.
- *Virus oligomórficos,* que poseen un conjunto reducido de funciones de cifrado y eligen una de ellas aleatoriamente. Requieren distintos patrones para su detección.
- *Virus polimórficos*, que en su replicación producen una rutina de cifrado completamente variable, tanto en la fórmula como en la forma del algoritmo. Con polimorfismos fuertes se requiere de emulación, patrones múltiples y otras técnicas antivirus avanzadas.

- *Virus metamórficos*, que reconstruyen todo su cuerpo en cada generación, haciendo que varíe por completo. De esta forma se llevan las técnicas avanzadas de detección al límite. Por fortuna, esta categoría es muy rara y sólo se encuentran en laboratorio.
- *Sobrescritura*, cuando el virus sobrescribe a los programas infectados con su propio cuerpo.
- *Stealth* o silencioso, cuando el virus oculta síntomas de la infección.

Existen más clasificaciones según su comportamiento, siendo las citadas, parte de las más significativas y reconocidas por la mayoría de los fabricantes de antivirus.

La tabla 2.9 muestra los virus más enviados según la ICVS (Informatic control virus scanner)

Tipo	1998	2000	2003	2005
Troyanos	20%	15%	22%	25%
Gusanos	22%	20%	25%	27%
Boot	5%	1%	4%	2%
Otros	52%	64%	49%	46%

Tabla 2.9 Los virus más enviados

Eliminar virus informáticos

Aún para un experto, quitar un virus de un equipo de manera adecuada suele ser con frecuencia una tarea abrumadora si no cuenta con la ayuda de las herramientas específicas diseñadas para este fin.

A veces, incluso algunos virus están diseñados para reinstalarse automáticamente después de haber sido detectados y quitados.

Si se **actualiza el equipo** y se usan **herramientas antivirus**, puede quitar de manera permanente (y prevenir) el software no deseado.

Entre las medidas encaminadas a eliminar los virus se encuentran las siguientes:

- Diagnóstico del PC o detección de virus por algunos síntomas en él, como: se reinicia continuamente, el sistema operativo demora mucho en alzar, el disco duro reporta fallas, aparecen extensiones desconocidas, entre otras más. El primer paso después de detectado el virus, es revisar el antivirus que se encuentra actualmente instalado en el PC, si no se tiene ninguno, es recomendable instalar uno (es mejor tener solamente un antivirus instalado ya que el tener más de uno podría causar conflictos en el PC).
- El segundo paso es eliminar el virus desactivando el restaurador de sistemas por lo que existen algunos virus capaces de restaurarse inmediatamente después de cada reinicio de la PC. Para esto se debe dar clic derecho a las propiedades de mi PC y marcar la casilla de desactivar restaurar sistema o desactivar restaurar sistema en todas las unidades. Después de haber seguido los pasos anteriores se deberá reiniciar la PC pero ahora en modo a prueba de fallos, después de esto debemos pasar el antivirus.
- El tercer paso es verificar la eliminación de virus, es decir, si después de realizar los pasos anteriores, la PC ya no presenta ningún síntoma de que aún se encuentra infectada, lo más recomendable es diariamente pasar el antivirus de la PC para así reducir el riesgo de que otro virus infecte la PC.
- Visite Microsoft Update e instale las actualizaciones más recientes.
- Visite el sitio Web del fabricante de su antivirus, actualice el software y a continuación, realicé un examen exhaustivo del equipo.
- Descargue, instale y ejecute la Herramienta de eliminación de software malintencionado (para usuarios de Microsoft Windows XP o Windows 2000)

e) Dialers

Un dialer o "marcador telefónico" es un programa que marca desde un módem a una línea telefónica con costo, esto es en la mayoría de los casos para acceder a material pornográfico, Estos programas muchas veces se auto descargan y auto instalan sin que el usuario este consciente de su existencia. Algunos de estos códigos maliciosos impiden incluso la instalación de software nuevo, lo importante aquí es conocer la manera de eliminar y detectar la presencia de estos códigos maliciosos.

Los dialers no funcionan conexiones ADSL y/o cable ya que este tipo de conexiones no realiza marcado para una conexión telefñonica.

Los dialers son una manera de ganar dinero que tienen algunas páginas web de dudosa moralidad. Estas páginas suelen obligarnos a instalar un programa para tener acceso a ciertos contenidos. Estos programas se instalan en nuestro ordenador y crean un acceso a Internet por línea de teléfono, aparte del que podamos tener en nuestro sistema. El acceso a Internet de un dialer se realiza por un número de teléfono especial, de alta tarifa, un 905 o algo similar, de modo que mientras estamos conectados a Internet por esa conexión, se nos está cobrando una cantidad realmente elevada, mucho más que lo que se nos cobraría accediendo a Internet por medio de nuestra conexión habitual.

Funcionamiento de los dialers

Cuando nos conectamos a Internet a través de la línea telefónica, estamos implícitamente realizando una llamada telefónica a nuestro proveedor de Internet a través del módem de nuestro computador. El módem marca un cierto número de teléfono, que ha sido proporcionado por nuestro proveedor para configurar el acceso a Internet. El coste de realizar esta llamada a nuestro proveedor de acceso a Internet, lo conocemos ya que en el momento de contratación del servicio lo elegimos nosotros.

El dialer aprovecha este mecanismo manipulando el número marcado y cambiando el del proveedor. Al cambiar la configuración de acceso, el computador marca a un proveedor de acceso a Internet de otro país.

Muchas veces el cliente no percibe esta modificación porque su navegación no se ve afectada, sin embargo está conectado y autenticado en otro proveedor diferente al que le vendió el servicio.

El usuario puede o no darse cuenta. Algunos marcadores telefónicos deshabilitan el volumen del parlante para no delatarse cuando corta la llamada del proveedor de servicios predeterminado y activa la llamada del dialer no deseado. También pueden llegar a ocultar el icono de conexión.

El peligro radica en que en la mayoría de los casos, la información ofrecida por las páginas Web a los usuarios que navegan es escasa:

- No ofrecen términos y condiciones de uso claros o los ubican en lugares poco visibles, empleando otros idiomas, letra de tamaño muy reducido o colores que no facilitan su lectura.
- No se avisa de su instalación en la página que lo suministra.
- Saturan al usuario y únicamente insisten en que debe hacerse clic en <Si> o en <Aceptar> en determinada ventana emergente (pop up), esto como requisito para tener acceso a cierto contenido o para cargar el "visor de contenidos" que dicho en otras palabras, es el mismo programa dialer.
- En algunos casos extremos, se aprovechan de vulnerabilidades del navegador para instalarse en el sistema sin intervención del usuario.
- Hace una reconexión a Internet sin previo aviso, o lo intenta.
- No se informa del alto coste que va a suponer esa conexión.

La tabla 2.10 resume las principales consecuencias para un usuario que puede tener instalado un dialer:

Consecuencias por tener instalado un dialer
1. Factura telefónica con llamadas no autorizadas y por un alto valor. 2. La creación de un nuevo acceso telefónico. 3. La modificación del acceso telefónico a redes que el usuario utiliza habitualmente para sus conexiones de manera que, cada vez que sea ejecutado, el número marcado no sea el correspondiente al proveedor de servicios de Internet del usuario, sino el de un número internacional. 4. Caídas frecuentes y repentinas en el acceso a Internet. 5. Escuchar conversaciones y voces en otros idiomas.

Tabla 2.10 Principales consecuencias de tener instalado un dialer

Medidas preventivas para no ser víctima de los dialers

Como la configuración del acceso a Internet es una actividad que se realiza sobre el computador personal, corresponde a cada uno de nosotros como usuarios establecer las medidas de protección más adecuadas. He aquí algunas de ellas:

- No dejar el módem del computador conectado a la red telefónica básica si no va a navegar.
- No dejar el módem del computador conectado a la red de telefonía básica como respaldo cuando se tiene otro tipo de conexión.
- Fijarse en el número que marca el módem cuando aparece la ventana de conexión de acceso a Internet. Compruebe de manera periódica que el número a través del cual se va a hacer conexión es realmente el contratado.
- Ser precavido cuando se navega en Internet y no aceptar la instalación o descarga de archivos si se desconoce su propósito.
- Desconfiar de la publicidad que ofrece “absolutamente gratis” servicios que normalmente son de pago.
- No silenciar el altavoz del módem, de esta manera se puede monitorear la actividad del mismo y oír si se produce el marcado de un número nuevo mientras está conectado a Internet.
- Configurar el navegador en el nivel más alto de seguridad que sea permitido.

Algunos de los tipos de dialers, no permiten ser desinstalados fácilmente o requieren de programas específicos para hacerlo, por esto es recomendable:

- Hacer uso de programas llamados Anti dialers, para bloquear marcadores telefónicos. Emplear uno que detecte y remueva posibles programas maliciosos que hayan podido instalarse sin su consentimiento.
- Utilizar herramientas de seguridad para proteger el computador.

Programas Anti-marcadores telefónicos (Anti-dialers)

Hay tres aspectos sobre los que se basan estos programas para acceder al módem:

1. La aplicación que realiza el marcado
2. La conexión de acceso telefónico a redes
3. El número de teléfono.

En la actualidad hay varios programas Anti-dialers que se pueden descargar de Internet de forma gratuita.

f) Hackers

Los piratas ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Llegando al año 2000, los piratas se presentan con un **cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica.**

Originalmente el término hacker se asocia a una persona entusiasta en alguna disciplina pero se ha vuelto término casi exclusivo del mundo computacional.

El hacker es un individuo que ansía conocimientos, disfruta explorando los detalles de un sistema operativo o un lenguaje de programación, programa constantemente (incluso obsesivamente), disfruta más programando que sólo haciendo teorías de

programación y disfruta del reto intelectual de vencer limitaciones buscando constantemente aumentar sus capacidades.

La palabra hacker proviene de “hack” hachar en inglés, término que se utilizaba para describir el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.

La figura 2.6 muestra el glider, emblema del hacker.

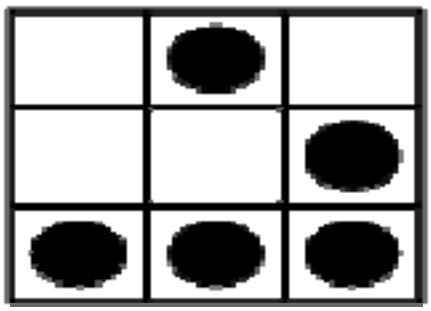


Figura 2.6 Emblema del hacker

Se dice que el término Hacker surgió de los programadores de Massachussets Institute of Technology (MIT) que en los años 60, por usar hacks, se llamaron así mismo hackers, para indicar que podían hacer programas mejores y aún más eficaces, o que hacían cosas que nadie había podido hacer.

Los hackers no son piratas. Los que roban información son los crackers. En este sentido, se suele decir que el sistema GNU/Linux ha sido creado y es mantenido por hackers. GNU/Linux es el sistema operativo nacido como consecuencia de la unión de GNU y de Linux. El kernel (o núcleo) del sistema, Linux, fue creado por el hacker *Linus Torvalds* y dio el nombre a este sistema al mezclar su primer nombre con el del sistema operativo Unix. Si bien esta definición es bastante artificial ya que ni *Linus Torvalds* ni ninguno de los principales desarrolladores del kernel Linux se han referido a si mismos como Hackers.

Dentro de los hackers hay subespecies, existen tres criterios para clasificarlos, según su ética; esta el hacker de sombrero blanco, el hacker de sombrero negro y el hacker de sombrero gris. La tabla 2.11 contiene las características principales de cada tipo.

Hacker de sombrero blanco	Es el administrador de sistemas, o el experto de seguridad, que tiene una ética muy alta y utiliza sus conocimientos para evitar actividades ilícitas.
Hacker de sombrero negro	Que algunos prefieren llamar cracker, es quien disfruta de penetrar en los sistemas de seguridad y crear software dañino (Malware)
Hacker de sombrero gris	No se preocupa mucho por la ética, sino por realizar su trabajo, si necesita alguna información o herramienta y para ello requieren penetrar en un sistema de cómputo, lo hace, además disfruta poniendo a prueba su ingenio contra los sistemas de seguridad, sin malicia y difundiendo su conocimiento, lo que a la larga mejora la seguridad de los sistemas.

Tabla 2.11 Tipos de hacker y sus características

Se distinguen 4 pasos importantes que todo hacker pone en práctica para llevar a cabo sus intenciones. Éstos son:

- Introducirse en el sistema que se tenga como objetivo.
- Una vez conseguido el acceso, obtener privilegios de root (superusuario)
- Borrar las huellas.
- Poner un sniffer para conseguir logias de otras personas.

Ideología de un hacker

Oscuros, malvados, desequilibrados, los hackers tienen mala prensa. Su nombre es sinónimo de **criminal**, cuando no **terrorista cibernético.** Pero si buceamos en su historia, descubrimos que muchas cosas cotidianas, empezando por nuestro ordenador, no existirían sin ellos. Los famosos estudiosos e investigadores pioneros de los virus de computadoras *Rob Rosenberg* y *Ross Rosenberg,* afirman categóricamente: "La revolución de la computación ha sido lograda gracias a los hackers." Por eso es importante resumir en diez puntos la ideología de éstos **entusiastas exploradores de los sistemas informáticos.** Así pues, los diez principios que rigen a los hackers son los siguientes:

1. Nunca destroces nada intencionalmente en la computadora que estás hackeando.
2. Para formar parte de este gremio es importante que estés permanentemente conectado a la red y en constante comunicación con los hackers, ya sea por vía e-mail o a través de las convenciones.
3. Por nada del mundo dejes tu dirección real, tu nombre o tu teléfono en ningún sistema, ya que alguien puede usar esa información y hacer mal uso de ella.
4. Ten cuidado a quien le pasas información. De ser posible mejor no lo hagas si no conoces a la persona o los fines a que tiene destinado ese archivo.
5. Un hacker debe proponer cambios tecnológicos, para que cada vez sean más los interesados en ellos, ya que su deber es ayudar a las empresas a verificar si los sistemas y las redes son efectivamente seguros.
6. Respeta y protege la privacidad.
7. Comparte los datos y el software, ya que un hacker es todo aquel que trabaja con gran pasión y entusiasmo por lo que hace.
8. Promueve el derecho a las comunicaciones de todas las personas y en todo el mundo.
9. Pon a prueba la seguridad y la integridad de todos los sistemas informáticos a tu alcance.
10. Su misión: crea arte y belleza en tu computadora. La idea es innovar nuevos programas que faciliten la vida de los usuarios.

g) Crackers

Cracker viene del inglés crack (romper) y justamente es lo que ellos hacen. Saben más o menos lo mismo que los hackers pero no comparten la ética. Por consiguiente no les importa romper una arquitectura o sistema una vez dentro, ni tampoco borrar, modificar o falsificar algo; es por eso que la teoría habla de que: "los hackers son buenos y los crackers malos".

Un cracker es aquélla persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, comienza a investigar la forma de bloquear protecciones hasta lograr su objetivo.

Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas Web de Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Obviamente que antes de llegar a ser un cracker se debe ser un buen hacker. Asimismo cabe mencionar que no todos los hackers se convierten en crackers.

h) Spam

Spam es todo aquel correo electrónico que contiene publicidad que no ha sido solicitada por el propietario de la cuenta de e-mail. El spam puede clasificarse como un tipo de correo electrónico no deseado.

La actividad de los spammers – aquéllos sujetos que se encargan de generar el spam – es considerada poco ética e incluso ilegal en muchos países.

Por extensión, spam también se aplica a todo tipo de método de publicidad engañosa, no solicitada u oculta.

Actualmente, se calcula que entre el 60 y el 80 % de los mails (varios miles de millones de mails por día) que se envían no son solicitados, o sea, spam. El spam es perjudicial para todos, hasta para la empresa que lo envía.

Aunque hay algunos spammers que te envían solamente un mensaje, también hay muchos que te bombardean todas las semanas con el mismo mensaje con archivos adjuntos.

El spam es un fenómeno que va en aumento día a día, y representa un elevado porcentaje del tráfico de correo electrónico total. Además, a medida que surgen nuevas soluciones y tecnologías más efectivas para luchar contra el spam, los spammers se vuelven a su vez más sofisticados, y modifican sus técnicas con objeto de evitar las contramedidas desplegadas por los usuarios.

Los spammers utilizan distintas técnicas, algunas de ellas altamente sofisticadas, como las siguientes:

- Listas de correo: el spammer se da de alta en la lista de correo, y anota las direcciones del resto de miembros.
- Compra de bases de datos de usuarios a particulares o empresas: aunque este tipo de actividad es ilegal, en la práctica se realiza, y hay un mercado subyacente.
- Uso de robots (programas automáticos), que recorren Internet en busca de direcciones en páginas web, grupos de noticias, weblogs, etc.
- Técnicas de DHA (Directory Harvest Attack): el spammer genera direcciones de correo electrónico pertenecientes a un dominio específico, y envía mensajes a las mismas. El servidor de correo del dominio responderá con un error a las direcciones que no existan realmente, de modo que el spammer puede averiguar cuáles de las direcciones que ha generado son válidas. Las direcciones pueden componerse mediante un diccionario o mediante fuerza bruta, es decir, probando todas las combinaciones posibles de caracteres.

Precauciones y acciones que cualquier usuario de correo electrónico debe tener en cuenta para evitar el spam.

- ✓ Habilitar la protección contra correo no deseado de su proveedor de correo electrónico: Los grandes proveedores de casillas de emails como Yahoo!, Google, AOL y Microsoft poseen filtros contra correos basura relativamente efectivos. Uno puede elegir el nivel de protección que desea y si quiere que los correos que considera spam sean eliminados directamente.
- ✓ No "exponer" la dirección de email a ajenos. Añadir la dirección de email personal a sitios en Internet (como blogs, foros, etc), exponen a que esta sea capturada por spammers y la incluyan en listas para luego enviarle publicidad. Al enviar emails, use la CCO (Copia Carbón Oculta o BCC en inglés) para enviar a múltiples personas el mismo email y debe también alertar a sus conocidos sobre esto. Cuando envía un email a múltiples usuarios usando simplemente CC (Copia Carbón), expone su dirección y la dirección de decenas de sus conocidos; si esa lista de contactos llega a usuarios malintencionados, puede ser capturada para enviar publicidad. Las cadenas de emails con chistes, noticias interesantes o pedidos de ayuda, son una mina de oro para spammers que buscan direcciones personales.
- ✓ Debe tener cuidado con los programas que instala. Muchas aplicaciones capturan las direcciones de email que encuentra en la PC para luego enviarles publicidad o incluso venderlas a terceros. Debe saber que la mayoría de estos programas – al instalarse – informan que tomarán esos datos personales, pero pocos leen las Políticas de Privacidad al instalarlos.
- ✓ Cuando se suscriba a sitios en Internet, debe estar seguro de que su email no será repartido o expuesto a terceros; por lo general poseen políticas de privacidad donde aclaran este punto.
- ✓ Instale programas anti-spams para ayudarlo en la tarea de revisar su casilla de correo electrónico. Mailwasher pro, el antivirus Kaspersky, entre otros, son buenos ejemplos de este tipo de programas.

2.5 Elaboración de cuestionarios para conocer el nivel de seguridad informática en los distintos sitios de Café Internet en la Ciudad de México

La figura 2.7 muestra una pequeña representación gráfica de las distintas delegaciones del Distrito Federal.

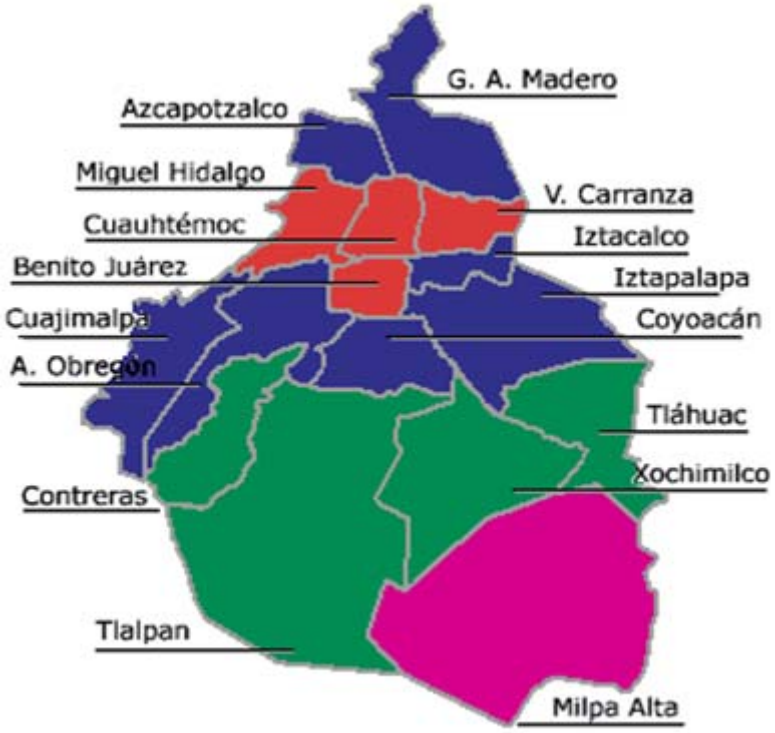


Fig. 2.7 Delegaciones políticas del Distrito Federal

Para cumplir con el objetivo de realizar un estudio sobre la seguridad informática actual en los sitios de Café Internet del Distrito Federal, recurrimos a la visita de diferentes sitios de Café Internet en distintas colonias de todas las delegaciones, en cuyo escenario se aplicaron dos instrumentos de investigación, previamente validados.

El primero es un Cuestionario de opción múltiple, con respuestas cerradas y algunas abiertas, aplicado a usuarios de los cibercafés. Este instrumento se estructuró basándose en las categorías siguientes: a) el perfil de los usuarios de los cafés internet; b) las temáticas y los servicios que son objeto de consulta y uso por parte de los cibernautas; C) las ventajas y las desventajas de los cibercafés. ***Véase Apéndice B1.1***

El segundo instrumento consiste en la aplicación de un segundo cuestionario a propietarios y/o administradores de los locales, del se han obtenido: a) cargos que ocupan las personas responsables de los Café Internet; b) acciones realizadas y servicios solicitados por los usuarios; d) actividades administrativas: publicidad, registro, tarifas, asociación, fijación de horarios y controles; e) ventajas y desventajas de sus negocios; y f) conocimiento sobre el tema de seguridad informática. ***Véase Apéndice B1.2***

Se decidió cargar estos cuestionarios a un servidor, para que, al momento de hacer las encuestas, el administrador y el usuario únicamente accedan a la página Web donde se alojan dichos cuestionarios y poderlos responder con mayor facilidad y agilidad.

Antes de poder iniciar con la aplicación de los cuestionarios, se decidió consultar en diferentes fuentes de información pública, el número de los Café Internet existentes en el Distrito Federal, para poder seleccionar una muestra representativa y entonces poder iniciar con la investigación de campo. Las fuentes consultadas fueron: el SIEM (Sistema de Información Empresarial Mexicano), la AMIPCI (Asociación Mexicana de Internet), el SAT (Sistema de Administración Tributaria), el INEGI (Instituto Nacional de Estadística y Geografía), la Sección Amarilla y Telmex, por ser este último el principal proveedor de servicio de Internet. La tabla 2.12, resume los datos obtenidos en estas fuentes.

SIEM	48
AMIPCI	53
SAT	158
INEGI	324
SECCIÓN AMARILLA	512
TELMEX	23
TOTAL	1,118

Tabla 2.12 Cafés Internet registrados en diferentes fuentes de información

Es importante destacar que en las fuentes aquí mencionadas no se tienen registrados sitios de Café Internet de todas las delegaciones, y en algunas otras se tienen registros de tan sólo 2 Café Internet en una delegación. Esto es un dato impreciso e incorrecto, pues desde luego hay muchos más sitios de Café Internet en todo el Distrito Federal, así como en cada delegación política del mismo.

Otro dato importante a destacar es que, muchos de los Café Internet publicados en estas fuentes de información, actualmente ya no están vigentes, es decir, ya no se encuentran operando. Los datos que se muestran en la tabla 2.13, han sido depurados, luego de acudir a las direcciones y realizar llamadas a los números registrados.

SIEM	48
AMIPCI	53
SAT	115
INEGI	234
SECCIÓN AMARILLA	416
TELMEX	23
TOTAL	889

Tabla 2.13 Número de Cafés Internet existentes en la Ciudad de México después de realizar la depuración

De las tablas anteriores se concluye que el número total de Cafés Internet registrados en cada fuente discrepa mucho entre una y otra, lo cual provoca un número total muy diferente. El propósito de este proyecto es analizar el nivel de seguridad actual en los sitios de Café Internet en todas las delegaciones del Distrito Federal, lo cual, dicho con anterioridad en el presente trabajo, no existen registros en dichas fuentes de Cafés Internet de todas las delegaciones. Dado que los datos obtenidos en cada fuente son muy disparejos, decidimos obtener la media de dichos números, obteniendo por resultado 148.

Para poder iniciar con nuestro propósito de analizar el nivel de seguridad informática en los sitios de Café Internet en la Ciudad de México, decidimos realizar nuestro estudio por muestreo, ya que después de consultar todas las fuentes antes mencionadas y encontrar números completamente distintos de los sitios de Café Internet registrados en cada una de ellas y al no poder tener un número exacto o preciso de los Café Internet existentes en el Distrito Federal, resulta entonces necesario hacer este estudio a solamente una muestra de dicha población, con la finalidad de “obtener una idea” del nivel de seguridad informática en estos sitios públicos.

Se entiende que la única forma de tener la certeza de que el objeto de estudio ha cubierto todos los elementos de la población, es analizar a todos y cada uno de los Café Internet en la Ciudad de México, para obtener entonces el número exacto y preciso de los que realmente operan. Este estudio exhaustivo, también llamado **Censo,** es el que entregaría el dato completo sin embargo ni las instituciones involucradas en regular o centralizar esta información lo han realizado y que, dicho sea de paso, tampoco es el propósito de este trabajo. Cuando se usa solo una parte de la población, es decir, una muestra (como en este proyecto), siempre se tendrá una aproximación de la realidad total, no la verdad exacta.

De manera general un censo es mejor que un muestreo cuando se trata de poblaciones pequeñas y cuando el investigador está dispuesto a incurrir en el costo evidentemente mayor del estudio. Sin embargo existen muchos casos en que un censo no es mejor, sino por el contrario menos exacto que un estudio por muestreo.

Por ejemplo, imaginemos que queremos conocer exactamente la calidad de un envío de fósforos. Tendríamos que abrir todas las cajas y encender todos los fósforos para estar seguros que si encienden. Al final nos quedaríamos sin fósforos útiles. En este caso evidentemente se debe hacer un muestreo y no un censo.

Otro ejemplo es cuando la realización de un censo implica mucho tiempo de trabajo, lo cual aumenta los riesgos de interferencias durante el período de estudio. La validez del trabajo se ve disminuida, pues inclusive permite que los que todavía no han sido encuestados se enteren de que en otro lugar se está realizando un estudio y que por lo tanto se preparen para cuando les toque (su respuesta no será entonces espontánea).

Ahora bien, evidentemente no siempre un tamaño grande de muestra es mejor que uno pequeño. Pues los mismos problemas señalados para un censo frente a una muestra se aplican en el caso de una muestra grande frente a una más pequeña. Por lo tanto, una muestra mayor es, en general mejor, pero existen excepciones. El tamaño de la muestra depende de muchos aspectos entrelazados, siendo los más importantes los siguientes:

a) De la necesidad de precisión del investigador
b) Del tamaño de la población

c) De la variedad al interior de la población
d) De la existencia de datos completos sobre el universo
e) De la calidad de colecta de los datos

El tamaño de la población tiene una importancia relativa pues, de manera general, a mayor población se necesita mayor tamaño de muestra. Sin embargo, desde un punto de vista práctico la precisión varía muy poco para tamaños de población diferente. Por ejemplo en Estados Unidos o Francia (200 y 50 millones de habitantes respectivamente) se pueden estimar adecuadamente los resultados de una votación nacional con una muestra igual de 300 personas.

Por lo tanto, lo importante de la muestra es su validez, lo que no depende de su tamaño o amplitud, sino de su representatividad, esto es, que represente a la población que se desea estudiar. Refleje fielmente los rasgos y características que aparecen en el grupo, en la población, en la proporción lo más aproximada posible. Esto se consigue con el muestro. El tamaño de la muestra hace referencia a la generalización de los resultados.

Ahora bien, para decidir finalmente el tamaño de muestra a ocupar para esta investigación, se recurre a la distribución normal.

La distribución normal es muy importante por lo siguiente:

a) Es la distribución a la que se aproximan la mayoría de los fenómenos físicos, químicos, biológicos y sociales.
b) Otras distribuciones bajo ciertas circunstancias se pueden aproximar a la normal.
c) Es la base para definir otras distribuciones de importancia tales como la Chi cuadrada, t de Student y F de Fisher.

La tabla 2.14 resume las características principales de la distribución normal

- Es una campana simétrica con respecto a su centro.
- La curva tiene un solo pico; por tanto es unimodal.
- La media de una población distribuida normalmente cae en el centro de su curva normal
- Debido a la simetría de la distribución normal de probabilidad, la mediana y la moda de la distribución también se encuentran en el centro; en consecuencia, para una curva normal, la media, la mediana y la moda tienen el mismo valor.
- Los dos extremos de la distribución normal de probabilidad se extienden indefinidamente y nunca tocan el eje horizontal.

Tabla 2.14 Características de la distribución normal

A continuación se muestra la forma en la cual se ha obtenido el tamaño de la muestra representativa para la investigación, tomando como base la distribución normal.

Se toma p= probabilidad de éxito =0.10

Por lo tanto, q= 1-p = 0.9.

Y proponemos un error $\varepsilon = .01$

$$n = \frac{z^2 pq}{\varepsilon^2} \quad \ldots\ldots\ldots\ldots (1)$$

De las tablas de distribución normal obtenemos el valor de z=1.96, sustituyendo valores en la ecuación (1), obtenemos.

$$n = \frac{(1.96)^2(0.1)(0.9)}{(.01)^2} = 3457.$$

Sabemos que $n_0 = \frac{z^2 pq}{\varepsilon^2}$ y que $\varepsilon = z\sqrt{(pq)} / n \sqrt{(N-n)} / (N-1)$ …… (2)

Despejando n de la ecuación (2) tenemos:

$$\varepsilon^2 = z^2 [(pq) / n] [(N-n) / (N-1)]$$

$$\downarrow$$

$$n_0$$

Entonces, $\varepsilon^2 = n_0 [(N-n) / (N-1)]$

$\varepsilon^2 (N-1) = n_0 (N-n)$

$$\varepsilon^2 = z^2 \frac{pq}{n} [(N-n) / (N-1)]$$

$$n = \frac{z^2 pq}{\varepsilon^2} [(N-n) / (N-1)]$$

$$n = n_0 [(N-n) / (N-1)]$$

$$n(N-1) = n_0 N - n_0 N$$

$$n = \frac{n_0 N}{N-1+n_0} \quad \ldots\ldots\ldots\ldots (3)$$

Conocemos ya el valor de n_0 y el valor de N, por lo que sustituyendo esos valores en la ecuación (3), obtenemos el tamaño de la muestra.

$$n = \frac{3457\ (148)}{148-1+3457} = \frac{511{,}636}{3604}$$

n = 141.96

Entonces el tamaño de la muestra para nuestra investigación es de 142 con un nivel de confiabilidad del 90%.

La aplicación de los cuestionarios se inicio el día 11 de julio de 2007 y se concluyó el día 24 de agosto de 2007. Por conveniencia se decidió iniciar por las delegaciones más retiradas, es decir, las que se localizan al Norte de la Ciudad por ser éstas las más alejadas de los domicilios propios y por consiguiente las menos conocidas, en su mayoría totalmente desconocidas. Así que el orden a seguir fue el siguiente: 1) Gustavo A. Madero, 2) Azcapotzalco, 3) Miguel Hidalgo, 4) Cuauhtémoc, 5) Benito Juárez, 6) Venustiano Carranza, 7) Iztacalco, 8) Cuajimalpa, 9) Álvaro Obregón, 10) Magdalena Contreras, 11) Iztapalapa, 12) Coyoacán, 13) Tláhuac, 14) Xochimilco, 15) Tlalpan, 16) Milpa Alta.

Al tener que tomar una muestra aleatoria, se decidió tomar como único criterio el llegar directamente al edificio de la delegación y de ahí partir a la búsqueda de los Café Internet, donde nos pudimos percatar que hay al menos 2 cerca de la zona. De ahí nos dirigimos a las escuelas circundantes, en donde también se encontraron al menos 2 Café Internet.

La situación en las distintas delegaciones es completamente diferente. El mismo concepto de Café Internet como tal, es diferente, por lo que se trató de apegar a la definición y a las características que debe tener un Café Internet.

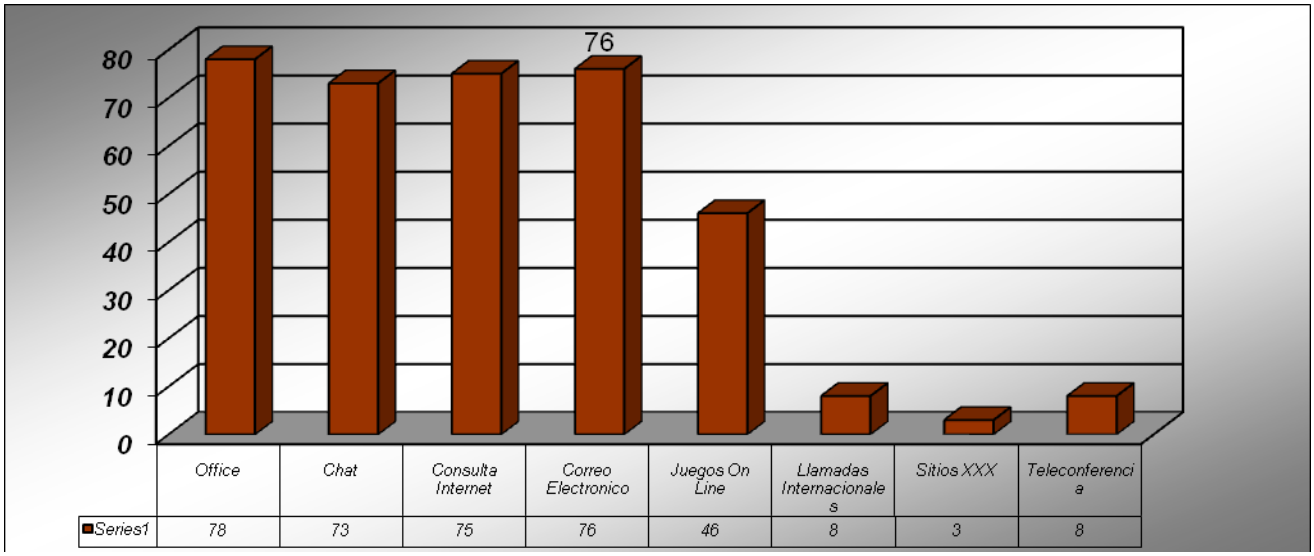
Se encontraron lugares que de ser papelerías, sitios de captura, escritorios públicos, entre otros, la gente de pronto los adaptó para convertirlos en Cibercafés, éste tipo de lugares fueron omitidos ya que por lo general solo se acondicionaban uno o dos equipos de computo, con este nuevo dato se procedió a localizar los sitios que si cuentan con los requisitos básicos para considerarse un Café Internet.

Lo que resultó un poco lamentable para la investigación es ver la falta de cooperación por parte de los administradores para este proyecto en delegaciones como Gustavo A. Madero, Azacapotzalco, Iztacalco, Cuauhtémoc, Contreras, resultado de la desconfianza que manifiestan.

Es importante señalar que el número total de los Cibercafés a los cuales se les intentó aplicar los cuestionarios es de 138, de ahí sólo los que accedieron a contestarlo y a formar parte de este proyecto fueron 78, repartidos aproximadamente de 4 Café Internet por cada delegación. En algunas más menos uno, por el tipo de zona, carencia de los mismos en la zona.

A continuación presentamos las gráficas que resumen las respuestas dadas por los administradores de dichos sitios.

La gráfica 2.1 muestra los distintos servicios solicitados y ofrecidos por los Café Internet del Distrito Federal.

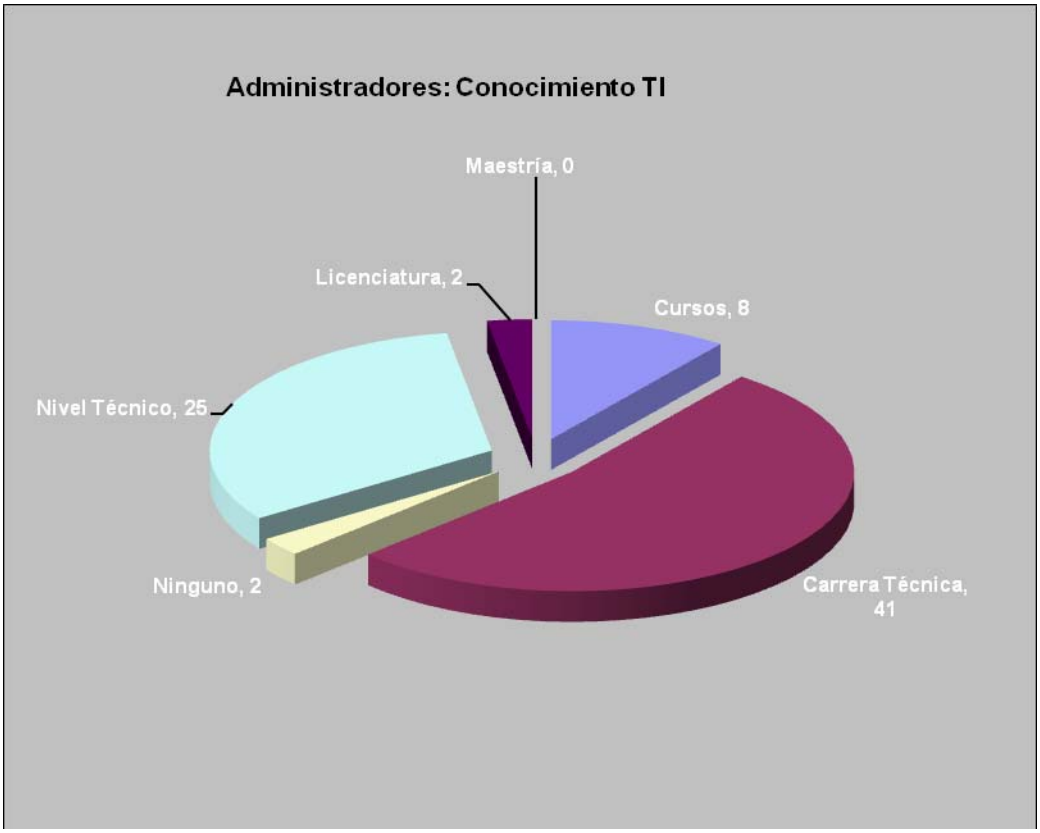


Gráfica 2.1 Distintos servicios solicitados y ofrecidos por los Café Internet en el Distrito Federal.

Office	Chat	Consulta Internet	Correo Electronico	Juegos on line	Llamadas internacionales	Sitios XXX	Teleconferencia
78	73	75	76	46	8	3	8

En esta gráfica se pueden apreciar las aplicaciones que más demanda tienen por parte de los usuarios de los Café Internet. Es claro que, la mayoría de las personas que acuden a estos sitios lo hacen en busca de la paquetería más comúnmente utilizada, como es el caso de Office (Word, Excel, Power Point, etc.), pero también para realizar búsquedas de información en los buscadores más potentes del Internet (Google, Altavista, Lycos, etc), y desde luego para chatear o enviar y realizar consultas de su correo electrónico. Un dato que conviene aclarar es el de Sitios XXX, ya que el número nos parece no real ya que los que contestaron el cuestionario no fueron honestos en esta respuesta, pues aún cuando los administradores de distintos sitios nos decían que no tenían permitido el acceso a páginas XXX, en alguno o algunos equipos, la realidad era otra, pues los usuarios de dichos equipos se encontraban efectivamente visitando éstas páginas, ya que el servicio de Internet ofrecido en la mayoría de los sitios que visitamos no tiene políticas restrictivas y sus equipos tampoco.

La gráfica 2.2 muestra los porcentajes del nivel académico sobre la tecnología de información por parte de los administradores de los Cybercafés.



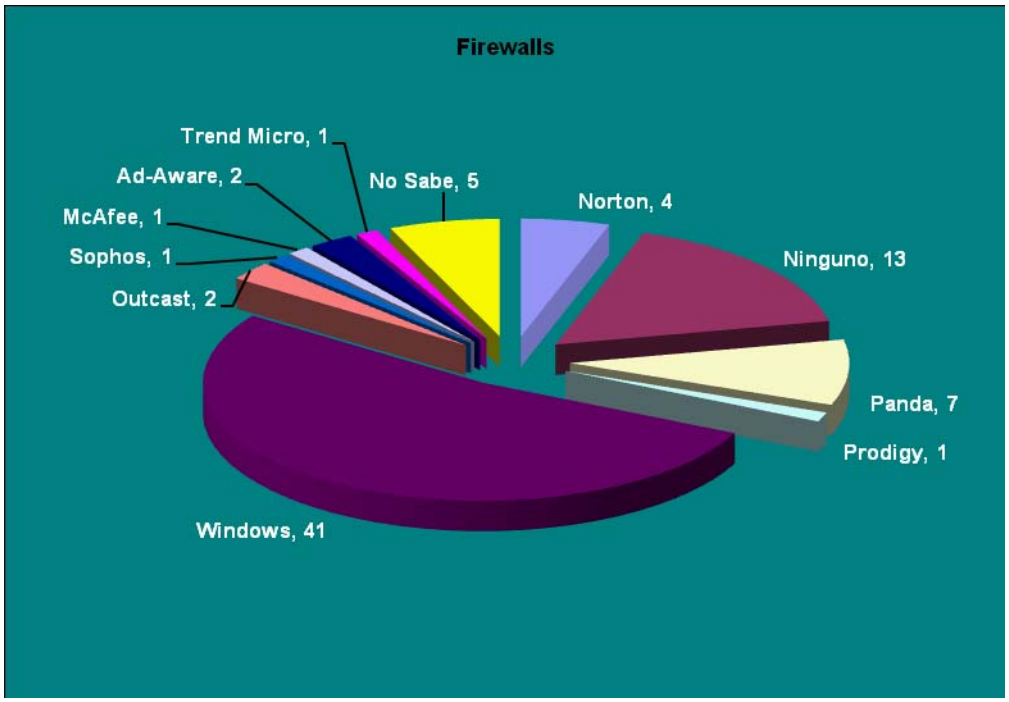
Gráfica 2.2 Porcentajes del nivel académico sobre TI de los administradores de los Café Internet

Nivel Académico TI	Administrador Cibercafé
Cursos	8
Carrera Técnica	41
Ninguno	2
Nivel Técnico	25
Licenciatura	2
Maestría	0
Total	78

Lo que mostramos en esta gráfica es el tipo de estudios (nivel académico) que han tenido los diferentes administradores de los sitios, respecto a las Tecnologías de Información, muchos de ellos son personas entre 16 y 24 años, que gustan de trabajar

con computadoras y que muchas veces se dedican a buscar información en el tiempo que pasan en el establecimiento para estar enterados de las últimas tecnologías.

La gráfica 2.3 muestra los Firewalls instalados en los distintos sitios donde se aplicaron los cuestionarios.

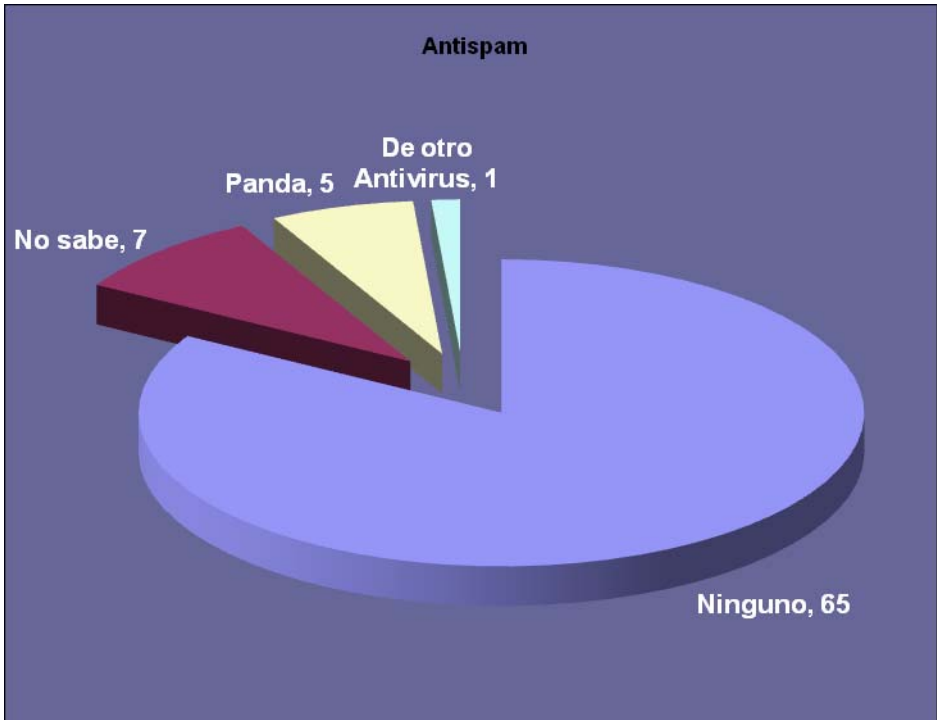


Gráfica 2.3 Firewalls instaldos en los distintos Café Internet encuestados

Firewall	Total Cibercafés
Norton	4
Ninguno	13
Panda	7
Prodigy	1
Windows	41
Outcast	2
Sophos	1
McAfee	1
Ad-Aware	2
Trend Micro	1
No Sabe	5
Total	78

Sobre los Firewalls existentes en el mercado, nos percatamos de que los administradores toman como punto de apoyo el Firewall suministrado por Microsoft en el sistema operativo de Windows, y son pocos los que incluyen productos de otra empresa. No se menosprecia la calidad de este Firewall, sin embargo Microsoft hace sistemas operativos un tanto vulnerables ante amenazas y es sugerible tener un firewall que sirva para apoyar al que viene de fábrica con Windows, para reforzar un poco más la seguridad.

La gráfica 2.4 muestra los porcentajes de los Café Internet que cuentan con alguna protección Antispam en sus equipos.

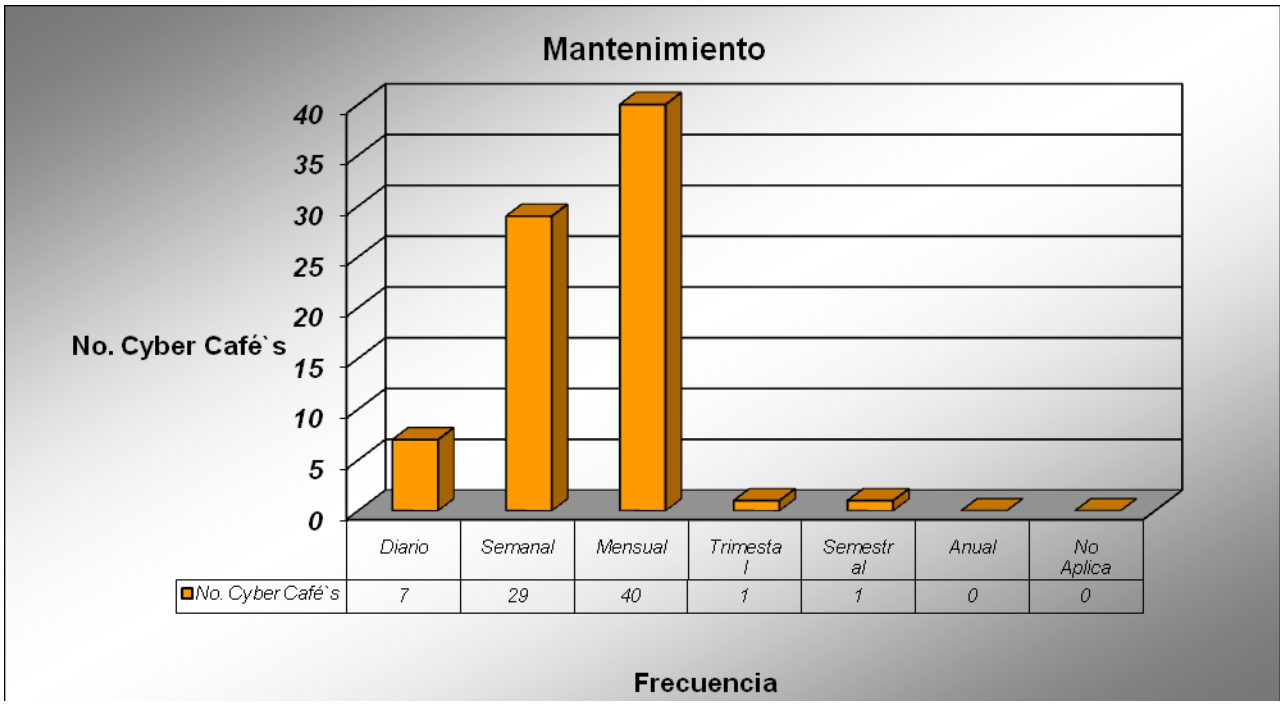


Gráfica 2.4 Cafés Internet que cuentan con software antispam en sus equipos

Anti-Spam	Total Cibercafés
Ninguno	65
No sabe	7
Panda	5
De otro Antivirus	1
Total	78

Sobre el spam, una amenaza que cada día crece más, los administradores no han puesto interés, pues consideramos que muchos de ellos no están concientes de la gravedad que representa esta amenaza para la seguridad informática. Dicho desinterés consideramos que se debe a que el spam se dedica a llenar bandejas de correos con elementos de tipo publicitario ocultando de esta manera sus verdaderas intenciones de fraude, ya que dichos mensajes comúnmente generan nuevos links que muchas veces son copias de las páginas originales que conllevan a las personas que se dedican al phishing.

La gráfica 2.5 muestra la frecuencia con la que los administradores dan mantenimiento a sus equipos informáticos.



Gráfica 2.5 Frecuencia de mantenimiento a equipos informáticos de Cybercafé.

Mantenimiento	No. Cibercafés
Diario	7
Semanal	29
Mensual	40
Trimestral	1
Semestral	1
Anual	0
No Aplica	0
Total	78

En esta gráfica podemos observar que los administradores tienen un interés por mantener en óptimas condiciones los equipos de cómputo en cuanto a desempeño se refiere, sin embargo es necesario generar mas conciencia de que la prevención ante amenazas informáticas tambien ayuda a mantener en condiciones operativas a los mismos y mas aún, evitando fraudes y preocupaciones para las personas que continuan utilizando estos equipos.

Después de haber aplicado las encuestas y de haber tratado los resultados de las mismas en las gráficas mostradas anteriormente, concluimos de manera general que los administradores de los Café Internet se han preocupado de muchas cosas, menos de la seguridad informática, y a pesar de que algunos cuentan con políticas restrictivas para los usuarios, no cuentan con los mecanismos apropiados para garantizar que dichas políticas se lleven a cabo.

Por lo tanto el tema u objetivo central de nuestro siguiente capítulo 3, es el generar propuestas de políticas y mecanismos de seguridad adecuados para proteger los equipos de los Café Internet.

Capítulo 3

Propuestas de políticas y mecanismos de seguridad indispensables en los Sitios de Café Internet

3.1 Análisis de riesgos

En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura…) que están expuestos a diferentes tipos de riesgos: los "normales" y los "excepcionales". La tabla 3.1 explica la diferencia entre estos dos tipos de riesgos.

Normales	Son aquéllos comunes a cualquier entorno.
Excepcionales	Son originados por situaciones concretas que afectan o pueden afectar a parte de una organización o a toda la misma.

Tabla 3.1 Tipos de riesgos

Para tratar de minimizar los efectos de un problema de seguridad se realiza un **análisis de riesgos**. Proceso que hace necesario responder a tres cuestiones básicas sobre nuestra seguridad (véase la tabla 3.2).

Preguntas básicas para llevar a cabo un análisis de riesgos
✓ ¿Qué queremos proteger?
✓ ¿Contra quién o qué lo queremos proteger?
✓ ¿Cómo lo queremos proteger?

Tabla 3.2 Preguntas básicas para llevar a cabo un análisis de riesgos

Un análisis de riesgos es, básicamente, un procedimiento de ayuda a la decisión. Sus resultados constituyen una guía para que la organización pueda tomar decisiones sobre si es necesario implementar nuevos mecanismos de seguridad y qué controles o procesos de seguridad serán los más adecuados.

El análisis de riesgos puede hacerse a través de un *método cuantitativo* ó de un *método cualitativo.*

El método cuantitativo es el menos usado, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del coste o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se conoce como *Costo Anual Estimado (EAC Estimated Annual Cost).*

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad especialmente entre las nuevas "consultoras" de seguridad, por ser mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, las vulnerabilidades, el impacto asociado a una amenaza y los controles o salvaguardas. La tabla 3.3 contiene una descripción de cada uno de estos elementos.

Amenazas	Por definición siempre presentes en cualquier sistema
Vulnerabilidades	Potencian el efecto de las amenazas
Impacto asociado a una amenaza	Indica los daños sobre un activo por la materialización de una amenaza
Controles o salvaguardas	Contramedidas para minimizar las vulnerabilidades

Tabla 3.3 Elementos a considerar en el análisis de riesgos a través del método cualitativo

Por ejemplo, una *amenaza* sería un pirata que va a tratar de modificar la página Web de algún sitio, el *impacto* sería una medida del daño que causaría si lo lograra, una *vulnerabilidad* sería una configuración incorrecta del servidor que ofrece las páginas, y un *control* la reconfiguración de dicho servidor o el incremento de su nivel parcheado.

Una vez que se hayan identificado los riesgos del entorno informático y analizado su probabilidad de ocurrencia, existen bases para controlarlos que son:

a) Planificación
b) Resolución de riesgos
c) Monitorización de riesgos

a) Planificación de riesgos

Su objetivo, es desarrollar un plan que controle a cada uno de los elementos perjudiciales a que se encuentran expuestas las actividades informáticas.

b) Resolución de riesgos

La resolución de riesgos está conformada por los métodos que controlan el problema de un diseño de controles inadecuado, los principales son:

1. Evitar el riesgo: No realizar actividades arriesgadas.
2. Conseguir información acerca del riesgo.
3. Planificar el entorno informático de forma que si ocurre un riesgo, las actividades informáticas sean cumplidas.
4. Eliminar el origen del riesgo, si es posible desde su inicio.
5. Asumir y comunicar el riesgo.

La tabla 3.4 ilustra los métodos de control de riesgos más comunes.

RIESGO	MÉTODOS DE CONTROL
Cambio de la prestación de servicio	➢ Uso de técnicas orientadas al cliente ➢ Diseño para nuevos cambios
Recorte de calidad	➢ Dejar tiempo a las actividades de control
Planificación demasiado optimista	➢ Utilización de técnicas y herramientas de estimación
Problemas con el personal contratado	➢ Pedir referencias personales y laborales. ➢ Contratar y planificar los miembros clave del equipo mucho antes de que comience el proyecto

Tabla 3.4 Métodos de control de riesgos más comunes

c) Monitorización de riesgos

La vida en el mundo informático sería más fácil si los riesgos apareciesen después de haber desarrollado planes para tratarlos. Pero los riesgos aparecen y desaparecen dentro del entorno informático, por lo que es necesaria una monitorización para comprobar cómo progresa el control de un riesgo e identificar como aparecen nuevos elementos perjudiciales en las actividades informáticas.

La tabla 3.5 muestra los objetivos básicos con los que cumple el análisis de riesgos.

Objetivos con los que cumple el análisis de riesgos
1. Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas
2. Llevar a cabo un minucioso análisis de los riesgos y las debilidades
3. Identificar, definir y revisar controles de seguridad
4. Determinar si es necesario incrementar las medidas de seguridad
5. Cuando se identifican los riesgos, los perímetros de seguridad y los sitios de mayor peligro, se puede hacer el mantenimiento más fácilmente

Tabla 3.5 Objetivos básicos con los que cumple el análisis de riesgos

3.2 Implementación de políticas de seguridad

El término *política de seguridad* se define como el conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indica en términos generales qué está y qué no está permitido en el área de seguridad durante la operación general de dicho sistema.

Existen dos tipos principales de políticas de seguridad que se muestran en la tabla 3.6

Prohibitiva	Si todo lo que está expresamente permitido está denegado.
Permisiva	Si todo lo que está expresamente prohibido está permitido.

Tabla 3.6 Tipos principales de políticas de seguridad

Cualquier política de seguridad debe contemplar seis elementos claves en la seguridad de un sistema informático.

a) Disponibilidad
b) Utilidad
c) Integridad
d) Autenticidad
e) Confidencialidad
f) Posesión

a) Disponibilidad

Se refiere a la necesidad de garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.

b) Utilidad

Los recursos del sistema y la información manejada en el mismo han de ser útiles para alguna función.

c) Integridad

La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.

d) Autenticidad

El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

e) Confidencialidad

La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

f) Posesión

Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control a favor de un usuario malicioso, compromete la seguridad del sistema hacia el resto de sus usuarios.

Las políticas de seguridad deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de las políticas.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, sin sacrificar su precisión.

Las políticas de seguridad deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, etc.

Parámetros para establecer políticas de seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los aspectos mostrados en la tabla 3.7.

Parámetros para establecer políticas de seguridad.
1. Efectuar un análisis de riesgos informáticos, para valorar los activos.
2. Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
3. Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
4. Identificar quien tiene la autoridad para tomar decisiones en cada departamento.
5. Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
6. Detallar explícita y concretamente el alcance de las políticas.

Tabla 3.7 Parámetros para establecer políticas de seguridad

Para implementar una política de seguridad se deben cubrir de forma adecuada los puntos anteriores, además de dividir dicha política en puntos más concretos llamados *normativas, estándares, procedimientos operativos, etc.* El estándar ISO 17799 define las siguientes líneas de actuación:

- **Seguridad organizacional:** se refiere a los aspectos relativos a la gestión de la seguridad dentro de la organización.
- **Clasificación y control de activos:** es necesario contar con un inventario de activos y definir sus mecanismos de control, así como etiquetar y clasificar la información corporativa.

- **Seguridad del personal:** se refiere a la formación en materias de seguridad, cláusulas de confidencialidad, reporte de incidentes, monitorización de personal, etc.
- **Seguridad física y del entorno:** bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos (incluyendo los humanos) de la organización y de los sistemas en sí, así como la definición de controles genéricos de seguridad.
- **Gestión de comunicaciones y operaciones:** engloba aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la protección frente a *malware,* la gestión de copias de seguridad o el intercambio de *software* dentro de la organización.
- **Controles de acceso:** definición y gestión de puntos de control de acceso a los recursos informáticos de la organización, como: contraseñas, seguridad perimetral, monitorización de accesos, etc.
- **Desarrollo y mantenimiento de sistemas:** seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de *software*, etc.
- **Gestión de continuidad de negocio:** definición de planes de continuidad, análisis de impacto, simulacros de catástrofes, etc.
- **Requisitos legales:** una política ha de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, exportación de resultados junto a todos los aspectos relacionados con registros de eventos en los recursos *(logs)* y su mantenimiento.

3.3 Implementación de un mecanismo de seguridad

A los mecanismos utilizados para implementar una política de seguridad se les denomina **mecanismos de seguridad.** Los mecanismos de seguridad son la herramienta básica para garantizar la protección de los sistemas o de la propia red.

Los mecanismos de seguridad se dividen en tres grandes grupos: de *prevención*, de *detección* y de *recuperación.*

Mecanismos de prevención

Son aquéllos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad. Por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema Unix en la red.

Mecanismos de detección

Se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como *Tripwire.*

Mecanismos de recuperación

Son aquéllos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el hardware adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar, de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad de los sistemas, Se debe enfatizar en el uso de mecanismos de prevención y de detección; la máxima popular *`más vale prevenir que curar'* se puede aplicar a la seguridad informática: para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina.

Los mecanismos de prevención más habituales en redes son los siguientes:

- *Mecanismos de autenticación e identificación*

  Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quien se dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.
  Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios.

- *Mecanismos de control de acceso*

  Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

- *Mecanismos de separación*

  Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso.

- *Mecanismos de seguridad en las comunicaciones*

  Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, se utilizan ciertos mecanismos, la mayoría de los cuales se basan en la Criptografía: cifrado de clave pública, de clave privada, firmas digitales.

3.4 Políticas y mecanismos de seguridad sugeridos para los sitios de Café Internet

Después de exponer los conceptos de política de seguridad y de mecanismo de seguridad, es necesario sugerir o proponer con base en los resultados obtenidos de nuestra investigación de campo explicada a detalle en el Capítulo anterior, lo que consideramos son las políticas y mecanismos de seguridad esenciales que todo Café Internet debe tener para contar con un "nivel de seguridad razonable".

Dichas políticas son las siguientes:

Primer política. Contar con un antivirus instalado en los equipos y mantenerlo actualizado

No basta con tener instalado un programa antivirus, es importante actualizarlo y hacerlo al menos una vez por semana. La actualización del antivirus disminuye considerablemente el riesgo de infección por alguna amenaza del Internet. Se cree que al menos entre 20 y 50 clases de virus nuevos son creados cada semana.

Es importante también realizar un chequeo completo contra virus por lo menos 3 veces al mes.

Segunda política. Instalar programas anti-espía

Como ya se explicó en el Capítulo 2, los spywares son programas parecidos a los virus pero que en lugar de afectar directamente el funcionamiento de los equipos, lo que hacen es saturarlos de publicidad, abrir ventanas emergentes, cambiar las páginas de inicio e instalar otros programas que funcionan como servidores de publicidad hacia otras redes. Los spywares se instalan por cientos en los equipos y pueden absorber todos los recursos de los mismos volviéndolos lentos e incontrolables. Esta situación puede generar además de los daños ya explicados a los equipos, la insatisfacción del usuario que llegue al sitio de Café Internet por el mal funcionamiento de los equipos, además de la probable molestia por el riesgo de contagiar sus memorias USBs con estos malwares.

Por eso es importante tener un software anti-espía instalado y ejecutarlo diariamente. Al igual que el antivirus, el antispyware debe ser constantemente actualizado para que tenga mejor eficiencia en la detección y eliminación de los espías.

Tercera política. Ejecutar el mantenimiento de software al menos 3 veces al mes

Esto debe incluir: limpieza de archivos temporales, limpieza de historial y archivos de los exploradores. Una desfragmentación de los discos duros en los equipos será útil al menos 2 veces cada 3 meses. Este mantenimiento debe incluir además la eliminación de programas que los usuarios puedan haber instalado y que no sean indispensables. (Aunque en la siguiente política se explica que es importante restringir la instalación de programas a los usuarios).

Cuarta política. Deshabilitar la utilización del usuario administrador en tus equipos

Esto limitara la instalación de software en los equipos por parte de los usuarios, así como la posibilidad de que puedan alterar o modificar la configuración básica de los mismos. Desde luego, dependiendo del software de control que se utilice, esta función puede estar ya protegida.

Otra sugerencia en este sentido es instalar un congelador en los equipos, en específico en la partición del sistema, por ejemplo el Deep Freeze. Este software lo que hace es “congelar” al disco duro, así no importa si instalan algo o si cambian la configuración de los equipos, sólo basta con reiniciarlos y vuelve a quedar como al inicio. La desventaja es que es un poco tedioso al momento de actualizar los equipos a cualquier nivel pero es muy efectivo, ligero y los usuarios no se dan cuenta de que lo tienen.

Quinta política. Control constante del ancho de banda

La velocidad de acceso a Internet es un buen indicador para saber si todo está funcionando bien o si algún equipo puede estar provocando problemas. Es importante monitorear constantemente el funcionamiento de los equipos y asegurarse de desactivar todo programa que pueda provocar un funcionamiento sospechoso, tales como Ares, Limewire, Dialers, etc.

Sexta política. Restricción absoluta a sitios con contenido para adultos

Es importante restringir el acceso a sitios XXX por parte de los usuarios, ya que no solamente pueden representar una enorme fuente de problemas como los citados arriba, sino que también atraen una gran cantidad de usuarios maliciosos que lejos de incrementar las ganancias, pueden diluirlas en gastos de mantenimiento.

Séptima política. Control de acceso

En el tema de control de acceso se puede solicitar como clave de acceso un número de identificación oficial del usuario que va a hacer uso del servicio, para tener un registro detallado de quien usa un equipo determinado, a qué hora y por cuánto a tiempo. Con esto y con una cámara de vigilancia puede ser suficiente para prevenir acciones delictivas en el sitio de Café Internet.

Octava política. Control de acceso a los equipos o recursos y a las aplicaciones

Es importante contar con una herramienta que ayude a monitorear el acceso a los recursos y aplicaciones del Café Internet por parte de los usuarios. Dar libertad absoluta a los usuarios en el uso de las mismas puede provocar graves problemas de seguridad. Entre las acciones más importantes a llevar a cabo para este fin se encuentran:

- Restringir el control de instalación/desinstalación de software por parte de los usuarios.
- Restringir a los usuarios la administración de características como el CTRL+ALT+DEL o las llamadas “winkeys” que permiten el acceso al administrador de tareas.
- Restringir a los usuarios la administración de los permisos de acceso al panel de control, impresoras de red, etc.
- Restringir a los usuarios la administración de acceso a unidades de red, discos duros o discos removibles.
- Controlar el acceso a sitios no deseados.
- Restringir el control de ejecución de aplicaciones no permitidas.

Novena política. Uso de Firewall

Esta herramienta permite un control sobre el tráfico de red en los puertos de la computadora lo que permite restringir la filtración de amenazas así como el acceso a páginas no deseadas, esto bloqueando las direcciones IP.

Capítulo 4

Diseño y Desarrollo Del Sistema de Apoyo Para Mantener Seguros Los Sitios De Café Internet

4.1 Software de seguridad existente en el mercado

En el mercado existe una infinidad de aplicaciones diseñadas para proteger los equipos de cómputo de las amenazas provenientes de internet, así como de dispositivos externos; la finalidad de citarlos en esta compilación es que el internauta vea la gama de herramientas que existen para un mejor aprovechamiento de la seguridad en equipos de cómputo.

Cabe recordar que algunas traducciones de las que se puede ser objeto son como los citados FIREWALL, traducidas al español como Servidores de Seguridad, POP-KILLERS, como Bloqueadores de Elementos Emergentes y los ANTI PHISHING, como anti fraude.

Para una mayor valoración de cómo estas aplicaciones, en el caso de antivirus, tienden a estar en continua mejora, existe una organización, cuya página anexamos, que semestralmente realizan pruebas en un equipo preparado para depositar el mayor número de virus posibles en él, con el objetivo de ejecutar en cada ocasión, cada uno de los antivirus existentes y conocer su capacidad de detección de amenazas. Así mismo, se pueden consultar todo tipo de consejos en cuestión de virus y antivirus.

http://www.virus.gr/portal/en/

De igual manera existe un sitio en el que se pueden ejecutar herramientas de prueba para los bloqueadores de elementos emergentes.

http://www.popuptest.com/

Nota: La lista de aplicaciones que abajo se muestra tiene ligas a páginas externas ajenas en su totalidad a este sitio y son propiedad de sus desarrolladores.

Antivirus

Kaspersky	Sophos Sweep
Active Virus Shield by AOL	ViRobot Expert
ZoneAlarm with KAV Antivirus	Antiy Ghostbusters
F-Secure 2007	Zondex Guard
BitDefender Professional	Vexira 2006
BullGuard	V3 Internet Security
Ashampoo	Comodo
AntiVir	A-Squared Anti-Malware
eScan	Ikarus
Nod32	Digital Patrol
CyberScrub	ClamWin
Avast Professional	Quick Heal
AVG Anti-Malware	Protector Plus
F-Prot	PcClear
McAfee Enterprise+AntiSpyware	AntiTrojan Shield
Panda 2007	PC Door Guard
Norman	Trojan Hunter
ArcaVir 2007	VirIT
McAfee	E-Trust PestPatrol
Norton Professional 2007	Trojan Remover
Rising AV	The Cleaner
Dr. Web	True Sword
Trend Micro Internet Security 2007	Abacre
Iolo	Virus Chaser
VBA32	

Firewall

Comodo Firewall Pro	Look 'n' Stop
ProSecurity	F-Secure Internet Security 2008
Outpost Firewall Pro	Panda Internet Security 2008
Online Armor Personal Firewall	Avira Premium Security Suite
Kaspersky Internet Security	AVG Internet Security
System Safety Monitor	PC Tools Firewall Plus
ZoneAlarm Pro	McAfee Internet Security Suite 2008
Lavasoft Personal Firewall	ESET Smart Security
Privatefirewall	Rising Personal Firewall 2007
Webroot Desktop Firewall	Windows Live OneCare
Norton Internet Security 2008	BitDefender Internet Security 2008
Jetico Personal Firewall	BullGuard Internet Security
Trend Micro Internet Security 2008	iolo Personal Firewall
Sunbelt Personal Firewall	Steganos Internet Security 2008
FortKnox Personal Firewall 2008	Filseclab Personal Firewall

Escaneadores de puertos

Upseros	Internet Security Alliance
Asociacion de Internautas	Gibson Research Corporation

Anti-Dialers

CheckDialer	AntiDialer
DialerControl	StopDialers

Popup Killers

Google Toolbar	Opera
Nopopups	Altavista Toolbar
Web Window Killer	Yahoo! Companion
Mozilla	MyPopupKiller
Pop-Down	Netscape
Ad Muncher	Super Popup Blocker
Advertising Killer	Zero Popup Killer

Anti-Spyware

Spyware Doctor	CA Spyware 2007 (PestPatrol)
Webroot SpySweeper	Ad-Aware SE
AntiSpy	Maxion Spy Killer
Spybot Search & Destroy	

Anti-Spam

Spam Combat	Comdom AntiSpam
Spamihilator	Cyberoam
Spam Assassin	Equiinet
SpamBayes	Juniper
Aladdin	Kaspersky
Softwin	PineApp
McAfee	Sophos
NetCore	Softscan
SpamTitan	Trend Micro
WatchGuard	

Anti-Fraude

Netcraft Toolbar	TrustWatch
ScamBlocker	SpoofStick

4.2 Selección del lenguaje de programación

Una de las principales decisiones que deben tomarse al momento de desarrollar un sistema es la selección adecuada del lenguaje de programación, ya que de ello dependerá el óptimo funcionamiento dicho sistema. En nuestro caso, después de analizar distintas opciones, elegimos PHP, ya que cuenta con una serie de ventajas que sirven de beneficio a nuestro sistema. Dichas ventajas se muestran en la tabla 4.1.

1.	Es un lenguaje multiplataforma. PHP corre casi en cualquier plataforma utilizando el mismo código fuente, pudiendo ser compilado y ejecutado en algo así como 25 plataformas, incluyendo diferentes versiones de Unix, Windows (95, 98, NT, ME, 2000, XP, etc.)
2.	Es libre, es de decir, no tiene costo, por lo que se presenta como una alternativa de fácil acceso para todos. El usuario no depende de una compañía específica para arreglar las cosas que no funcionan, además no estás forzado a pagar actualizaciones anuales para tener una versión que funcione.
3.	PHP es completamente expandible. Está compuesto de un sistema principal (escrito por Zend), un conjunto de módulos y una variedad de extensiones de código.
4.	Cuenta con muchas interfaces distintas para cada tipo de servidor. PHP se puede ejecutar bajo Apache, IIS, AOLServer, Roxen y THTTPD. Otra alternativa es considerarlo como módulo CGI.
5.	Tiene la capacidad de conexión con la mayoría de los manejadores de bases de datos que se utilizan en la actualidad, tales como: MySQL, MS SQL, Oracle, Informix, PostgreSQL, y otros muchos.
6.	Cuenta con una gran variedad de módulos, por lo que es fácil crear APIS.
7.	Es un lenguaje veloz, dado que generalmente es utilizado como módulo de Apache. Está completamente escrito en C, así que se ejecuta rápidamente utilizando poca memoria.
8.	Se pueden leer y manipular datos desde distintas fuentes, incluyendo datos que pueden ingresar los usuarios desde formularios HTML.

Tabla 4.1 Ventajas de PHP

4.3 Desarrollo del Sistema

El desarrollo del sistema constó de tres etapas. La primera etapa fue el diseño de unos instrumentos de investigación (cuestionarios) para los administradores y los usuarios de los sitios públicos de Café Internet en las 16 delegaciones de la Ciudad de México. Dichos cuestionarios fueron implementados en una página Web, de tal manera que fuera más oportuno y efectivo el almacenamiento de las respuestas de los usuarios. El proceso es el siguiente, el administrador o el usuario se registran para poder acceder a las preguntas, una vez registrado contesta y dichas respuestas quedan almacenadas en la base de datos. De esta manera, se ahorra papel además de obtener datos concretos sobre las características y los problemas de seguridad más comunes en estas salas. Es aquí donde se empieza a notar la capacidad del lenguaje de programación que se ha elegido, ya que con el código PHP adecuado, se puede guardar información a una base de datos en un servidor, en este caso MySQL, con la finalidad de graficar la información posteriormente y poder así ilustrar los resultados.

A continuación se presenta el algoritmo de solución empleado en este apartado, así como una breve explicación del mismo.

Algoritmo de solución

- Inicio
- Recibir valores
- Asignar a variables
- Realizar suma datos recibidos
- Realizar evaluación sumatoria

    Si calificación = aprobatoria

        Desplegar Resultado Aprobado

    Si no cumple condición entonces

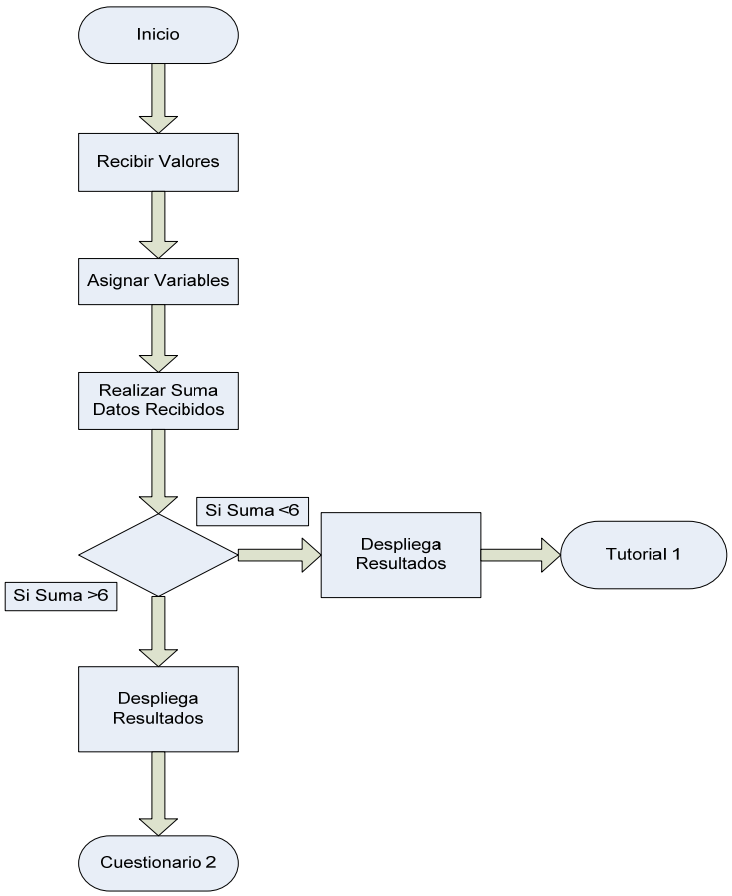
        Desplegar Resultado No Aprobado

- Fin

Explicación del algoritmo de solución

Para poder realizar la evaluación de las preguntas de cada uno de los formularios se le asigno un valor a cada pregunta; 1=Si y 0=No, con estos valores se pudo tomar una cuenta numérica que al pasarlas por el método POST a un código PHP, el cual dicho anteriormente en el algoritmo recibe los valores insertados de cada una de las preguntas, después se le asigna a diferentes variables para poder realizar la suma de dichos valores y así realizar una comparación en la cual se evalúa posteriormente la calificación con un valor ya establecido por el aplicador del formulario y ésta comparación es la que toma la decisión de cuál será la ruta a seguir a fin de evaluar al usuario.

La figura 4.1 ilustra el algoritmo de solución citado y explicado arriba.



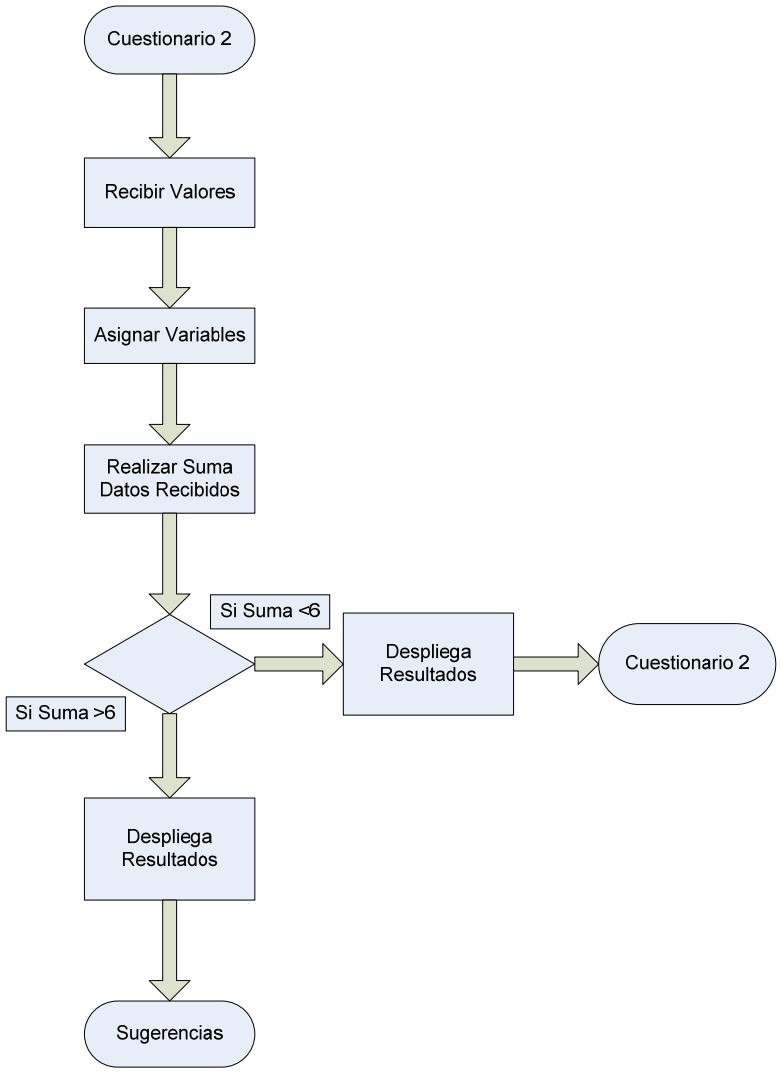
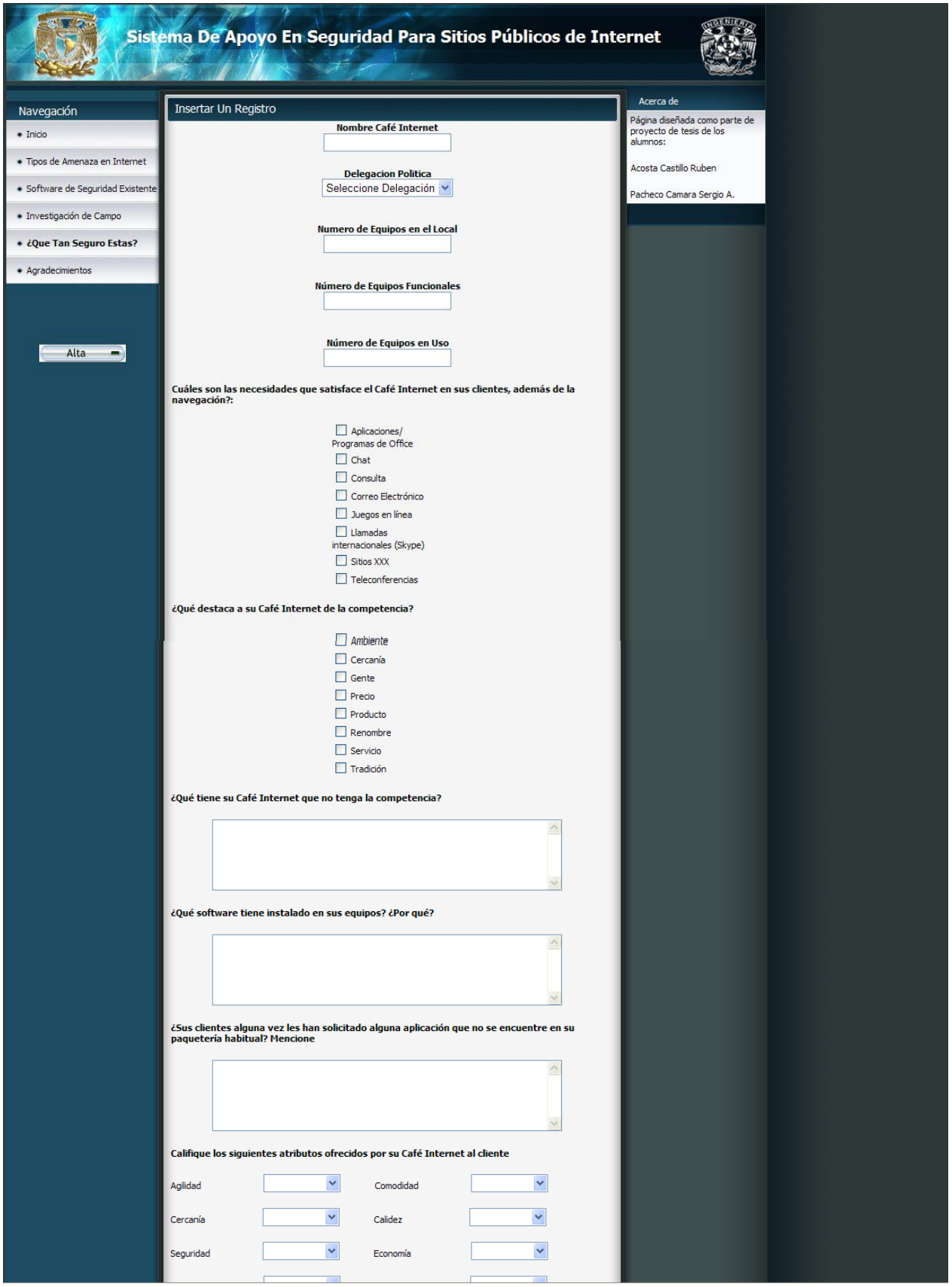


Fig 4.1 Algoritmo de solución del Sistema de Apoyo

Esta es la parte de la página que permite a los visitantes adentrarse en los temas de amenazas informáticas e interactuar para comprender algunos términos que se utilizan en informática para infectar un equipo de cómputo.

La página desarrollada es la que se muestra en la figura 4.2.


Sistema De Apoyo En Seguridad Para Sitios Públicos de Internet
Navegación
Inicio
Tipos de Amenaza en Internet
Software de Seguridad Existente
Investigación de Campo
¿Que Tan Seguro Estas?
Agradecimientos
Alta
Insertar Un Registro
Nombre Café Internet
Delegacion Politica
Seleccione Delegación
Numero de Equipos en el Local
Número de Equipos Funcionales
Número de Equipos en Uso
Cuáles son las necesidades que satisface el Café Internet en sus clientes, además de la navegación?:
Aplicaciones/ Programas de Office
Chat
Consulta
Correo Electrónico
Juegos en línea
Llamadas internacionales (Skype)
Sitios XXX
Teleconferencias
¿Qué destaca a su Café Internet de la competencia?
Ambiente
Cercanía
Gente
Precio
Producto
Renombre
Servicio
Tradición
¿Qué tiene su Café Internet que no tenga la competencia?
¿Qué software tiene instalado en sus equipos? ¿Por qué?
¿Sus clientes alguna vez les han solicitado alguna aplicación que no se encuentre en su paquetería habitual? Mencione
Califique los siguientes atributos ofrecidos por su Café Internet al cliente
Agilidad
Comodidad
Cercanía
Calidez
Seguridad
Economía
Acerca de
Página diseñada como parte de proyecto de tesis de los alumnos:
Acosta Castillo Ruben
Pacheco Camara Sergio A.

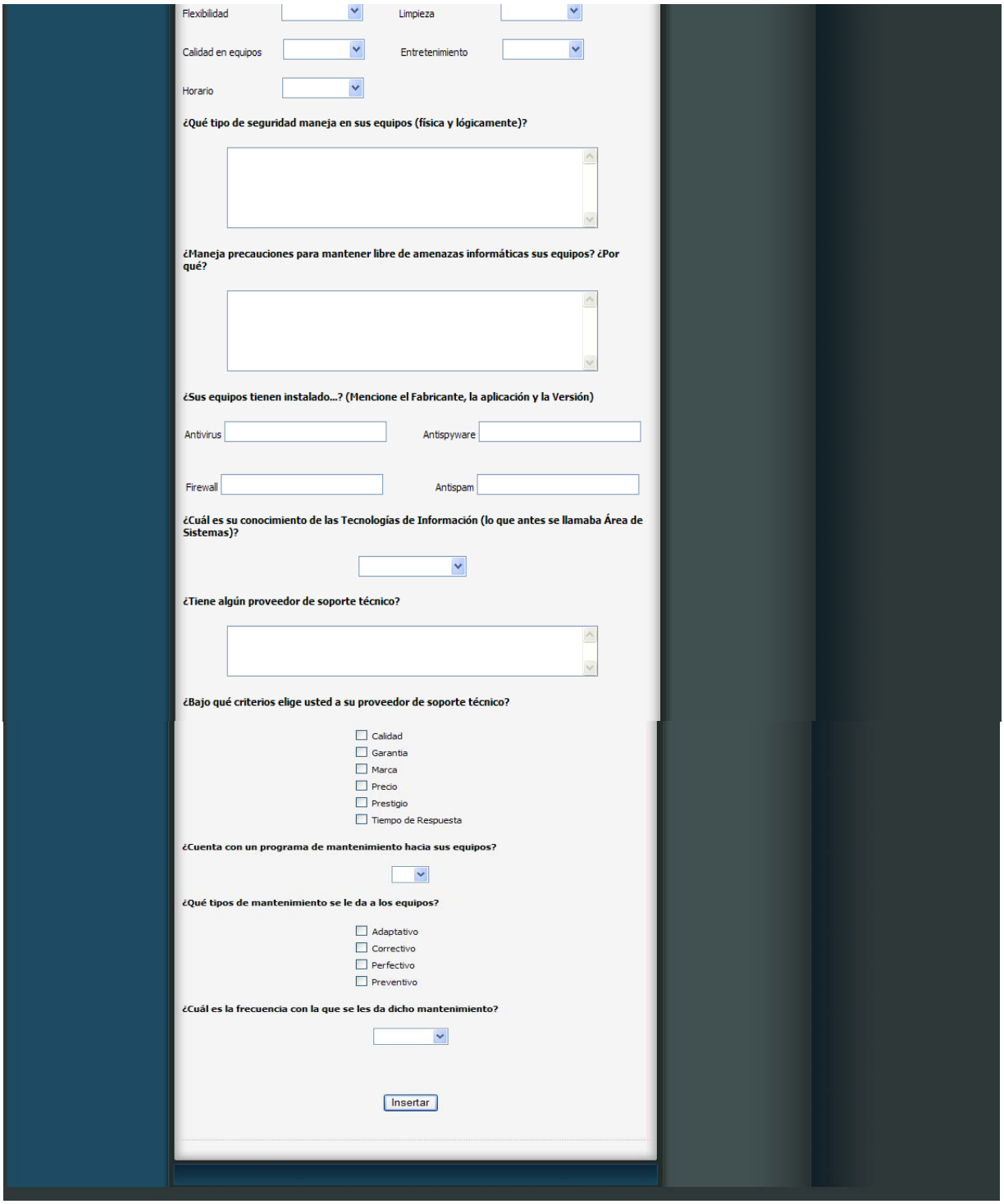


Figura 4.2 Cuestionario para administradores de los Café Internet

La segunda etapa consistió en la interpretación de los datos obtenidos. Se hizo una interpretación de esos datos lo más completa posible, la cual dio origen a la última y tercera etapa de nuestro proyecto. Dicha interpretación de datos ha sido detallada en el capítulo anterior.

La tercera etapa de nuestro proyecto fue la construcción de un sistema que titulamos: **"*Sistema de Apoyo en Seguridad para Sitios Públicos de Internet".*** Para ello realizamos una página Web que fue montada en el Laboratorio de Redes y Seguridad de la Facultad de Ingeniería en la sección de Proyectos. La dirección de dicha página es: http://redyseguridad.fi-p.unam.mx. La figura 4.3 muestra la página principal del sistema de apoyo.

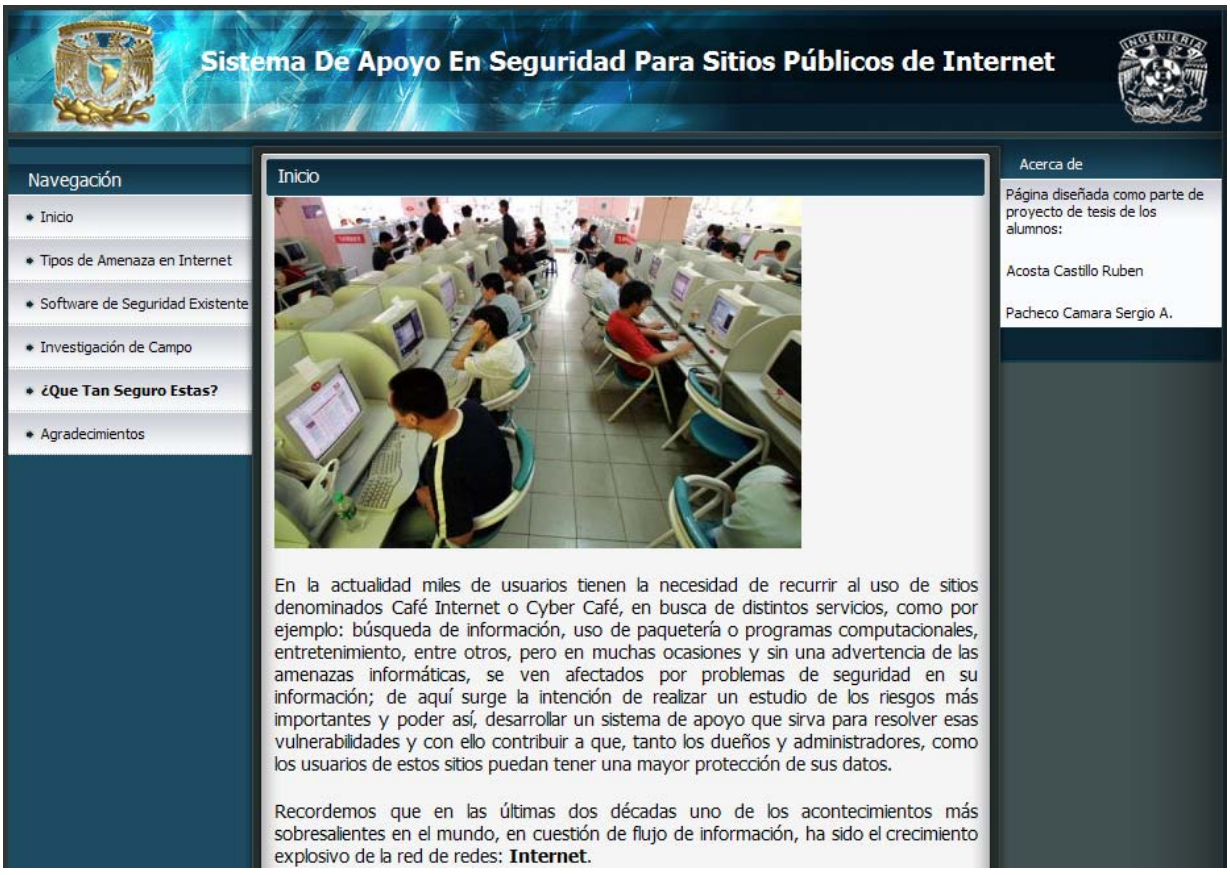


Figura 4.3 Página principal del Sistema de Apoyo.

La figura 4.4 muestra los elementos que componen el menú del Sistema de Apoyo.

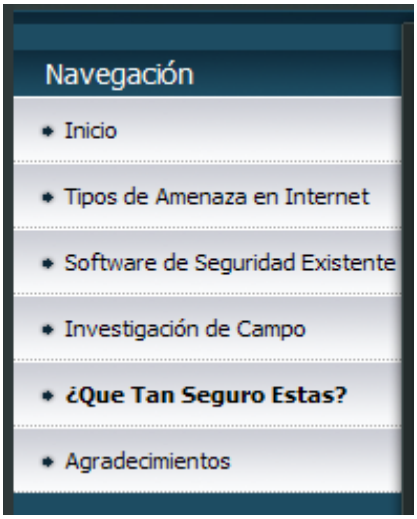


Figura 4.4 Elementos del menú del Sistema de Apoyo.

Como se observa en la figura 4.4, el menú está compuesto de 6 apartados, cuyo contenido se explica a continuación.

- *Inicio:* Contiene una breve explicación de la intención de realizar un estudio de las amenazas informáticas más importantes en los Café Internet, que nos llevó a la realización de éste proyecto.
- *Tipos de amenazas en Internet:* Aquí se presentan las amenazas en Internet que consideramos más comunes e importantes. Cada tipo de amenaza cuenta con una explicación breve que el usuario aún sin conocimientos sólidos en el tema, creemos puede comprender con facilidad.
- *Software de seguridad existente:* Contiene una compilación del software de seguridad existente de mayor demanda y que han dado mejores resultados. Esta compilación incluye: antivirus, firewalls, escaneadores de puertos, popup killers, antispyware, antispams y antifraudes. Cada uno del software presentado en este apartado contiene la liga al lugar donde el usuario puede descargar dicha aplicación para probarla de acuerdo a sus necesidades particulares.
- *Investigación de campo:* Esta sección incluye la interpretación de los datos obtenidos durante el estudio realizado a los Café Internet en las 16 delegaciones del Distrito Federal. Se muestran las gráficas para una mejor comprensión de

dicha interpretación y para que el usuario logre un panorama más específico de la situación actual de estos sitios públicos en materia de seguridad.

- *¿Qué tan seguro estás?:* Esta sección cuenta con un "subsistema" creado para medir a través de unos cuestionarios que el usuario previamente tiene que resolver, el nivel de seguridad de su Café Internet, dándole la oportunidad de elegir por su propia cuenta y en base a todo lo leído en los otros apartados explicados anteriormente y en los pequeños tutoriales incluidos en esta sección, las medidas de acción a tomar para mejorar sus problemas de seguridad existentes, eligiendo a su vez las herramientas que considere más adecuadas del listado incluido en el apartado: "Software de seguridad existente".
- *Agradecimientos:* En esta sección se brinda el reconocimiento a todas las personas que hicieron posible la realización de este trabajo. Aquéllas personas que aportaron sus contribuciones valiosas que lograron enriquecer y pulir el presente proyecto.

Cuando el usuario da clic en el apartado *¿Qué tan seguro estás?,* se despliega un menú que se muestra en la figura 4.5.

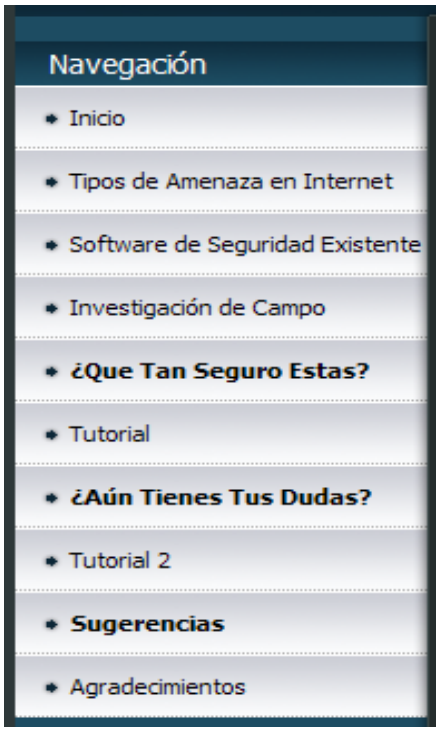


Figura 4.5 Menú desplegado al dar clic en ¿Qué tan seguro estás?

Como se puede observar en la figura 4.5 la sección ¿Qué tan seguro estás? se despliega un submenú con los siguientes elementos:

- Tutorial
- ¿Aún tienes tus dudas?
- Tutorial 2
- Sugerencias

Esto es porque, justo aquí es donde se encuentra la parte medular de nuestra investigación, ya que en esta sección el usuario puede acceder a la lectura de un tutorial que muestra información oportuna sobre la seguridad informática en estos sitios considerando un nivel básico de conocimientos en el área y posterior a la lectura de dicho tutorial el usuario es invitado a resolver un cuestionario para medir su comprensión de dicho tutorial, si este cuestionario es aprobado, inmediatamente el usuario es direccionado a la sección titulada ¿Aún tienes tus dudas?, en caso contrario es nuevamente enviado al tutorial 1. Cuando el usuario pasa a la sección ¿Aún tienes tus dudas? tiene que leer un nuevo tutorial que considera un nivel de conocimientos intermedio-avanzado en el área de seguridad y nuevamente al concluir la lectura es enviado a resolver el cuestionario 2, si este cuestionario es aprobado, el sistema le presenta al usuario una serie de sugerencias para el mejoramiento de la seguridad, en caso contrario el usuario es enviado nuevamente a leer el tutorial 2.

Capítulo 5

Pruebas y liberación Del Sistema

5.1 Importancia de las pruebas en un sistema

La calidad, tanto en la industria como en el comercio y en las organizaciones de servicios y nuevas tecnologías, es hoy en día un claro factor diferencial competitivo. Y, evidentemente, la industria del software no es una excepción, pues en el desarrollo de software las posibilidades de error son innumerables. Las empresas dedicadas al desarrollo de software intentan aumentar la calidad de sus productos para evitar o disminuir los problemas inherentes a sus procesos: plazos y presupuestos incumplidos, insatisfacción del usuario, escasa productividad y la baja calidad en el software producido. Las empresas son conscientes de que el mercado valora, cada día más, la calidad. Por lo tanto, las compañías exigen la disminución de errores y penalizan los retrasos en entregas y las cancelaciones de proyectos.

Una herramienta clave para conseguir una aplicación de alta calidad y libre de errores es contar con un proceso de pruebas efectivo. Debido a la complejidad de probar una aplicación, la etapa de pruebas puede llegar a ser de las más lentas del proceso de desarrollo de software.

La fase de pruebas del sistema es una de las últimas fases del ciclo de vida antes de entregar un programa para su explotación. Tiene como objetivo verificar el software para comprobar si este cumple sus requisitos. Las pruebas de software son un elemento crítico para la garantía de calidad del software y representa una revisión final de las especificaciones, del diseño y de la codificación.

Las pruebas del software son siempre necesarias. El objetivo específico de la fase de pruebas es encontrar cuántos errores, mejor. ***Probar un programa es ejercitarlo con la peor intención de encontrarle fallos.***

5.2. Concepto de Probar o Testing

Los procesos de prueba o testing son una herramienta que asegura que un sistema hace lo que tiene que hacer. Probar es una práctica habitual de todo proceso productivo, que consiste básicamente en comprobar que un producto tiene las

características deseadas. Prácticamente todos los productos que llegan al mercado son probados: se “prueban” los materiales que van a formar parte de un producto, se “prueba” que las partes a ensamblar tienen las dimensiones adecuadas y se “prueba”, por ejemplo, que el producto final tiene la resistencia adecuada. Es decir, a lo largo del proceso productivo de cualquier producto se hacen comprobaciones que hacen que el producto final sea el adecuado.

En el caso del software ocurre lo mismo. El proceso de desarrollo de software consta de una serie de etapas. En cada etapa se van “desarrollando” y “ensamblando” partes que al final van a conformar el producto final.

La prueba ideal de un sistema sería exponerlo en todas las situaciones posibles, así encontraríamos hasta el último fallo. Sin embargo, esto es imposible desde todos los puntos de vista: humano, económico e incluso matemático. Por eso es recomendable buscar formas humanamente abordables y económicamente aceptables de encontrar errores.

5.3. Proceso de generación de pruebas del sistema

Toda prueba consta tradicionalmente de los siguientes tres elementos:

- Interacciones entre el sistema y la prueba
- Valores de prueba
- Resultados esperados

Los dos primeros elementos permiten realizar la prueba y el tercer elemento permite evaluar si la prueba se superó con éxito o no.

Un proceso de pruebas consta generalmente de las siguientes cuatro fases:

- La fase de diseño de pruebas
- La fase de codificación
- La fase de ejecución

- La fase de análisis de resultados

El objetivo de un proceso de generación de pruebas del sistema es desarrollar las dos primeras fases y obtener estos tres elementos a partir del modelo de requisitos del propio sistema bajo prueba. Dicho proceso toma como punto de partida los requisitos y, a partir de ellos genera los resultados y construye las pruebas.

5.4. Características de las pruebas de software

Las características más importantes de las pruebas de software se muestran en la tabla 5.1.

✓ Son siempre necesarias.
✓ Pretenden descubrir errores.
✓ Tienen éxito si descubren un error nuevo.
✓ Pueden demostrar la existencia de errores, pero no su ausencia.
✓ Empiezan por lo pequeño y progresan hacia lo grande.
✓ No son posibles las pruebas exhaustivas.

Tabla 5.1 Características de la pruebas de Software.

La prueba y validación de los resultados no es un proceso que se realiza una vez desarrollado el software sino que debe efectuarse en cada una de las etapas de desarrollo.

En la **especificación de requisitos** el tener una explicación clara, precisa y competa del problema facilita el análisis de errores y la generación de casos de prueba. Hay que generar los datos necesarios para determinar si se han cubierto todos los requisitos y determinar en base a éstos los valores esperados de los casos de prueba. Es importante asegurar la corrección, coherencia y exactitud de los requisitos.

En el **diseño** hay que comprobar los algoritmos individuales, las interfaces entre módulos y analizar las estructuras de datos para localizar posibles inconsistencias o torpezas en su construcción.

En la **codificación** hay que comprobar la coherencia con el diseño, se ejecutan los casos de prueba, conservando la información referente al proceso de prueba. Se fuerza al máximo la consistencia de la estructura del programa, las estructuras de datos y su funcionalidad.

Durante el **mantenimiento** debe de existir documentación de pruebas que incluya casos de prueba y resultados esperados. Si se producen modificaciones en el programa, habrá que probar de nuevo todas las partes del programa afectadas por las modificaciones.

5.5 Enfoques de diseños de pruebas

Existen tres enfoques principales para el diseño de casos:

1. El enfoque **estructural** o de **caja blanca.** Se diseña analizando/ejecutando el código del componente, por lo tanto, se centra en la estructura interna del programa (analiza los caminos de ejecución). Permite detectar errores de flujo de control y de estructuras de datos locales. (Véase Fig. 5.1)

2. El enfoque **funcional** o de **caja negra.** Se diseña considerando las responsabilidades del componente, por lo tanto, se centra en las funciones, entradas y salidas. Permite detectar errores de asignación de responsabilidades y de la interfaz del componente. (Véase Fig. 5.2)

3. El enfoque **aleatorio** consiste en utilizar modelos (en muchas ocasiones estadísticos) que representen las posibles entradas al programa para crear a partir de ellos los casos de prueba.

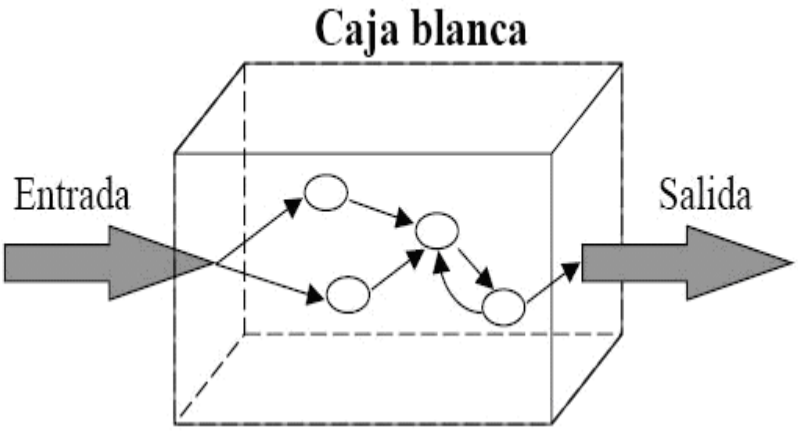


Fig. 5.1 Enfoque estructural o de caja blanca

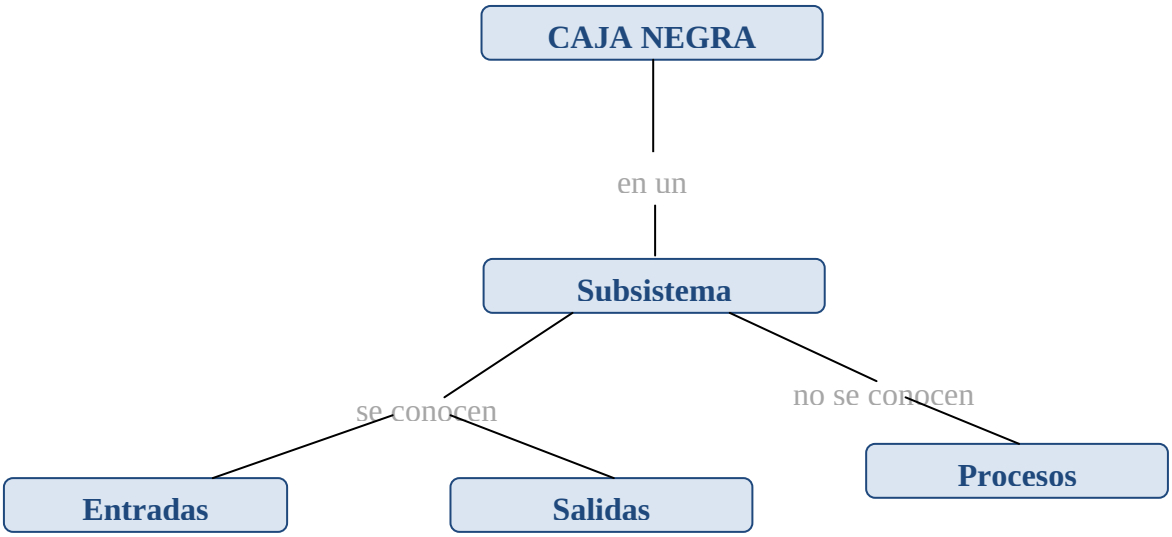


Fig. 5.2 Enfoque funcional o de caja negra

5.6 Tipos de pruebas de Software

Pruebas de unidad

- Centra la prueba en el componente.
- Puede realizarse en paralelo a otros componentes.
- Básicamente son pruebas de caja blanca.
- Se prueban los caminos de control importantes para descubrir errores en el componente.
- Debemos simular el "comportamiento" del resto de los componentes.

Pruebas de integración

Son aquéllas que se realizan una vez que se han aprobado las pruebas unitarias. Consiste en realizar pruebas para verificar que un gran conjunto de partes de software funcionan juntos. Existen tres tipos:

- Pruebas de integración descendente: Es una estrategia de integración incremental a la construcción de la estructura de programas, en el cual se integran los módulos moviéndose en dirección hacia abajo por la jerarquía comenzando por el control principal (Programa principal). Los módulos subordinados de control principal se incorporan en la estructura, bien, de forma primero-en-profundidad, bien primero-en-anchura.
- Pruebas de integración ascendente: Es donde la construcción del diseño empieza desde los módulos más bajos hacia arriba (módulo principal), el procesamiento requerido de los módulos subordinados siempre está disponible y elimina la necesidad de resguardo.

Pruebas de validación

- Se llevan a cabo cuando se han terminado las pruebas de integración, el software está ensamblado y se han realizado todas las pruebas de unidad e integración.

- La validación se consigue cuando el software funciona según las expectativas del usuario.

Existen dos tipos principales:

- Pruebas alfa: Realizadas por el usuario con el desarrollador como observador en un entorno controlado (simulación de un entorno de producción).
- Pruebas beta: Realizadas por el usuario en su entorno de trabajo y sin observadores.

5.7 Pruebas realizadas a nuestro sistema

Ahora que hemos desarrollado la pagina web que nos permitirá crear una ventana a nuevas maneras de visualizar la seguridad informática y algunas de las características que esta conlleva, es importante realizar pruebas de compatibilidad en diferentes equipos de cómputo, esto con el fin de otorgar a los administradores de cibercafés toda la funcionalidad con la que se pensó originalmente.

Empecemos con la dificultad para montarlo en servidor:

En principio se realizó la instalación en una computadora casera. Decidimos realizar una instalación de elementos separados, como es el caso del servidor apache, MySQL, y el lenguaje de programación PHP, sin embargo, nos encontramos que al realizar esta instalación de elementos por separado, las aplicaciones no se ejecutaban de manera correcta, esto es, que no hay conexión a base de datos, y el servidor apache no reconoce el lenguaje PHP.

Dada esta circunstancia, recurrimos a una aplicación llamada WAMP, de uso libre y que integra todas las características necesarias como el acceso a base de datos, el servidor apache y el lenguaje de programación PHP, mas la posibilidad de utilizar lenguaje JAVA.

A pesar de que el freeware Wamp es útil en un principio, nos encontramos con una falla de conexión al querer crear los pop-up que utilizamos para dar el resultado de los

cuestionarios de la página, sin darnos cuenta, estábamos utilizando una versión llamada Wamp5, al revisar en el sitio oficial, http://www.wampserver.com, encontramos q existe una nueva versión de Wamp, llamada WampServer 2.0, que integra de manera más eficiente, el trabajo con JAVA, con esta solución es que podemos integrar los cuestionarios y el manejo de las respuestas en los llamados Pop-up o ventanas emergentes.

La figura 5.3 ilustra la apariencia de la aplicación utilizada para el desarrollo de nuestro proyecto.

Fig. 5.3 Apariencia de WampServer 2.0

De acuerdo a la naturaleza del proyecto, las pruebas que hicimos se basaron en el diseño de caja blanca, debido a que conforme ensamblamos cada parte de la página, se iba probando su funcionalidad, es decir, de la página de inicio:

http://localhost/Proyect2daparte/index.html

Véase la figura 5.4.

Figura 5.4 Página Web Principal

Se estableció la conexión a las páginas secundarias desde el panel lateral. La Figura 5.5 muestra el menú de navegación.

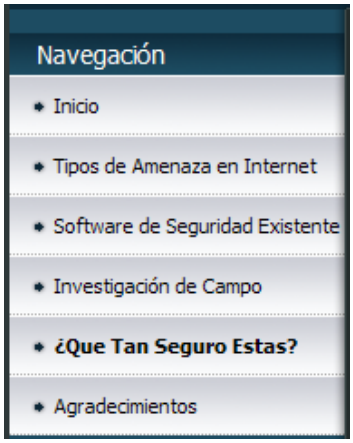


Figura 5.5 Menú de Navegación

http://localhost/Proyect2daparte/Amenazas.htm (Figura 5.6)

Figura 5.6Tipos de Amenaza en Internet

http://localhost/Proyect2daparte/swmercado.htm (Figura 5.7)

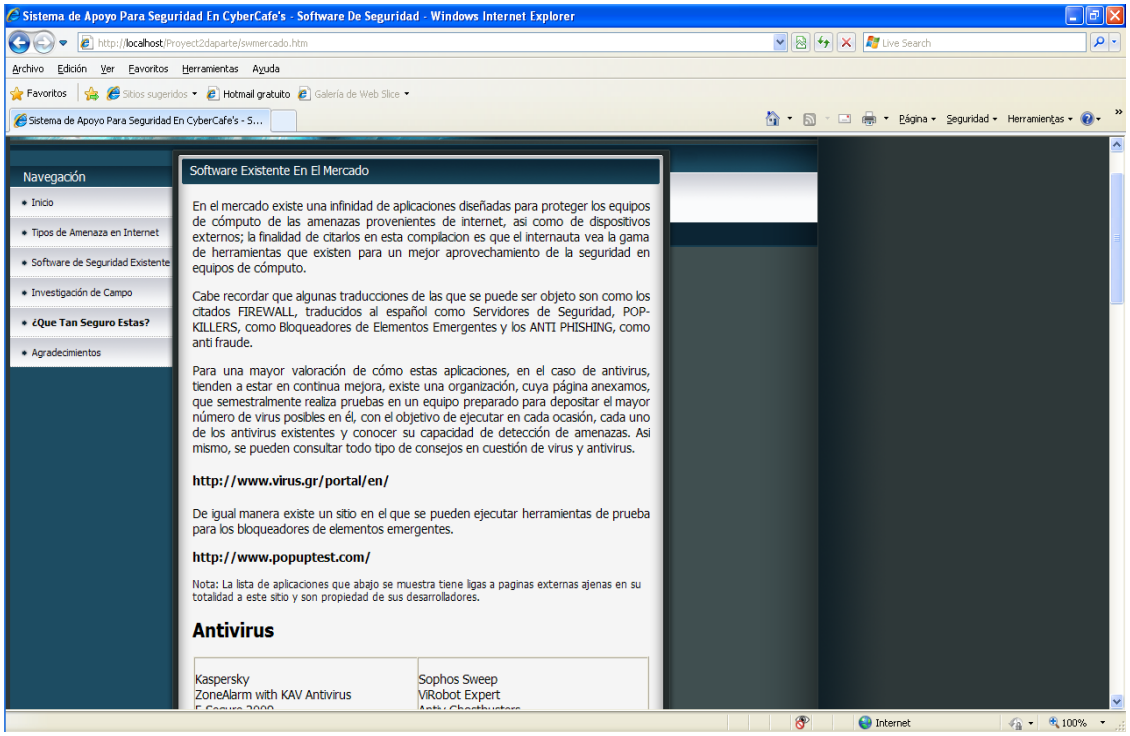


Figura 5.7 Software de Seguridad Existente

http://localhost/Proyect2daparte/invest.htm (Figura 5.8)

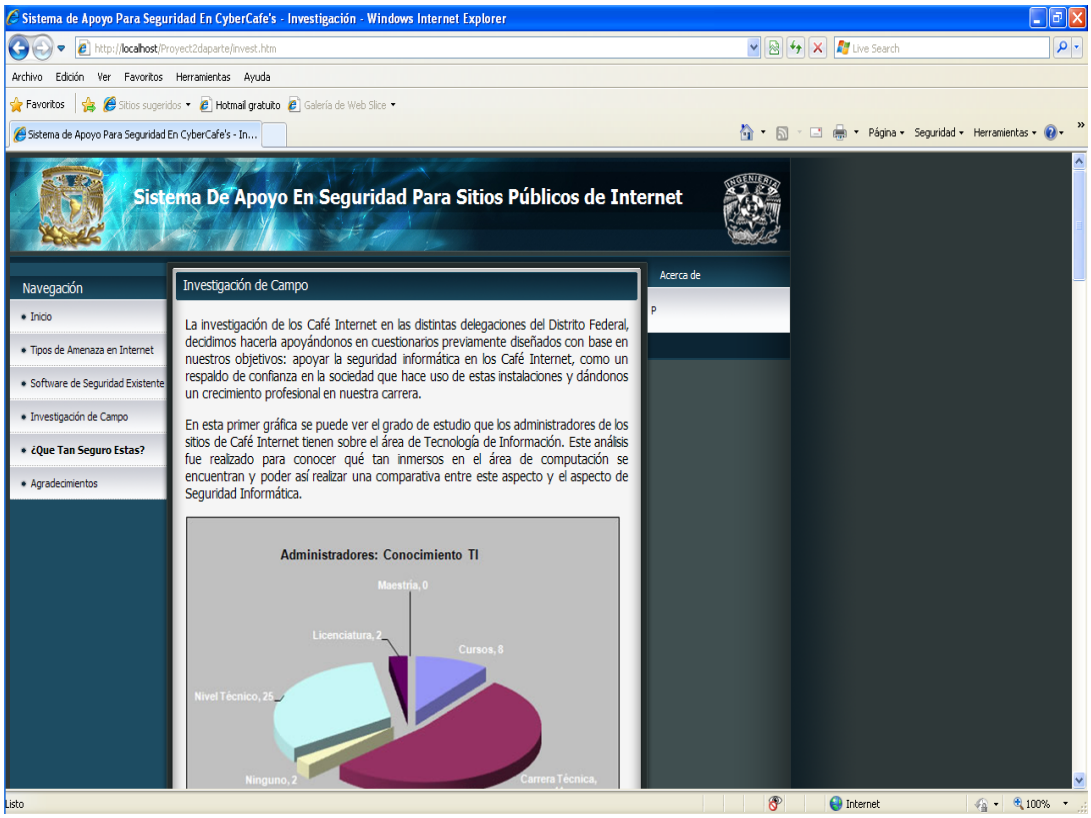


Figura 5.8 Página Investigación de Campo

http://localhost/Proyect2daparte/Cuestionario.htm (Figura 5.9)

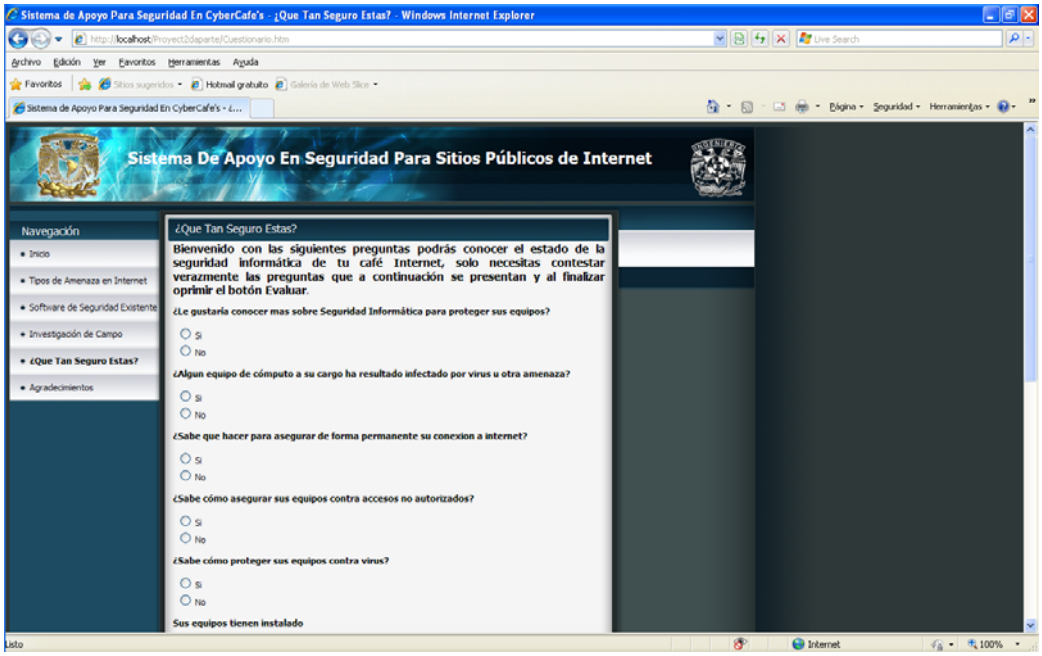


Figura 5.9 Página Cuestionarios

http://localhost/Proyect2daparte/Agradecimientos.htm (Figura 5.10)

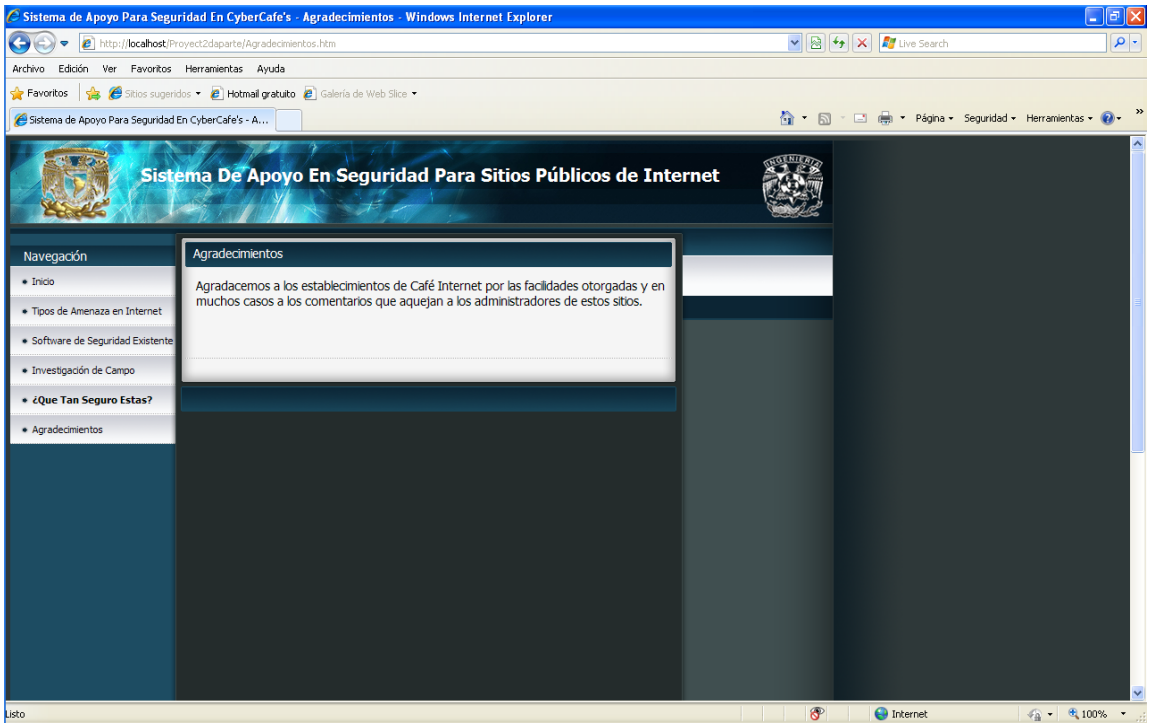


Figura 5.10 Página Agradecimientos

Dentro de las pruebas detectamos errores de desarrollo de las páginas, como un mal direccionamiento como fue el caso de la página:

http://localhost/Proyect2daParte/Sugerencia.htm (Figura 5.11)

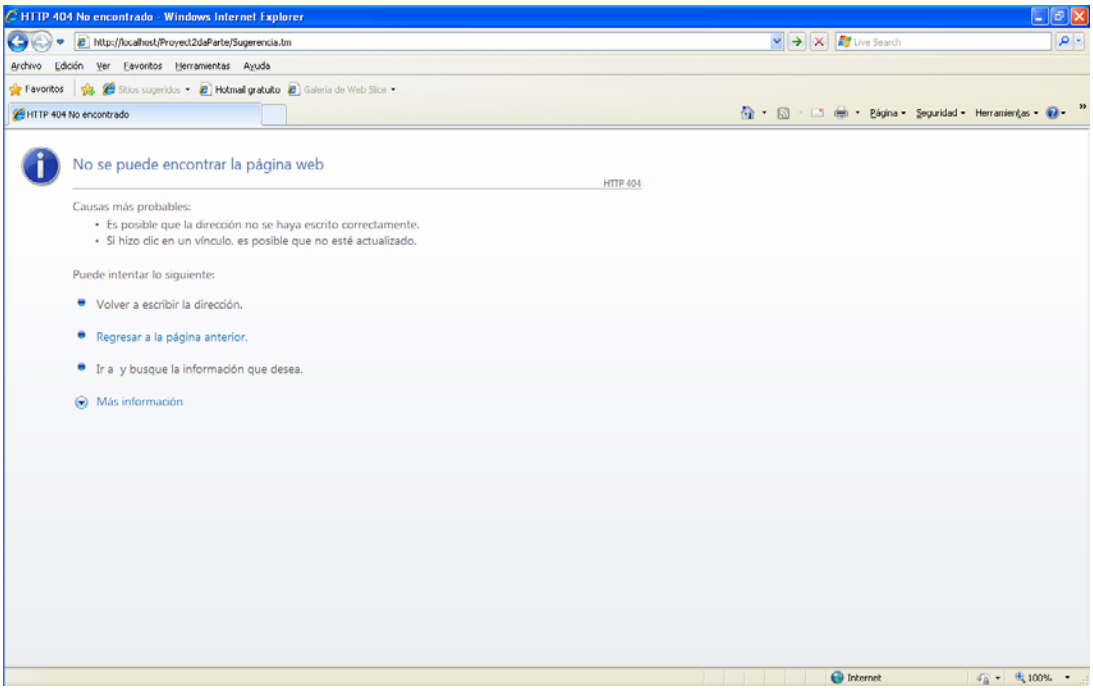


Figura 5.11 Página con error de direccionamiento

Estos errores fueron corregidos revisando que la ruta a la que estuviera direccionada la siguiente página concordara con la ruta de la liga en el servidor local.

Dentro del desarrollo de la parte interactiva, es decir, tratándose de los cuestionarios y los tutoriales, nos encontramos primeramente con la situación de que php podía evaluar el resultado de cada cuestionario, mostrarlo en una ventana emergente y permitir agregar una liga (la palabra SEGUIR), sin embargo, no permitía que la ventana emergente regresara a la pantalla principal cerrando automáticamente el "pop-up". (Véase Figuras 5.12 y 5.13)

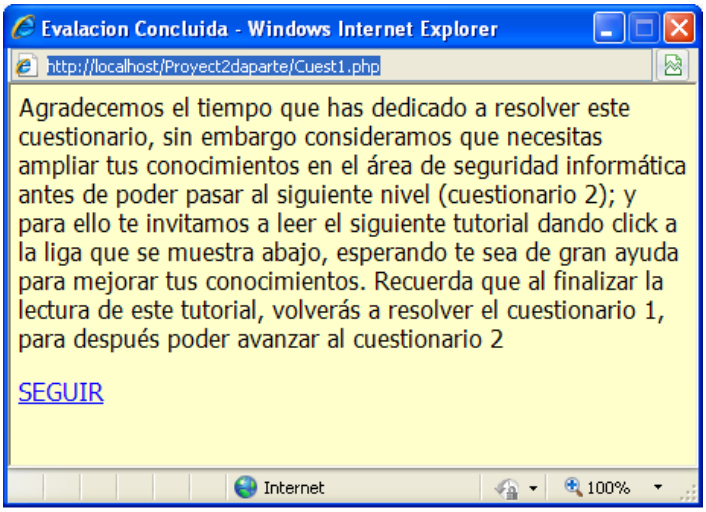


Figura 5.12 Ventana Emergente 1

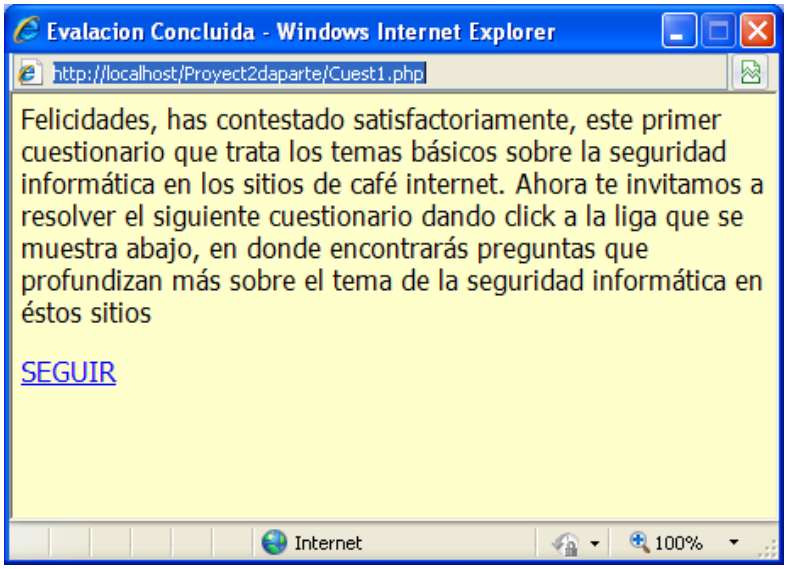


Figura 5.13 Ventana Emergente 2

La solución fue integrar un comando del lenguaje de programación Java, cuyas pruebas preliminares demostraron cerrar correctamente una ventana emergente, refrescando la ventana de donde provenía.

Aunque no lo hizo de la misma manera sobre la plataforma php, tras diversos intentos, encontramos que la versión de php en la que realizamos el anexo de la sentencia java que estábamos corriendo, que dicho sea de paso era la 5.0.3, no era la versión más actual.

Al instalar la versión Wamp 2.0, cuyo paquete de PHP es la versión 5.2.6, la sentencia:

<p><p>SEGUIR

Resulto eficaz para los propósitos del retorno de página que necesitamos.

Tras las pruebas preliminares y los ajustes en el servidor local, nos hicimos a la tarea de entregar el sistema para su montaje en el servidor de Seguridad Informática de la Facultad de Ingeniería, donde la instalación fue transparente.

Conclusiones

Después de haber realizado esta interesante investigación a los sitios de Café Internet en la Ciudad de México en el área de seguridad informática se ha logrado conocer con mayor precisión las distintas amenazas que aquejan a dichos sitios, descubriendo de esta manera que el nivel de seguridad es muy bajo debido a que los administradores y usuarios que diariamente recurren a estos sitios para llevar a cabo un sinfín de actividades de diferentes tipos no muestran ningún interés en cerciorarse de contar con un nivel de "seguridad razonable" de su información.

Este descubrimiento junto con el análisis de los datos obtenidos en nuestra investigación de campo nos llevó a cumplir con el objetivo de proponer las políticas y mecanismos de seguridad que consideramos elementales en cualquier sitio de Café Internet (pequeño o grande) y que hemos escrito y explicado en el Capítulo 3 de este trabajo. Pero además de eso, también hemos logrado la creación del sistema de apoyo para los dueños o administradores de estos sitios, que consideramos es una aportación valiosa que servirá para mejorar el nivel de seguridad en los Café Internet.

Consideramos que la sociedad mexicana seguirá impulsando el crecimiento de los Café Internet, pues todavía son mayoría los que tienen que recurrir a estos sitios a realizar alguna tarea de su interés; por ejemplo, los jóvenes que no cuentan con una computadora en casa y que para poder hacer sus tareas tienen que hacer uso de un Café Internet, o aquéllos jóvenes que si cuentan con computadora pero no con impresora y tienen que recurrir a imprimir sus tareas a alguno de estos sitios, o como el empleado de empresa que requiere imprimir archivos personales y que en su empresa se lo prohíben, etc. También consideramos que las amenazas seguirán siendo un problema constante a las que tendrán que enfrentarse los administradores de éstos sitios, pero también estamos seguros que surgirán nuevas herramientas que ayudarán a salvaguardar la seguridad de los mismos.

APÉNDICES

Estándar Ethernet	Fecha	Descripción
Ethernet experimental	1972 (patentado en 1978)	2.94 Mbit/s sobre cable coaxial en topología de bus.
Ethernet II (DIX v2.0)	1982	10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio.
IEEE 802.3	1983	10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.
802.3a	1985	10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 metros
802.3b	1985	10BROAD36
802.3c	1985	Especificación de repetidores de 10 Mbit/s
802.3d	1987	FOIRL (Fiber-Optic Inter-Repeater Link) enlace de fibra óptica entre repetidores.
802.3e	1987	1BASE5 o StarLAN

802.3i	1990	10BASE-T 10 Mbit/s sobre par trenzado (UTP). Longitud máxima del segmento 100 metros.
802.3j	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
802.3x	1997	Full Duplex (Transmisión y recepción simultáneos) y control de flujo.
802.3y	1998	100BASE-T2 100 Mbit/s sobre par trenzado (UTP). Longitud máxima del segmento 100 metros
802.3z	1998	1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
802.3ab	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado
802.3ac	1998	Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para 802.1Q VLAN y manejan prioridades según el estandar 802.1p.
802.3ad	2000	Agregación de enlaces para enlaces gemelos.

802.3ae	2003	Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR
IEEE 802.3af	2003	Alimentación sobre Ethernet.
802.3ah	2004	Ethernet en el último kilómetro.
802.3ak	2004	10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial.
802.3an	2006	10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado (UTP)
802.3ap	en proceso	Ethernet de 1 y 10 Gbit/s sobre circuito impreso.
802.3aq	en proceso	10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo.
802.3ar	en proceso	Gestión de Congestión
802.3as	en proceso	Extensión de la trama

Insertar un registro

Género

Edad

Actividad

¿Por qué frecuentas este Café Internet?

¿Qué destaca a este Café Internet de la competencia?

- Ambiente
- Cercanía
- Gente
- Precio
- Producto
- Renombre
- Servicio
- Tradición

¿Que servicios utilizas en un CyberCafé?:

- Aplicaciones/ Programas de Office
- Chat
- Consulta
- Correo Electrónico
- Juegos en línea

☐ Llamadas internacionales (Skype)

☐ Sitios XXX

☐ Teleconferencias

¿Has solicitado alguna aplicación que no se encuentre en la paquetería habitual? Menciona

Califica los siguientes atributos ofrecidos por el Café Internet

Agilidad Comodidad Cercanía

Calidez Seguridad Economía

Flexibilidad Limpieza

Calidad de sus equipos Entretenimiento Horario

Insertar

Insertar un registro

Nombre Café Internet

Delegación Política

Seleccione Delegación

Número de Equipos en el Local

Número de Equipos Funcionales

Número de Equipos en Uso

Cuáles son las necesidades que satisface el Café Internet en sus clientes, además de la navegación?:

- Aplicaciones/ Programas de Office
- Chat
- Consulta
- Correo Electrónico
- Juegos en línea
- Llamadas internacionales (Skype)
- Sitios XXX
- Teleconferencias

¿Qué destaca a su Café Internet de la competencia?

- Ambiente
- Cercanía
- Gente
- Precio
- Producto
- Renombre
- Servicio

☐ Tradición

¿Qué tiene su Café Internet que no tenga la competencia?

¿Qué software tiene instalado en sus equipos? ¿Por qué?

¿Sus clientes alguna vez les han solicitado alguna aplicación que no se encuentre en su paquetería habitual? Mencione

Califique los siguientes atributos ofrecidos por su Café Internet al cliente

Agilidad Comodidad Cercanía

Calidez Seguridad Economía

Flexibilidad Limpieza

Calidad de sus equipos Entretenimiento Horario

¿Qué tipo de seguridad maneja en sus equipos (física y lógicamente)?

¿Maneja precauciones para mantener libre de amenazas informáticas sus equipos? ¿Por qué?

¿Sus equipos tienen instalado...? (Mencione el Fabricante, la aplicación y la Versión)

Antivirus

Antispyware

Firewall

Antispam

¿Cuál es su conocimiento de las Tecnologías de Información (lo que antes se llamaba Área de Sistemas)?

¿Tiene algún proveedor de soporte técnico?

¿Bajo qué criterios elige usted a su proveedor de soporte técnico?

- Calidad
- Garantia
- Marca
- Precio
- Prestigio
- Tiempo de Respuesta

¿Cuenta con un programa de mantenimiento hacia sus equipos?

¿Qué tipos de mantenimiento se le da a los equipos?

- Adaptativo
- Correctivo
- Perfectivo

☐ Preventivo

¿Cuál es la frecuencia con la que se les da dicho mantenimiento?

Insertar

Glosario

Glosario

Adware: Comprende programas que muestran anuncios para usuarios finales, independientemente de la actividad del usuario. Este tipo de software por lo general se instala en los equipos víctimas desde sitios remotos, sin el conocimiento del usuario. Por lo general, no es peligroso, pero es molesto y hace perder tiempo y recursos del sistema.

Acceso remoto: Utilidad para que un usuario acceda desde su propio PC a otro que esté ubicado remotamente y pueda operar sobre él.

Accesos autorizados: Permiso de acceso a diversos recursos limitado a usuarios, procesos o aplicaciones que disponen de una autorización específica.

Access point: Un punto de acceso inalámbrico es un dispositivo que conecta dispositivos de comunicación inalámbrica entre sí para formar una red.

Active X: Un software desarrollado por Microsoft y lanzado al mercado en 1997, que permite que programas o contenido sea llevado a computadoras con Windows por medio del World Wide Web.

Active X Control: Lenguaje de programación desarrollado por Microsoft con el cual es posible crear aplicaciones exportables a Internet y pueden ser vistas desde cualquier navegador compatible. Puede otorgar grandes posibilidades a las páginas Web que los utilizan. Dada su potencialidad, pueden infectarse con virus o similares, por esta razón no deben aceptarse de forma indiscriminada.

Actualización de antivirus: Incorporación en el programa antivirus de la última versión archivo de identificación de virus. Dependiendo de la configuración del antivirus, la actualización se hace automáticamente a través de Internet o de forma manual.

Administrador: Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo sistema informático o red de ordenadores.

Amenaza: Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las amenazas se pueden materializar y volverse agresiones. Pueden afectar a la integridad, confidencialidad o disponibilidad.

Amenaza activa: Amenaza de un cambio no autorizado del estado del sistema.

Amenaza pasiva: Amenaza relativa a la confidencialidad de la información sin cambiar el estado del sistema. Consiste en el acceso no autorizado a la información protegida.

Análisis de riesgo: Estudio de los activos, sus vulnerabilidades y las probabilidades de materialización de amenazas, con el propósito de determinar la exposición al riesgo de cada activo ante cada amenaza.

Ancho de banda: Bandwith en inglés. Cantidad de bits que pueden viajar por un medio físico (cable caoxial, fibra óptica, par trenzado, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información.

Antiespía: Aplicación que se encarga de prevenir, detectar y/o eliminar espías (spyware) de una computadora.

Antispam: Aplicación o herramienta informática que detecta y elimina el spam y los correos no deseados.

Antivirus: Aplicación o grupo de aplicaciones dedicadas a la prevención, detección y eliminación de programas malignos en sistemas informáticos. Entre los programas con códigos malignos se incluyen virus, troyanos, gusanos, spywares, entre otros malwares.

Aplicación: Programa informático que permite a un usuario utilizar una computadora con un fin específico. Una aplicación de software suele tener un único objetivo: navegar en la Web, revisar correo, etc. Una aplicación que posee múltiples programas se considera un paquete. Son ejemplos de aplicaciones: Internet Explorer, Outlook, Word, Excel, WinAmp, etc.

Applet: Pequeña aplicación escrita en Java la cual se difunde a través de la red en orden de ejecutarse en el navegador cliente.

Ataque: Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

Ataques activos: Ataques que producen cambios no autorizados y deliberados en el estado del sistema.

Ataques pasivos: Ataques que se limitan a acceder de forma no autorizada a información protegida.

Autenticación: Proceso en el que se da fe de la velocidad y autenticidad de un producto, de unos datos o de un servicio, así como de la fiabilidad y legitimidad de la empresa que los ofrece.

Autorización: Proceso en el que se acredita a un sujeto o entidad para realizar una acción determinada.

Base de datos: Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

BHO (Browser Helper Object): Es un plugin que se ejecuta automáticamente junto con el navegador de Internet, y extiende sus funciones. Generalmente son depositados por otro software y son típicamente instalados por las barras de herramientas. Algunos se emplean con fines maliciosos, para capturar información y monitorizar las páginas web solicitadas.

BIOS: Identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido.

Bit: Es la unidad más pequeña de información digital con la que trabajan los sistemas informáticos, puede tener dos estados “0” o “1”. La unión de 8 bits da lugar a un byte.

Bridge: Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar.

Browser Hijackers: Son los programas que procuran cambiar la página de inicio y búsqueda y/o otros ajustes del navegador. Estos pueden ser instalados en el sistema sin nuestro consentimiento al visitar ciertos sitios Web mediante controles Active X o bien ser incluidos por un troyano.

Bus: Es la ruta de data en el motherboard o tarjeta madre, que interconecta al microprocesador con extensiones adjuntas conectadas en espacios o slots de expansión, por ejemplo disco duro, CD-ROM drive y tarjetas de video.

Buscador: Los buscadores o motor de búsqueda son aquéllos que están diseñados para facilitar encontrar otros sitios o páginas Web.

Café Internet: Lugar comercial que permite por medio de un pago determinado, obtener por un tiempo establecido, acceso a la navegación en Internet y a los servicios de valor agregado que se encuentran actualmente en la red.

Chain email: Es cualquier email enviado a una o más personas pidiéndoles que reenvíen el mensaje a una o más personas, con la promesa por reenviarlo o castigo en caso de no hacerlo.

Chat: Se trata de conversaciones escritas en Internet. Mediante un programa a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas al mismo tiempo.

Confidencialidad: Capacidad de mantener datos inaccesibles a todos, excepto a una lista determinada de personas.

Conexión remota: Operación realizada en una computadora remota a través de una red de computadoras, como si se tratase de una conexión local.

Contraseña: Password. Código utilizado para acceder a un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

Cookie: Procedimiento ejecutado por el servidor que consiste en guardar información acerca del cliente para su posterior recuperación. En la práctica la información es proporcionada por el visualizador al servidor del World Wide Web vía una forma o un método interactivo que puede ser recuperado nuevamente cuando se accede al servidor en el futuro. Es utilizado por ejemplo para el registro a un servicio.

Cracker: Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio.

Desinfección: Acción que realizan los programas antivirus cuando, tras detectar un virus, lo eliminan del sistema y, en la medida de lo posible, recuperan o restauran la información infectada.

Dialer: Programa que permite cambiar el número de acceso telefónico automáticamente, de acuerdo a la situación geográfica del usuario. Estos códigos (que se descargan de sitios a veces sin percatarnos) toman el control sólo de la conexión telefónica vía módem, desviando las llamadas normales que se efectúan a través del proveedor hacia un número del tipo 908, 906, etc., números de tarifa especial y bastante cara por lo general.

DNS: Servidor de Nombres de Dominio. Servidor automatizado utilizado en el Internet cuya tarea es convertir nombres fáciles de entender (como www.panamacom.com) a direcciones numéricas de IP.

Dominio: Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Los más comunes son .com, .edu, .net, .org, .biz, .info.

Download: Descarga. Proceso en el cual la información es transferida desde un servidor a una computadora personal.

E-mail: El e-mail, del inglés electronic mail (correo electrónico) es uno de los medios de comunicación que por medio del protocolo de comunicación TCP/IP, permite el intercambio de mansajes entre las personas conectadas a la red de manera similar al correo tradicional. Para ello es necesario tener una dirección de correo electrónico, compuesta por el nombre de usuario, la arroba "@" y el nombre del servidor de correo. Por ejemplo, sample@panamacom.com, donde "sample" es el usuario y panamacom.com el nombre del host o del servidor.

Escáner: Programa que busca virus en la memoria del PC o en los archivos.

Estándar: Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc.

Estándar 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.

Ethernet: Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. En cooperación con DEC e Intelque. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps. Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

Fallo: Error en un programa. Cuando uno de ellos tiene errores, se dice que tiene Bugs. Como los virus son programas, también pueden contener bugs. Esto implica que, si el virus debe realizar determinadas acciones, podría no realizarlas, o no hacerlo bajo las condiciones que su programador ha establecido inicialmente.

Filtros Anti-spam: Son herramientas para filtrar el spam o correo basura no solicitado en los programas de correo.

Firewall: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

FTP: Protocolo de Transferencia de Archivos. Permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.

Gusano: Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications (Marzo 1982). El primer gusano famoso de Internet apareció en Noviembre de 1998 y se propagó por si solo a más de 6,000 sistemas a lo largo de Internet.

Hacker: Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad al mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

Hoax: No se trata de virus, sino de falsos mensajes de alarma (bromas o engaños) sobre virus que no existen. Estos se envían por correo electrónico con la intención de extender falsos rumores por Internet.

HTTP: En inglés *Hypertext Transfer Protocol*. Protocolo de Transferencia de Hipertexto. HTTP es un protocolo con la ligereza y velocidad necesaria para distribuir y manejar sistemas de información hipermedia. HTTP ha sido usado por los servidores World Wide Web desde su incio en 1993.

HTTPS: Creado por Netscape Communications Corporation para designar documentos que llegan desde un servidor web seguro. Esta seguridad es dada por el protocolo SSL (Secure Socket Layer) basado en la tecnología de encriptación y autenticación desarrollada por RSA Data Security Inc.

Hub: El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

Infección: Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo.

Internet: Una red mundial, de redes de computadoras. Es una interconexión de redes grandes y chicas alrededor del mundo. El Internet empezó en 1962 como una red para los militares llamada ARPANet, para que en sus comunicaciones no existan "puntos de falla". Con el tiempo fue creciendo hasta convertirse en lo que es hoy en día, una herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar múltiples servicios como por ejemplo emails, WWW, etc. que usen TCP/IP.

Internet Café: Ver Café Internet.

Internet Explorer: Conocido también como IE es el browser web de Microsoft, creado en 1995 para Windows y mucho después para Mac. No fue el primero en el mercado y Netscape le sacó delantera por muchos años, pero la penetración de Windows en el mercado es muy fuerte. Microsoft empezó a distribuir Windows junto con IE. Poco a poco las personas simplemente preferían usar lo que venía en la computadora a tener que descargar una aplicación de gran tamaño como era Netscape. En la actualidad navegadores como Firefox están ganando terreno.

Intranet: Red privada dentro de una compañía u organización que utiliza el navegador favorito de cada usuario, en su computadora, para ver menús con opciones desde cumpleaños del personal, calendario de citas, mensajería instantánea privada, repositorio de archivos y las normativas de la empresa entre otras. Es como si fuera un sitio Web dentro de la empresa. Al usar los browser de internet como Internet Explorer, Firefox o Safari el intranet se convierte en multiplataforma. No importa la marca o sistema operativo de las computadoras dentro de la red, todos se pueden comunicar.

IP: Internet Protocol, Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como por ejemplo, 132. 248. 53. 10.

ISO: International Standards Organization es una red de institutos nacionales de estándares constituido por 157 países, un miembro por país, con un secretariado central en Geneva, Suiza, en donde se coordina todo el sistema. Es el desarrollador y publicador de Estándares Internacionales más grande del mundo.

ISP: Internet Service Provider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

LAN: Red de área local. Es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). Cada ordenador tiene su propio CPU y programas pero también puede acceder a los datos y dispositivos de otros nodos así como comunicarse con éstos (e-mail). Sus características son: Topología anillo o lineal, arquitectura punto a punto o cliente/servidor, conexión para fibra óptica, cable coaxial o entrelazado, ondas de radio.

Malware: Software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el consentimiento de su dueño, con finalidades muy diversas.

Mecanismo de seguridad: Es el mecanismo (procedimiento) utilizado para implementar una política de seguridad. Se dividen en tres grandes grupos: de prevención, de detección y de recuperación.

Phishing: Técnica que consiste en atraer mediante engaños a un usuario hacia un sitio Web fraudulento donde se le insta a introducir datos privados, generalmente números de tarjetas de crédito, nombres y passwords de las cuentas, números de seguridad social, etc. Uno de los métodos más comunes para hacer llegar al PC infectado a la página falsa es a través de un email que aparenta provenir de un emisor de confianza (banco, entidad financiera u otro) en el que se introduce un enlace a una Web en la que el “phisher” ha reempalzado en la barra de dirección del navegador la verdadera URL para que parezca una legal.

Pirata informático: Persona que accede a un sistema informático sin autorización para ver su funcionamiento interno y explotar vulnerabilidades.

Política de seguridad: Enunciado formal de las reglas que los usuarios que acceden a los recursos de la red de una organización deben cumplir.

Protección de datos: Conjunto de técnicas utilizadas para preservar la confidencialidad, la integridad y la disponibilidad de la información.

Protocolo: Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

Punto de acceso (PA): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

Riesgo: Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Sector de arranque: Todo disco tiene un sector de arranque que el PC lee cuando se enciende. Este sector contiene todos los códigos necesarios para cargar los archivos de sistema DOS.

Seguridad: Se entiende como seguridad, una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Seguridad de Información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden también ser consideradas.

Servidor de autenticación: Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.

Spyware: Pequeñas aplicaciones cuyo fin es el obtener información, sin que el usuario se dé cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

Spam: También conocido como junk-mail o correo basura, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

Troyano: En inglés, trojan. Programa informático cuya ejecución tiene unos efectos imprevistos y generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

Virus: Programa que está diseñado para copiarse a si mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

Bibliografía y Mesografía

Bibliografía

1) Artero, J.L. **"Seguridad en la información".** Thomson Paraninfo, S.A., 2008.

2) Baños Navarro, Raúl y Gómez López, Julio. **"Seguridad en sistemas operativos Windows y Linux".** RA-MA, 2006.

3) Bradley, Tony. **"Protección del PC y Seguridad en Internet".** Anaya Multimedia, 2007.

4) Burgos, Alexis. **"Como proteger la PC".** MP Ediciones, 2007.

5) Casals, Pedro. **"Piratas en la red".** Anaya Multimedia, 1997.

6) Cheswick R., William. **"Firewalls and Internet Security: Repelling the Wily Hacker".** Addison-Wesley Publishing Company, 1994.

7) Devore, Jay L. **"Probabilidad y estadística para ingeniería y ciencias".** Quinta edición, Thomson Paraninfo, S.A., 2001.

8) Erickson, John. **"Hacking. Técnicas fundamentales".** Anaya Multimedia, 2008.

9) Franck, Mikkel. **"Seguridad en Internet".** Know Ware E.U.R.L., 2003.

10) Gómez Vieites, Álvaro. **"Enciclopedia de la Seguridad Informática".** Primera edición, Alfaomega Grupo Editor, 2007.

11) Hernández Sampieri, Roberto. **"Metodología en la investigación".** McGraw-Hill/Interamericana de México, 2006.

12) Howard, Michael. **"19 puntos clave sobre seguridad de software".** McGraw-Hill/Interamericana de México, 2006.

13) Huidobro Moya, José Manuel y Roldán Martínez, David. **"Seguridad en redes y sistemas informáticos".** Thomson Paraninfo, 2005.

14) Jurado Rojas, Yolanda. **"Técnicas de investigación documental: Manual para la elaboración de tesis, monografías, ensayos e informes".** Thomson Paraninfo, S.A., 2003.

15) Lockhart, Andrew. **"Seguridad de redes: los mejores trucos".** Amaya Multimedia, 2007.

16) Marcelo Rodao, Jesús de. **"Piratas cibernéticos: Cyberwars, Seguridad informática e Internet".** Segunda edición, RA-MA, 2003.

17) McNab, Chris. **"Seguridad de redes".** Anaya Multimedia, 2004.

18) Meloni, Julie C. **"PHP, MySQL y Apache".** Anaya Multimedia, 2009.

19) Minera, Francisco. **"PHP y MySQL".** MP Ediciones, 2006.

20) Montero Ayala, Ramón. **"Protección ante Internet".** Creaciones Copyright, 2007.

21) Parker, B. Donn. **"Computer Security Management".** Prentice Hall, 1981.

22) Rhodes Oosley, Mark y Bragg, Roberta. **"Network Security. The complete reference".** McGraw-Hill, 2003.

23) Ríos García, Sixto. **"Iniciación a la estadística".** Thomson Paraninfo, 1999.

24) Rodríguez Iglesias, Marina y Sánchez, Javier. **"Actualización y mantenimiento del PC".** Anaya Multimedia, 2008.

25) Rosales Herrera, Humberto David. **"Determinación de riesgos en los centros de cómputo".** Editorial Trillas, 1996.

26) Smith, Ben y Komar, Brian. **"Seguridad en Microsoft Windows: Kit de recursos".** McGraw-Hill/Interamericana de España, S.A., 2003.

27) Tyan, Dan. **"Privacidad informática".** Anaya Multimedia, 2006.

28) W., A.A. **"Protege tus datos de virus y hackers".** Ediciones Axel Springer España, S.A., 2006.

29) Zacker, Craig. **"Redes (Manual de referencia)".** McGraw-Hill/Interamericana de España, S.A., 2002.

Mesografía

1) http://cafeinternet.com.co

2) http://www.trabajo.com.mx/cafeinternet_emprende_tu_cibercafe.htm

3) http://www.taringa.net/posts/info/1058734/Historia-de-los-Cibercaf%C3%A9s.html

4) http://www.arghys.com/casas/cibercafes-construccion.html

5) http://es.wikipedia.org/wiki/Ethernet

6) http://zator.com/Hardware/H12_4.htm

7) http://www.monografías.com/trabajos13/modosi/modosi.shtml

8) http://es.wikipedia.org/wiki/Modelo_OSI

9) http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

10) http://www.monografias.com/trabajos12/giga/giga.shtml

11) http://www.alegsa.com.ar/Dic/seguridad%20informatica.php

12) http://www.definicionabc.com/tecnologia/seguridad-informatica.php

13) http://sociedaddelainformacion.wordpress.com/2007/02/25/la-familia-de-normas-isoiec-27000/

14) http://webstore.iec.ch/preview/info_isoiec27000%7Bed1.0%7Den.pdf

15) http://es.kioskea.net/contents/secu/secuintro.php3

16) http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node334.html

17) http://danielomarrodriguez.blogspot.com/2008/09/analisis-de-riesgos.html

18) http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html

19) http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad

20) http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO/TEMA_7.htm

21) http://www.authorstream.com/Presentation/jemarinoi-86620-seguridad-informtica-8-informatica-education-ppt-powerpoint/

22) http://lsi.ugr.es/~ig1/docis/pruso.pdf

23) http://kybele.escet.urjc.es/Documentos/ISI/Pruebas%20de%20Software.pdf

24) http://www.amipci.org.mx/

25) http://www.siem.gob.mx/siem2008/

26) http://www.sat.gob.mx/

27) http://www.seccionamarilla.com.mx/

28) http://www.telmex.com/mx/