UNIVERSIDAD DE SOTAVENTO, A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

"SEGURIDAD INFORMÁTICA DENTRO DE LA RED DE LA UNIVERSIDAD DE SOTAVENTO"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN INFORMÁTICA

PRESENTA:

ILEANA BERMEJO HERNÁNDEZ

ASESOR DE TESIS:

LIC. RAÚL DE JESÚS OCAMPO COLÍN

COATZACOALCOS, VERACRUZ. JULIO DEL 2007.

QUIERO EXPRESAR MI AGRADECIMIENTO

En especial por que todo esto no hubiera sido posible sin el amparo incondicional de mis padres; María Angélica Hernández García, Fernando Bermejo Reyes y a mi hermano Jorge Alberto Bermejo Hernández, por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos.

A mi Asesor de Tesis, Mtro. Juan Antonio Haaz Zetina por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia profesional en un marco de confianza, afecto y amistad, fundamentales para la concreción de este trabajo.

Al Mtro. Edgar Ernesto Paxtián Ortiz, por sus valiosas sugerencias, acertados aportes durante el desarrollo de este trabajo y su permanente disposición y desinteresada ayuda.

Debo un Especial Reconocimiento a mi Padrino el Dr. Juan Manuel Rodríguez García por la confianza que mostró en mí y el apoyo al concederme una Beca Universitaria, con la cual fue posible finalizar mis estudios académicos.

A la Dra. Rosa Aurora Rodríguez Caamaño, al Mtro. Raúl Ocampo Colín y al Mtro. Jorge Martínez Estrada por su continuo y afectuoso aliento, cariño y comprensión.

No puedo olvidar a mis compañeros y amigos con los cuales he compartido incontables horas de trabajo, en los diferentes departamentos de la Institución. Gracias por los buenos y malos momentos, por aguantarme y escucharme. A mi gran Amigo Esteban Lara Solís a quien le agradezco

infinitamente me ayudara con la información recaudada ya que sin él no hubiese sido posible el término de la tesis.

ÍNDICE

CAPÍTULO 3

CAPÍTULO 4

INTRODUCCIÓN

El motivo del presente es desarrollar un estudio completo del estado actual y futuro posible de Seguridad Informática dentro de la Universidad de Sotavento y de cada uno de sus departamentos escolares, que continuamente en realidad se conoce muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas. Podrá cubrir parte del "agujero" que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el Conocimiento con que se cuenta. Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Todos pueden acceder a las herramientas que necesitan y los costos (la inversión que cada uno debe de realizar) va de acuerdo con el tamaño y potencialidades de la herramienta.

Paradójicamente, en el mundo informático, existe una demanda constante y muy importante que está esperando a que alguien los atienda.

Desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

En el presente, cada vez que se mencione Información se estará haciendo referencia a la Información que es procesada por un Sistema Informático; definiendo este último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."[1]

Luego:

"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."[1]

[1] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997. Página 22.

CAPÍTULO 1

1.1 PLANTEAMIENTO DEL PROBLEMA

Teniendo en cuenta las necesidades de la Institución para tener un manejo y control eficiente de los recursos con los que cuenta la Universidad de Sotavento y que se ve reflejado en las necesidades que tienen los alumnos y el personal docente que labora en los diferentes departamentos, requiere de una buena administración y control del flujo de información, teniendo en cuenta su reflejo en dicha organización.

Tomando en cuenta lo anterior, encontramos en algunos de los departamentos las siguientes problemáticas:

En el Departamento de Contabilidad no hay un proceso actual para dar de alta en inventarios los activos de la empresa ya que no se cuenta con el suficiente personal para poder llevarlo acabo, esto sucede a que el dueño de la empresa no esta al pendiente de que se realice periódicamente.

No existe un tipo de administración que este al pendiente de entradas y salidas de los equipos, ya sean del equipo interno o externo de las máquinas de cualquier departamento.

En cuanto al Centro de Cómputo lo que le falta es seguridad ya que no cuentan con un sistema de control interno. Aquí los alumnos pasan con mochilas, en lo cual no hay revisión de las mismas; no les piden credencial, no hay vigilancia cuando el alumnado u otra persona ajena a la Institución entra y de lo que bajan de la red cuando se encuentra en el centro de cómputo, por lo cual los usuarios entran y salen sin que exista un control

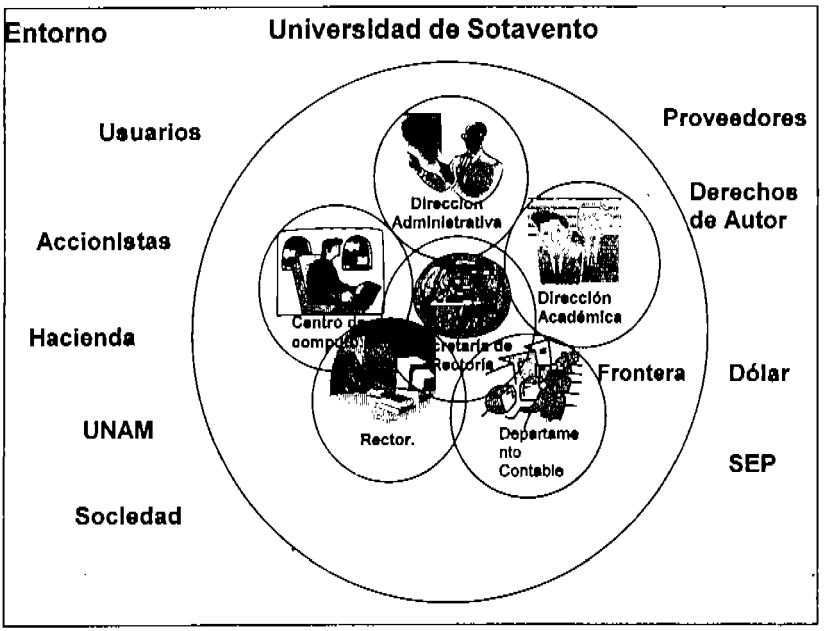
adecuado. Los catedráticos de la institución no firman su hora de salida del centro de cómputo y de lo que ocuparon en su momento.

Para las personas que se encuentran a cargo del Centro de Cómputo deberían llevar un registro interno y externo del equipo inventariándolo cada semana, pero por desgracia no se lleva a cabo, ya que así se verían las deficiencias del mismo equipo y el saber si no falta algún material. Así como también tener en cuenta el registro de las personas que se quedan a cargo del cuidado del equipo y de las personas que llegan a utilizarlo.

Cuando uno ingresa al Centro de Cómputo esta ingresando también a la red de la institución ya que esta conectada con la biblioteca, sistemas operativos de la institución y a todos sus campos de información de datos, para poder entender esto explico que la Institución cuenta con una Red Inalámbrica, que aunque tenga restricciones a departamentos y accesos a puertos o páginas de Internet y chat pueden ser burladas por cualquier estudiante o persona que sepa como hackear al igual que cualquiera puede llevarse algún equipo y cambiarlo con algún otro departamento de la institución, a la persona que se lleva el equipo no le hacen firmar un vale de resguardo. Por consiguiente no existe el control de entradas y salidas de los equipos, ya que también no hay el suficiente personal para en algún momento roben el equipo de la institución. Además de que no existe una canalización adecuada, lo cual ocasiona encargarse de todas las actividades del centro de cómputo en especial el aula 2 que ahí no hay nadie por lo regular o si llegase haber alguien solo esta una persona que es la que no se da abasto.

En los centros de cómputo no cuentan con protecciones diseñadas especialmente para evitar que inestabilidad de la red y

tropezones. No hay un sistema de tierra adecuado y no cuentan con una administración de la red.



1.2 ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD INFORMÁTICA

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la Información.

La **Integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal

autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La **Disponibilidad** u **Operatividad** de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La **Privacidad o Confidencialidad** de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño o volverse obsoleta.

El **Control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La **Autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica:** mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego

reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

- **No Repudio:** mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** este aspecto, íntimamente relacionado con la **Confidencialidad**, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoría:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuando las realiza.

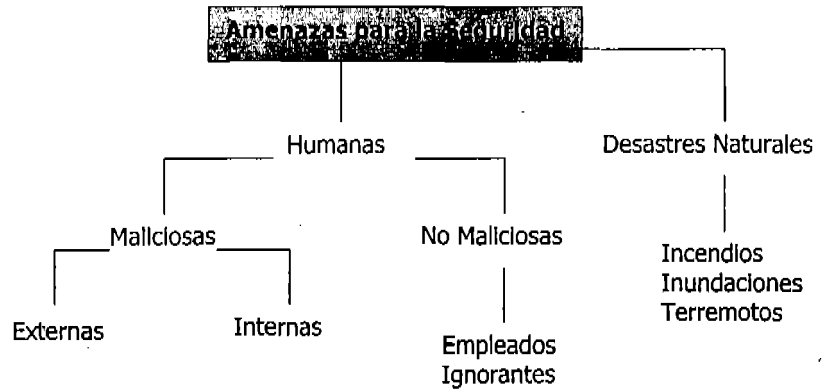


Gráfico 1.1 – Amenazas para la Seguridad

Las amenazas pueden ser analizadas en tres momentos: antes del taque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.

3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que **no existe el 100% de seguridad esperado o deseable en estas circunstancias.**

1.2.1 DE QUIEN DEBEMOS PROTEGERNOS

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita[2] contesta lo siguiente:

"Los tipos de Intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide."

1. **Clase A:** el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando (...) son pequeños grupitos que se juntan y dicen vamos a probar.
2. **Clase B:** es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como

[2] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en Instalaciones de Cybsec S.A. *http://www.cybsec.com*

detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.

3. **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

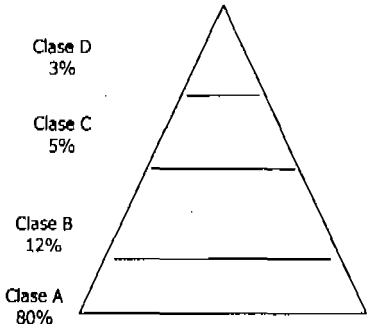


Gráfico 1.2 – Tipos de Intrusos. Fuente: CybSec S.A. *http://www.cybsec.com*

1.2.2 QUÉ DEBEMOS PROTEGER

En cualquier sistema informático existen tres elementos básicos a proteger: **el hardware, el software y los datos.**

Además, generalmente se habla de un cuarto elemento llamado **fungible**; que son los aquellos que se gastan o desgastan con el uso continuo: papel, tonner, tinta, cintas magnéticas, disquetes.

De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de

pasar obligatoriamente por un sistema de coplas de seguridad, y aún así es difícil de devolver los datos a su forma anterior al daño.

Para cualquiera de los elementos descritos existen multitud de amenazas y ataques que se los puede clasificar en:

1. **Ataques Pasivos**: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico.
2. **Ataques Activos**: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías

- **Interrupción**
- **Intercepción**
- **Modificación**
- **Destrucción**

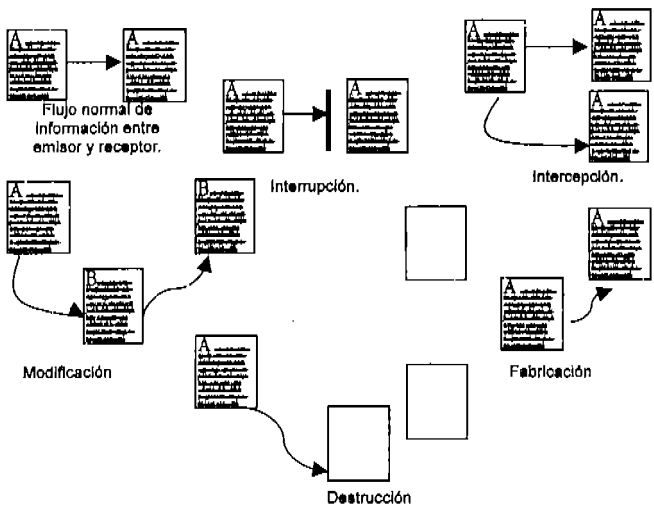


Gráfico 1.3 – Tipos de Ataques Activos. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989–1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org*. Capítulo 6–Página 59.

CAPÍTULO 2

2.1 SEGURIDAD FÍSICA

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); 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. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no.

Así, la **Seguridad Física** consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"[3]. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto dentro y fuera del 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.

---

[3] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000. *http://www.kriptopolis.com*

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

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

2.1.1 CONTROL DE ACCESOS

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

2.2 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 cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la **Seguridad Lógica** consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Los objetivos que se plantean serán:

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

2.2.1 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 la 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.

Al respecto, el National Institute for Standars and Technology (NIST)[4] ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

2.2.2 IDENTIFICACIÓN Y AUTENTIFICACIÓN

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.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, etc.
2. Algo que la persona **posee:** por ejemplo una tarjeta magnética.
3. Algo que el individuo **es** y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. Algo que el individuo es capaz de **hacer:** por ejemplo los patrones de escritura.

[4] *http://www.nist.gov*

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.

2.2.3 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.

2.2.4 TRANSACCIONES

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

2.2.5 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.

2.2.6 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**
- **Escritura**
- **Ejecución**
- **Borrado**

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

- **Creación**
- **Búsqueda**

2.2.7 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.

2.2.8 CONTROL DE ACCESO INTERNO

2.2.8.1 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.
- **Caducidad y control**: este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el periodo mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un periodo máximo que puede transcurrir para que éstas caduquen.

2.2.8.2 ENCRIPTACIÓN

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

2.2.8.3 LISTAS DE CONTROL DE ACCESOS

Se refiere a un registro donde se encuentran los nombres de los usuarios 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.

2.2.8.4 LÍMITES SOBRE LA INTERFASE DE USUARIO

Esto 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.

2.2.8.5 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.

2.2.9 CONTROL DE ACCESO EXTERNO

2.2.9.1 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.

2.2.9.2 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.

2.2.9.3 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.

2.2.9.4 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

CAPÍTULO 3

3.1 DELITOS INFORMÁTICOS

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Adicionalmente, la OCDE (Organización e Cooperación y Desarrollo Económico) elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran elegir un marco de seguridad para los sistemas informáticos.

En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

3.2TIPOS DE DELITOS INFORMÁTICOS

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

a. Fraudes cometidos mediante manipulación de computadoras.
b. Manipulación de los datos de entrada.
c. Daños o modificaciones de programas o datos computarizados.

Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información. Ellas son:

- "Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos."[5]

[5] CARRION, Hugo Daniel. **Tesis** "Presupuestos para la Punibilidad del Hacking". Julio 2001. *www.delitosinformáticos.com/tesis.htm*

3.2.1 CONCLUSIÓN

Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, es un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

No solo debe pensarse en la forma de castigo, sino algo mucho más importante como lograr probar el delito. Este sigue siendo el principal inconveniente a la hora de legislar por el carácter intangible de la información.

"Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía (...).

Y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras, a la antigua usanza. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día. Mejores y más rápidos mecanismos de legislación, juicios y sentencias...quizás algún día."[6].

[6] SCHNEIER, Bruce. Secrets & Lies. Página 28–29.

3.3 AMENAZAS HUMANAS

Este capítulo trata sobre cada uno de los personajes que pueden ser potenciales atacantes de nuestro sistema: el mundo under y el personal perteneciente a la organización.

En el presente sólo se tratará de exponer el perfil de la persona encargada de una de las principales, (publicitariamente), si bien no la mayor amenaza que acechan nuestro sistema Informático; para luego sí entrar en las formas de ataques propiamente dichos.

Se mueven en una delgada e indefinida barrera que separa lo legal de lo ilegal. Las instituciones y las multinacionales del software les temen, la policía los persigue y hay quien los busca para contratarlos. Se pasean libremente por las mayores computadoras y redes del mundo sin que ellas tengan secretos.

Como expresa Cybor, hay quienes los llaman piratas y delincuentes. Ellos reivindican su situación e intentan aclarar las diferencias entre los distintos clanes del Underground asegurando que sus acciones se rigen por un código ético.

3.3.1 LA CONEXIÓN HACKER – NERD

Un **Hacker** es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (Free Information), distribución de software sin costo y la globalización de la comunicación.

Contrariamente al mito popular, no es necesario ser un nerd para ser un hacker. Ayuda, sin embargo, y muchos hackers son nerds.

Al ser un marginado social, el nerd puede mantenerse concentrado en las cosas realmente importantes, como pensar y hackear.

Por esta razón, muchos hackers han adoptado la etiqueta nerd" e incluso utilizan el término "Geek" como insignia de orgullo: es una forma de declarar su propia independencia de las expectativas sociales normales.

3.3.2 CRACKERS

Los **Crackers**, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la manera equivocada o simplemente personas que hacen daño solo por diversión. Los hackers opinan de ellos que son "... Hackers mediocres, no demasiados brillantes, que buscan violar (literalmente "break") un sistema".

3.3.3 PHREAKERS

El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que lo Phreakers son Cracker de las redes de comunicación. Personas con amplios (a veces mayor que el de los mismos empleados de las compañías telefónicas) conocimientos en telefonía.

3.3.4 CARDING – TRASHING

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabajaba para conseguir una tarjeta de crédito ajena. Así nació:

1. El **Carding**, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacking y el Cracking, mediante los cuales se consiguen los números de las tarjetas.
2. El **Trashing**, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

3.3.5 OTROS HABITANTES DEL CIBERESPACIO

3.3.5.1 GURÚS

Son considerados los maestros y los encargados de "formar" a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas.

3.3.5.2 LAMERS O SCRIPT–KIDDERS

Son aficionados jactosos. Prueban todos los programas (con el título "como ser un hacker en 21 días") que llegan a sus manos. Generalmente son los responsables de soltar virus y bombas lógicas en la red sólo con el fin de molestar y que otros se enteren que usa tal o cual programa. Son aprendices que presumen de lo que no son aprovechando los conocimientos del hacker y lo ponen en práctica sin saber.

3.3.5.3 COPYHACKERS

Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).

3.3.5.4 BUCANEROS

Son comerciantes sucios que venden los productos crackeados por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los copyhackers. Son personas sin ningún (o escaso) conocimiento de informática y electrónica.

3.3.5.5 NEWBIE

Son los novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido.

3.3.5.6 WANNABER

Es aquella persona que desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consiga avanzar en sus propósitos.

3.3.5.7 SAMURAI

Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers. Se basan en el principio de que cualquiera puede ser atacado y saboteado, solo basta que alguien lo desee y tenga el dinero para pagarlo.

3.3.5.8 PIRATAS INFORMÁTICOS

Este personaje (generalmente confundido con el hacker) es el realmente peligroso desde el punto de vista del Copyright, ya que copia soportes audiovisuales (discos compactos, cassettes, DVD, etc.) y los vende ilegalmente.

3.3.5.9 CREADORES DE VIRUS

Si de daños y mala fama se trata estos personajes se llevan todos los premios. Aquí, una vez más, se debe hacer la diferencia entre los creadores:

que se consideran a sí mismos desarrolladores de software; y los que infectan los sistemas con los virus creados. Sin embargo es difícil imaginar que cualquier "desarrollador" no se vea complacido al ver que su "creación" ha sido ampliamente "adquirida por el público".

3.4 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70%[7] son causados por el propio personal de la organización propietaria de dichos sistemas ("Inside Factor").

Hablando de los Insiders Julio C. Ardita[8] explica que "(...) desde mitad de 1996 hasta 1999 la empresa tuvo dos casos de intrusiones pero en el 2000 registramos siete, de las cuales 5 eran intrusos internos o ex–empleados (...)".

El siguiente gráfico detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos.

---

[7] Fuente: Cybsec S.A. *http://www.cybsec.com*

[8] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

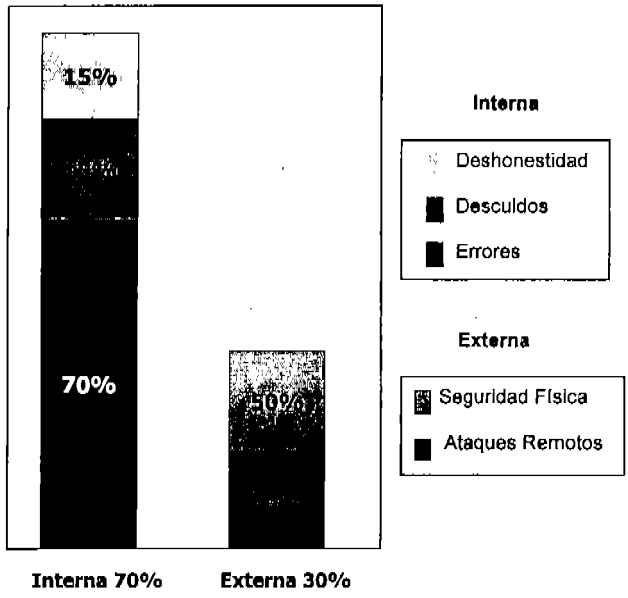


Grafico 2.1 - Intrusiones Fuente: *http://www.cybsec.com*

3.5 AMENAZAS LÓGICAS

La Entropía es una magnitud termodinámica que cuantifica el grado de desorden de un sistema; y según las leyes físicas todo sistema tiende a su máxima entropía. Si extrapolamos este concepto a la Seguridad resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir:

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

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.
- Todo sistema es inseguro.

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

3.6 DETECCIÓN DE INTRUSOS

A finales de 1996, Dan Farmer creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow). Los problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados. Así por ejemplo, un problema de seguridad del grupo rojo es un equipo que tiene el servicio de FTP anónimo mal configurado.

Los problemas de seguridad del grupo amarillo son menos serios pero también reseñables. Implican que el problema detectado no compromete inmediatamente al sistema pero puede causarle serios daños o bien, que es

necesario realizar tests más intrusivos para determinar si existe o no un problema del grupo rojo.

La tabla 6.1 resume los sistemas evaluados, el número de equipos en cada categoría y los porcentajes de vulnerabilidad para cada uno. Aunque los resultados son límites superiores, no dejan de ser... escandalosos.

Tipo de sitio	# Total sitios testeados	% Total Vulnerables	% Yellow	% Red
Bancos	660	68,34	32,73	35,61
Créditos	274	51,1	30,66	20,44
Sitios Federales US	47	61,7	23,4	38,3
News	312	69,55	30,77	38,78
Sexo	451	66,08	40,58	25,5
TOTALES	**1.734**	**64,93**	**33,85**	**31,08**
Grupo aleatorio	**469**	**33,05**	**15,78**	**17,27**

Tabla 2.1 – Porcentaje de Vulnerabilidades por tipo de sitio. Fuente: *http://www.trouble.org/survey*

Como puede observarse, cerca de los dos tercios de los sistemas analizados tenían serios problemas de seguridad y Farmer destaca que casi un tercio de ellos podían ser atacados con un mínimo esfuerzo.

3.7 IDENTIFICACIÓN DE LAS AMENAZAS

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

- **Data Corruption:** la información que no contenía defectos pasa a tenerlos.
- **Denial of Service (DoS):** servicios que deberían estar disponibles no lo están.
- **Leakage:** los datos llegan a destinos a los que no deberían llegar.

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

La Tabla 6.2 detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos[9].

[9] HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org.* Capítulo 6–Página 71

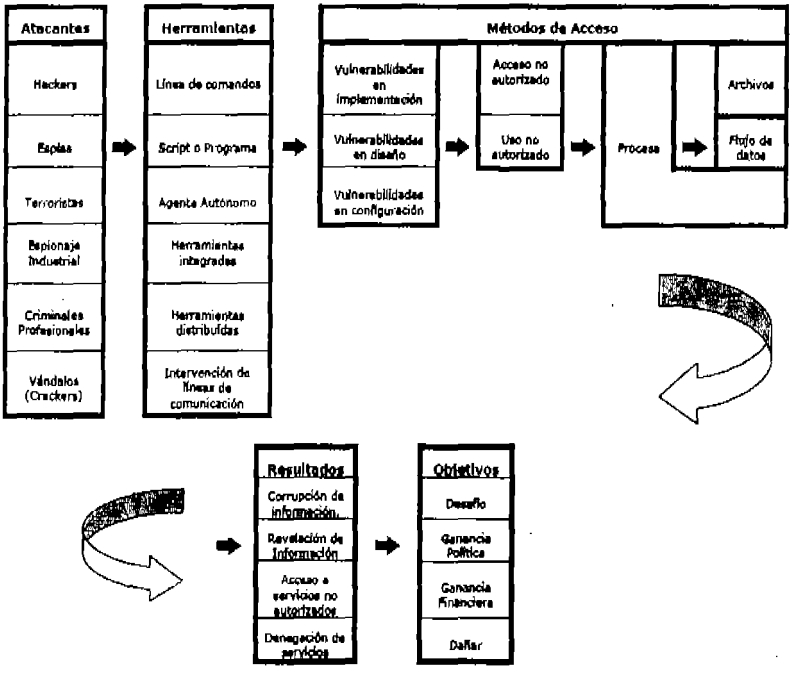


Tabla 2.2. Detalle de Ataques. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. http://www.cert.org. Capítulo 6–Página 71

Cualquier adolescente de 15 años (Script Kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Nota I: En 1992 el DISA[10] realizó un estudio durante el cual se llevaron a cabo 38.000 ataques a distintas sitios de organizaciones gubernamentales (muchas de ellas militares). El resultado de los ataques desde 1992 a 1995 se resume en el siguiente cuadro[11]:

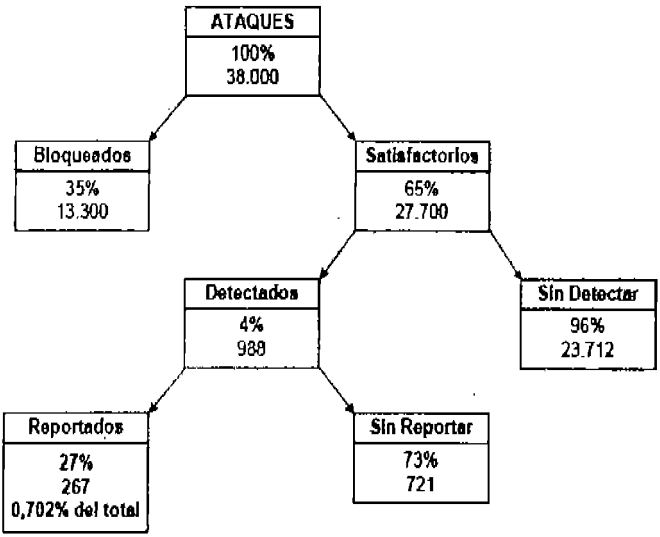


Gráfico 2.2 – Porcentaje de Ataques. Fuente: *http://www.disa.mil*

Puede observarse que solo el 0,70% (267) de los incidentes reportados. Luego, si en el año 2000 se denunciaron 21.756 casos eso arroja 3.064.225 incidentes en ese año.

[10] DISA (Defense Information System Agency). *http://www.disa.mil*
[11] Idem Capítulo 12–Página 168.G

3.8 TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros.

Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de las mismas. Cada uno de los ataques abajo descriptos será dirigido remotamente. Se define **Ataque Remoto** como un ataque iniciado contra una máquina sobre la cual el atacante no tiene control físico. Esta máquina es distinta a la usada por el atacante y será llamada **Víctima**.

3.8.1 INGENIERÍA SOCIAL

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad.

3.8.2 INGENIERÍA SOCIAL INVERSA

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería Social.

3.8.3 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo recuerda, lo arroja a la basura.

3.8.4 ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

3.8.4.1 SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente.

3.8.4.2 DECOY (SEÑUELOS)

Son programas diseñados con la misma interface que otro original.

3.8.4.3 SCANNING (BÚSQUEDA)

La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular.

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

3.8.4.3.1 TCP Connect Scanning

Esta es la forma básica del scaneo de puertos TCP. SI el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

3.8.4.3.2 TCP SYN Scanning

La técnica TCP SYN Scanning, implementa un scaneo de "media-apertura", dado que nunca se abre una sesión TCP completa.

3.8.4.3.3 TCP FIN Scanning– Stealth Port Scanning

Este tipo de Scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

3.8.4.3.4 Fragmentation Scanning

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

3.8.4.4 EAVESDROPPING–PACKET SNIFFING

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Packet Sniffers, son programas que monitorean los paquetes que circulan por la red.

Un Sniffers consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).

3.8.4.5 SNOOPING–DOWNLOADING

Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de

documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

3.8.5 ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo.

3.8.5.1 SPOOFING–LOOPING

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver a continuación Ataques de Modificación y Daño).

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

3.8.5.2 SPOOFING

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing.

3.8.5.3 IP SPLICING–HIJACKING

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

3.8.5.4 UTILIZACIÓN DE BACKDOORS

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas.

Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo"[12].

[12] HUERTA, Antonio Villalón. "Seguridad en Unix y redes". Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000. Capítulo 5–Página 81. *http://www.kriptopolis.com*

3.8.5.5 UTILIZACIÓN DE EXPLOITS

Son programas para explotar "agujeros" en los algoritmos de encriptación y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo.

3.8.5.6 OBTENCIÓN DE PASSWORDS

Este método comprende la obtención por "Fuerza Bruta" de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. atacados.

Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error.

Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

3.8.5.6.1 Uso de Diccionarios

Los Diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave hallada.

3.8.6 DENIAL OF SERVICE (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua.

La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.
2. Se necesita cubrir inmediatamente sus acciones o un uso abusivo de CPU. Para ello provoca un "crash" del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio Web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.

5. El administrador del sistema tiene un proceso que no puede "matar" en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DoS deteniendo los servicios.

3.8.6.1 JAMMING O FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

3.8.6.2 SYN FLOOD

El SYN Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista under Phrack; y se basa en un "saludo" incompleto entre los dos hosts.

SYN Flood aprovecha la mala implementación del protocolo TCP, el problema es que muchos sistemas operativos tienen un límite muy bajo en el número de conexiones "semiabiertas" que pueden manejar en un momento determinado (5 a 30). Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan

llegando. Las conexiones "semiabiertas" van caducando tras un tiempo, liberando "huecos" para nuevas conexiones, pero mientras el atacante mantenga el SYN Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

3.8.6.3 CONNECTION FLOOD

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre con el caso del SYN Flood) para mantener fuera de servicio el servidor.

3.8.6.4 NET FLOOD

En el caso de Net Flooding el atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.

En casos así el primer paso a realizar es el ponerse en contacto con el Proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea.

El siguiente paso consiste en localizar las fuentes del ataque e informar a sus administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento.

3.8.6.5 LAND ATTACK

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows.

El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

3.8.6.6 SMURF O BROADCAST STORM

Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Gráficamente:

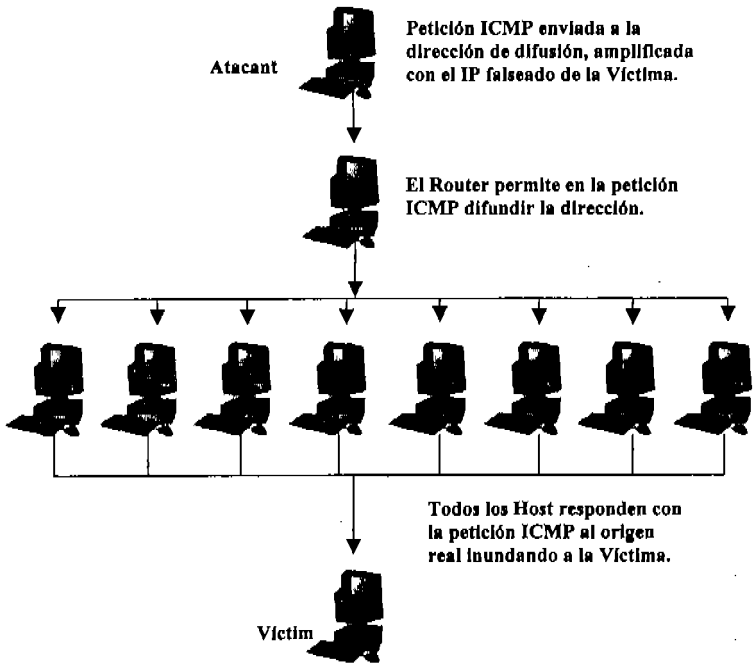


Gráfico 2.3 – Ataque Smurf

3.8.6.7 OOB, SUPERNUKE O WINNUKE

Un ataque característico, y quizás el más común, de los equipos con Windows es el Nuke, que hace que los equipos que escuchan por el puerto NetBIOS sobre TCP/UDP 137 a 139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados.

Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina víctima detecta como inválidos pasando a un estado inestable. OOB es el término normal, pero realmente consiste en configurar el bit Urgente

(URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido.

3.8.6.8 TEARDROP I Y II–NEWTEAR–BONK-BOINK

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes.

Los ataques tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

3.8.6.9 E–Mail Bombing--Spamming

El e-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario.

El Spamming, en cambio se refiere a enviar un e–mail a miles de usuarios, haya estos solicitado el mensaje o no. Es muy utilizado por las empresas para publicitar sus productos.

3.8.7 ATAQUES DE MODIFICACIÓN–DAÑO

1. TAMPERING O DATA DIDDLING: Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos.

2. BORRADO DE HUELLAS: Son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo.
3. ATAQUES MEDIANTE JAVA APPLETS
4. ATAQUES CON JAVASCRIPT Y VBSCRIPT
5. ATAQUES MEDIANTE ACTIVEX: ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft. Es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc.
6. VULNERABILIDADES EN LOS NAVEGADORES

3.8.8 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
5. Filtrar el tráfico IP Spoof.

6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, **la capacitación continúa del usuario**.

3.9 CREACIÓN Y DIFUSIÓN DE VIRUS

Quizás uno de los temas más famosos y sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los Virus.

Pero como siempre en esta obscura realidad existe una parte que es cierta y otra que no lo es tanto. Para aclarar este enigma veamos porque se eligió la palabra Virus (del latín Veneno) y que son realmente estos "parásitos".

Virus Informático (VI): Pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando réplicas de sí mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica).[13]

[13] Revista Virus Reports. Ediciones Ubik Número 16–Página 2.

3.9.1 DESCRIPCIÓN DE UN VIRUS

Si bien un VI es un ataque de tipo Tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o a través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse rápidamente.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.EXE, .COM, .DLL, etc.), los sectores de Boot y la Tabla de Partición de los discos.

Actualmente los que causan mayores problemas son los macro-virus y script–virus, que están ocultos en simples documentos, planillas de cálculo, correo electrónico y aplicaciones que utiliza cualquier usuario de PC. La difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no dependen de un sistema operativo en particular, ya que un documento puede ser procesado tanto en Windows 95/98/NT/2000, como en una Macintosh u otras.

3.9.1.1 TIPOS DE VIRUS

Un virus puede causar daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada y nadie en su sano juicio deseará ejecutarlo.

Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para que su "programa" pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas:

3.9.1.1.1 Archivos Ejecutable (virus ExeVir)

El virus se adosa a un archivo ejecutable y desvía el flujo de ejecución a su código, para luego retornar al huésped y ejecutar las acciones esperadas por el usuario. Al realizarse esta acción el usuario no se percata de lo sucedido. Una vez que el virus es ejecutado se aloja en memoria y puede infectar otros archivos ejecutables que sean abiertos en esa máquina.

3.9.1.1.2 Virus en el Sector de Arranque (Virus ACSO Anterior a la Carga del SO)

En los primeros 512 bytes de un disquete formateado se encuentran las rutinas necesarias para la carga y reconocimiento de dicho disquete. Entre ellas se encuentra la función invocada si no se encuentra el Sistema Operativo. Es decir que estos 512 bytes se ejecutan cada vez que se intenta arrancar (bootear) desde un disquete (o si se dejó olvidado uno en la unidad y el orden de booteo de la PC es A: y luego C:). Luego, esta área es el objetivo de un virus de booteo.

Se guarda la zona de booteo original en otro sector del disco (generalmente uno muy cercano o los más altos). Luego el virus carga la antigua zona de booteo. Al arrancar el disquete se ejecuta el virus (que obligatoriamente debe tener 512 bytes o menos) quedando residente en

memoria; luego ejecuta la zona de booteo original, salvada anteriormente. Una vez más el usuario no se percata de lo sucedido ya que la zona de booteo se ejecuta iniciando el sistema operativo (si existiera) o informando la falta del mismo.

3.9.1.1.3 Virus Residente

Como ya se mencionó, un virus puede residir en memoria. El objetivo de esta acción es controlar los accesos a disco realizados por el usuario y el Sistema Operativo. Cada vez que se produce un acceso, el virus verifica si el disco o archivo objetivo al que se accede, está infectado y si no lo está procede a almacenar su propio código en el mismo. Este código se almacenará en un archivo, tabla de partición, o en el sector de booteo, dependiendo del tipo de virus que se trate.

3.9.1.1.4 Macrovirus

Estos virus infectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Últimamente son los más expandidos, ya que todos los usuarios necesitan hacer intercambio de documentos para realizar su trabajo.

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macrovirus.

3.9.1.1.5 Virus de Mail

El "último grito de la tecnología" en cuestión de virus. Su modo de actuar, al igual que los anteriores, se basa en la confianza excesiva por parte del usuario: a este le llega vía mail un mensaje con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

3.9.1.1.6 Virus de Sabotaje

Son virus construidos para sabotear un sistema o entorno específico. Requieren de conocimientos de programación pero también una acción de inteligencia que provea información sobre el objetivo y sus sistemas.

3.9.1.1.7 Hoax, los Virus Fantasmas.

El auge del correo electrónico generó la posibilidad de transmitir mensajes de alerta de seguridad. Así comenzaron a circular mensajes de distinta índole (virus, cadenas solidarias, beneficios, catástrofes, etc.) de casos inexistentes

3.9.1.1.8 Virus de Applets Java y Controles ActiveX

Este tipo de virus se copian y se ejecutan a sí mismos mientras el usuario mantiene una conexión a Internet.

3.9.1.1.9 Reproductores–Gusanos

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

3.9.1.1.10 Caballos de Troya

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

3.9.1.1.11 Bombas Lógicas

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada o dado algún evento particular en el sistema, bien destruye y modifica la información o provoca la baja del sistema.

3.9.1.2 MODELO DE VIRUS INFORMÁTICO

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

1. **Módulo de Reproducción:** es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticiamente, permitiendo su transferencia a otras computadoras.
2. **Módulo de Ataque:** Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.
3. **Módulo de Defensa:** Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus.

3.9.2 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS

Los virus informáticos no afectan (en su gran mayoría) directamente el hardware sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la siguiente clasificación se ha tenido en cuenta que el daño es una acción de la computadora, no deseada por el usuario:

a) **Daño Implícito:** es el conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar su accionar y propagación.
b) **Daño Explícito:** es el que produce la rutina de daño del virus.

Con respecto al modo y cantidad de daño, encontramos:

A. **Daños triviales:** daños que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario.
B. **Daños menores:** daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos.
C. **Daños moderados:** los daños que el virus provoca son formatear el disco rígido o sobrescribir parte del mismo.
D. **Daños mayores:** algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad también infectadas.
E. **Daños severos**: los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos.
F. **Daños ilimitados:** el virus "abre puertas" del sistema a personas no autorizadas.

3.9.3 LOS AUTORES

Tras su alias (nic), los creadores de virus sostienen que persiguen un fin educacional para ilustrar las flaquezas de los sistemas a los que atacan. Pero... ¿es necesario crear un problema para mostrar otro?

La creación de virus no es ilegal, y probablemente no debería serlo: cualquiera es dueño de crear un virus siempre y cuando lo guarde para sí. Infectar a otras computadoras sin el consentimiento de sus usuarios es inaceptable, esto sí es un delito y debería ser penado, como ya lo es un algunos países.

Inglaterra pudo condenar a ¡18 meses! de prisión al autor de SMEG. Sin embargo, el autor del virus Loverletter no fue sentenciado porque la legislación vigente en Filipinas (su país de origen) no era adecuada en el momento del arresto.

Existen otros casos en que el creador es recompensado con una oferta de trabajo millonaria por parte de multinacionales. Este, y no las condenas, es el mensaje que reciben miles de jóvenes para empezar o continuar desarrollando virus y esto se transforma en una "actividad de moda", lejos de la informática ética sobre la cual deberían ser educados.

3.9.4 PROGRAMA ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Debe tenerse en cuenta que:

- Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.
- No será eficaz el 100% de los casos, no existe la protección total y definitiva.

Las funciones presentes en un antivirus son:

1. **Detección:** se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
2. **Identificación de un virus:** existen diversas técnicas para realizar esta acción:
    a. **Scanning**: técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales).

b. **Heurística**: búsqueda de acciones potencialmente dañinas perteneciente a un virus informático.

3. **Chequeadores de Integridad**: Consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma.

Es importante diferencia los términos **detectar:** determinación de la presencia de un virus e **identificar:** determinación de qué virus fue el detectado. Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

3.9.4.1 MODELO DE UN ANTIVIRUS

Un antivirus puede estar constituido por dos módulos principales y cada uno de ellos contener otros módulos.

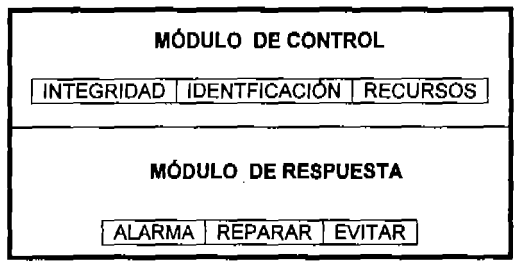


Gráfico 2.4 – Modelo de un Antivirus

3.9.4.2 UTILIZACIÓN DE LOS ANTIVIRUS

La mayoría de los antivirus ofrecen la opción de reparación de los archivos dañados. Puede considerarse este procedimiento o la de recuperar el/los archivos perdidos desde una copia de seguridad segura.

3.9.5 CONSEJOS

Aunque existe una relativa concientización, generalmente no se toman todas las precauciones necesarias para anular el peligro. No basta con tener un antivirus, sino que éste hay que actualizarlo periódicamente para contemplar los nuevos virus que van apareciendo.

Además de poseer la cualidad de chequeo manual, detección y eliminación, debe ser sobre todo capaz de actuar como vacuna o filtro, impidiendo la entrada de los nuevos virus que aparecen cada día. De esta forma, aunque al usuario se le olvide pasar el antivirus, sabe que al menos existe una protección automática.

CAPÍTULO 4

4.1 SEGURIDAD PARA LA UNIVERSIDAD DE SOTAVENTO

En el plantel universitario no existe una adecuada seguridad en cuanto a la información de calificaciones, altas, bajas de alumnos y a todos los sistemas de pagos que se maneja ahí, sería bueno implementar seguridad de información en todas las maquinas, ya que se encuentran todas en red.

Los puntos más relevantes que en un momento dado pueden perjudicar a la Universidad de Sotavento son los que describiremos a continuación:

4.1.1 La Seguridad Informática.

La manera en que se puede solucionar el problema de infiltración, sustracción, daño por virus u otras amenazas, es que la información de las computadoras en la universidad, adquieran un software que maneje sesiones de usuarios pero a nivel de red es decir creando una jerarquía de usuarios con permisos para cada uno de estos.

Un ejemplo de esto es que cuando un usuario "alumno" al iniciar su sesión solo tendrá acceso a cierta parte del software, es decir que solo pueda utilizar la paquetería permitida para este usuario y guardando la

información en un área designada a cada usuario; el usuario solamente podrá modificar su ambiente de trabajo si lo desea, pero no podrá instalar o desinstalar nuevas aplicaciones.

Con lo antes citado facilitara el manejo de la información y la seguridad de esta, ya que el sistema debe llevar un registro interno de cada usuario: en el uso de la computadora, la hora y la fecha que ingreso.

Con la problemática de los virus se tienen ciertas limitantes para su erradicación al 100%. Para ello se pueden tomar las siguientes medidas, contar con una firma de alguna compañía de antivirus con la finalidad de tener un respaldo inmediato y continuo en la presencia de cualquier amenaza. Otra alternativa que se daría en conjunto con el antivirus sería la implementación de un firewall para prevenir las amenazas internas o externas de la red.

Algunas de las recomendaciones de antivirus que pueden ser utilizados para lograr este objetivo dentro del plantel educativo:

McAfee	$ 415.00 al año
Kaspersky Lab Internet Security 6.0 - 2 Year License	$ 1,000.00
Symantec Norton AntiVirus 2007	$ 170.00 al año

- Control de la Red:

- GFI Events Manager 7.1
- GFI LANguard N.S.S. $6,300.00 para 32 IP´s

# NODOS PERMITIDOS	[illegible]	[illegible]
3 nodos	ESM3	$ 10,150.00
5 nodos	ESM5	$ 14,350.00
10 nodos	ESM10	$ 20,650.00
25 nodos	ESM25	$ 42,700.00
50 nodos	ESM50	$ 75,600.00
100 nodos	ESM100	$ 140,350.00
150 nodos	ESM150	$ 211,750.00
250 nodos	ESM250	$ 277,200.00
500 nodos	ESM500	$ 403,200.00
más de 500 nodos	ESM500+	Contactar con comercial
Licencia de consultor *	ESMCON	Contactar con comercial

4.1.2 La Privacidad o Confidencialidad de la Información.

Para mantener la privacidad y confidencialidad del la información del usuario y sus datos privados es necesario que no hagan lo siguiente:

- No dar el nombre de usuario y contraseña a nadie y crearlas lo más seguras posibles.
- No realizar compras por Internet, no dar información sobre su domicilio o intereses ni proporcionar algo que pueda comprometerlos o identificarlos aunque sea un poco.
- No realizar descargas desde programas de descargas.

Pero esto no es lo único que se tiene que hacer para asegurar totalmente la privacidad del usuario, otra manera de tener privacidad y confidencialidad es teniendo un espacio reservado para el usuario y no guardando ningún tipo de información personal o importante en el equipo y si a de hacerlo mantener estos con llave, es decir, poniéndola con contraseña y en lugares difíciles de encontrar (modo oculto) en carpetas.

Para cumplir los objetivos será necesario que el administrador de la red sea el que provea las cuentas, las llaves y los accesos restringidos de acuerdo con la jerarquía de los usuarios.

Programas recomendados:

PROGRAMA	COSTO
GFI Network Server Monitor	$ 5,040.00 por 50 IP´s.
McAfee Enterprise Control de acceso a la red	$ 2,500.00 al año

4.1.3 El Control sobre la Información

Para tener el control sobre la información se debe de tener un buen manejo de esta, es decir, quién va a tener acceso a ella y quién no, esto se logra por medio de filtros de identificación, es decir usuario y contraseña; y dependiendo de esto, le permitirá acceso a cierto tipo de información.

Para poder implementar el control de la información en la Universidad de Sotavento será necesario la implementación de un software que sirva como gestor con los usuarios, donde se implementara el proceso de identificación (usuario-contraseña) o bien, la implementación de hardware especializado como los detectores de iris, huellas digitales o firmas electrónicas.

Los programas recomendados:

PROGRAMA	
McAfee Enterprise Control de acceso a la red	$ 2,500.00 al año
Llaves de identificación USB	$ 1,750.00 permanentemente
GFI Events Manager 7.1	$ 10,150.00 - $ 403,200.00 Variable

4.1.4 Auditoría de Sistemas

En la Universidad de Sotavento no se cuenta con auditorías internas y externas. Dando como consecuencia la falta de registros del control de usuarios, el inventario de computadoras y el inventario de los programas que se requieren.

No cuenta con registros o bitácoras de la asignación de equipos, o fallas presentadas en la red interna o en ausencia de Internet. Así también como las anomalías de virus o programas malíciosos que se encuentran en los equipos.

Las recomendaciones para satisfacer estas necesidades serían la implantación de estándares de auditoría de sistemas en la Universidad de Sotavento. Con la finalidad de que se imprima los reportes tanto de usuario, súper usuarios y administradores de cuando utilizaron en ciertos recursos y aplicaciones del sistema.

Recomendaciones:

1. Es crear un estándar de las funciones de los encargados (COBIT)
2. Tener actualizados los inventarios, tanto físicos como contables.
3. Tener bien definidos los puestos de trabajo así como los perfiles
4. Y calendarizar las fechas de las auditorías internas

Programas recomendados:

MySQL	Software Gratuito (Manejo de usuarios y password)
GFI Network server monitor	$ 5,040.00

4.1.5 Amenazas Humanas Externas e Internas.

La Universidad de Sotavento mantiene diversas amenazas tanto mal intencionadas como intencionadas y para ello es necesario tener un buen equipo anti-hacker, antivirus y contraseñas difíciles para el acceso al sistema, así como un filtro que prohíba la descarga de archivos en el equipo de cómputo.

Para eliminar las amenazas externas se tendría que llevar un control de quien va a utilizarlas, tener una cuenta de invitado con recursos limitados y mantener un sistema de monitoreo.

Recomendaciones:

1. Se deberá contratar personal de vigilancia
2. Se tendrán que instalar protecciones en los laboratorios, centros de cómputos y oficinas administrativas.
3. Instalar un firewall capa 5

Programas recomendados:

Firewall	Gratuito
Antivirus McAfee	$ 415.00 al año
GFI Network server monitor	$ 5,040.00

4.1.6 Amenazas No Maliciosas (empleados ignorantes).

La única forma de erradicar este problema de amenazas es dando cursos de capacitación para el buen uso y manejo de los equipos. Instruirlos de todos los peligros y amenazas latentes que se encuentran en la red. Y transmitir el riesgo de instalar programas no autorizados por el encargado, ya que estos riesgos pueden ser perdida de información, infiltración al sistema y problemas legales por licenciamiento.

Recomendaciones:

1. Contratar más personal administrativo, de preferencia tener dos turnos.
2. Contar con más becados
3. Brindar capacitación cada 3 meses a los encargados y becarios.
4. Realizar cursos a los usuarios por lo menos una vez al año.
5. Auditorías internas.

Programas recomendados:

Programa	Precio
Antivirus McAfee	$ 415.00 al año
Firewall	Gratuito

4.1.7 Desastres Naturales (Incendio, Tormentas Eléctricas, Inundaciones, etc.)

Para proteger los equipos de cómputo de los desastres naturales es muy difícil. Una manera de prever los incendios es contar con detectores de humo y extinguidores, en caso de terremotos tener una alarma antisismos y en cuanto a tormentas eléctricas siempre es bueno tener el equipo conectado a tierra y contar con sistemas de respaldo de energía (UPS).

Recomendaciones:

1. Hacer una brigada contra siniestros. Donde participen todas las facultades
2. Tener puntos de reunión
3. Contar con detectores de humo.
4. Tener capacitado al personal para el uso de extinguidores y de control de grupo.
5. Tener un plan de contingencia
6. Tener calendarizados las revisiones de equipos.

Programas recomendados:

- Solo tener respaldo de toda la base de datos en un servidor independiente al que se encuentra en el plantel, o bien, todo respaldado en discos duros o Dvd´s fuera del plantel.

4.1.8 Control de Accesos Externos e Internos.

El control de acceso interno.- Para tener un control más sólido en la institución es necesario que los password de los usuarios sean cambiados cada mes o dos meses creando caducación de password para hacerlo de manera automática, en cuanto a los demás archivos que maneje cada usuario, deben estar y guardarse encriptados y solo pueda entrar el usuario con su contraseña, así como manejar una bitácora de que usuario, hora, fecha y a que recursos del sistema entro.

El control de acceso externo.- Para tener el control en este medio solo es posible instalando dispositivos de control de puertos, un buen firewall, y tener una cuenta de invitado muy limitada y restringida para usuarios que no pertenezcan al plantel educativo.

Recomendaciones:

1. Interno:
    a. Manejo de permisos de usuario.
    b. Encriptación de la información.
2. Externo:
    a. Instalación de Firewall.
    b. Instalación de Antivirus.

Programas recomendados:

Producto	Precio
Antivirus McAfee	$415.00 al año
Firewall	Gratuito
MySQL	Software Gratuito (Manejo de usuarios y password)
GFI Network server monitor	$ 5,040.00

4.1.9 Palabras Claves (Passwords)

En la institución se debe de manejar un usuario y contraseña, la contraseña se debe de cambiar cada mes o dos meses pidiendo de manera automática que se cambie al pasar este tiempo y que al cambiarla la cambie automáticamente también para los archivos encriptados y que tengan un nivel de dificultad alto para que no sean fáciles de averiguar.

Programas recomendados:

Programa	Costo
MySQL	Software Gratuito (Manejo de usuarios y password)
Firma Digital USB	$ 1,750.00 permanente
Código PHP	

4.1.10 Encriptación

Para mantener la seguridad de la Información en la Universidad de Sotavento, es necesario que se tengan encriptados todos los archivos, así solamente podrá abrirlo quien cuente con la clave (password) para poder ver el contenido y modificarlo.

Programas recomendados:

Programa	Costo
CryptoForge	$ 299.50 cada seis meses
File Waster	Gratuito
Criptod	Gratuito

4.1.11 Los Hackers, LAMERS O SCRIPT–KIDDERS

Para protegerse de los hacker solamente se puede contar con firewall, contraseñas difíciles, dispositivos de puertos entrantes, archivos encriptados y muchos filtros de accesos, y antivirus actualizados así como spyware para protegerla mas de los intrusos.

Programas recomendados:

Programa	Precio
CryptoForge	$ 299.50 cada seis meses
MySQL	Software Gratuito (Manejo de usuarios y password)
Firma Digital USB	$ 1,750.00 permanente
Firewall	Gratuito
Antivirus McAfee	$ 415.00 al año
GFI Network server monitor	$ 5,040.00
GFI Events Manager 7.1	$10,150.00 - $403,200.00 Variable

4.1.12 Creadores de Virus

La solución sería el registro de que usuario se encuentra usando el sistema y el acceso de usuarios restringidos, y bloqueando la descarga de software, así un antivirus, firewall y spyware que no permita la creación o liberación de virus.

Programas recomendados:

Programa	Precio
CryptoForge	$ 299.50 cada seis meses
MySQL	Software Gratuito (Manejo de usuarios y password)
Firewall	Gratuito
Antivirus McAfee	$ 415.00 al año
AntiSpyware by Microsoft	Gratuito
AVG Anti-Spyware 7.5.1.43	Gratuito

4.1.13 Trashing (Cartoneo)

Crear un login y contraseña que le sea fácil de recordar al usuario pero que este tenga un nivel de seguridad alto, es decir que sea alfanumérico y este nunca lo tiene que escribir en ningún lado solo tenerlo en su memoria.

Recomendar a los usuarios de la Universidad de Sotavento que la construcción de paswords debe ser con letras y números. No deben ser números consecutivos (1,2,3,4...) y no deben de representar fechas de cumpleaños, aniversarios o algo que sea fácil de descifrar.

4.1.14 Scanning (Búsqueda)

Solo manda eco de los puertos abiertos.

Programas recomendados:

Programa	Costo
Superscan 2.06	$ 1,523 al año
Agnitum outpost firewall	Gratuito

4.1.15 Spoofing–Looping

Para detener el espionaje o el ultraje de información, se necesita tener cerrado todos los puertos que no se estén utilizando para no dejar una entrada disponible y los que se estén utilizando estarlos monitoreando y tenerlos con códigos de seguridad necesarios, en las validaciones de contraseña a la hora de ir validando contraseñas tras contraseñas solo

queda ir guardando un historial del orden en que se fueron ingresando y tener muy limitados los permisos de los usuarios para que ninguno tenga el suficiente permiso de entrar a la Base de Datos y manipularla.

Programas recomendados:

Programa	Precio
Superscan 2.06	$ 1,523 al año
Agnitum outpost firewall	Gratuito
Firewall	Gratuito
Antivirus McAfee	$ 415.00 al año
AntiSpyware by Microsoft	Gratuito

4.1.16 Utilización De Exploits

Este solo se puede evitar con un software que siempre este vigilando los puertos para que ninguno quede abierto y en caso que encuentre uno lo cierre.

Programas recomendados:

Programa	Precio
Superscan 2.06	$ 1,523 al año
Agnitum outpost firewall	Gratuito
Firewall	Gratuito
Antivirus McAfee	$ 415.00 al año
AntiSpyware by Microsoft	Gratuito

4.1.17 Virus En El Sector De Arranque (Virus Acso Anterior A La Carga Del So)

Son virus que llegan a dañar archivos de arranque solo se puede solucionar con antivirus y antispyware.

Programas recomendados:

Programa	Costo
Antivirus McAfee	$ 415.00 al año
Kaspersky Lab Internet Security 6.0 - 2 Year License	$ 1,000.00 al año
Symantec Norton AntiVirus 2007	$ 170.00 al año
AVG Anti-Spyware 7.5.1.43	Gratuito
AntiSpyware by Microsoft	Gratuito

4.1.18 Virus De Mail

Solo se pueden erradicar con antivirus y antispyware, y no abriendo correos de desconocidos o que marquen como peligrosos para el equipo.

Programas recomendados:

Programa	Costo
Antivirus McAfee	$ 415.00 al año
Kaspersky Lab Internet Security 6.0 - 2 Year License	$ 1,000.00 al año
Symantec Norton AntiVirus 2007	$ 170.00 al año
AVG Anti-Spyware 7.5.1.43	Gratuito
AntiSpyware by Microsoft	Gratuito

4.1.19 Reproductores–Gusanos

Es solo para prevenir su ingreso en el equipo de cómputo.

Programa	Costo
Antivirus McAfee	$ 415.00 al año
Kaspersky Lab Internet Security 6.0 - 2 Year License	$ 1,000.00 al año
Symantec Norton AntiVirus 2007	$ 170.00 al año
AVG Anti-Spyware 7.5.1.43	Gratuito
AntiSpyware by Microsoft	Gratuito

4.1.20 Caballos De Troya

Son virus que tienden a crear una rutina en el sistema de la computadora que no están permitidas para generar errores en el programa, para evitar esto se debe de tener antivirus antispyware y monitorear la red.

Programas recomendados:

Programa	Costo
Antivirus McAfee	$ 415.00 al año
Kaspersky Lab Internet Security 6.0 - 2 Year License	$ 1,000.00 al año
Symantec Norton AntiVirus 2007	$ 170.00 al año
AVG Anti-Spyware 7.5.1.43	Gratuito
AntiSpyware by Microsoft	Gratuito
GFI Network server monitor	$ 5,040.00

CONCLUSIÓN

Teniendo en cuenta que la seguridad hoy en dia es uno de los problemas más significativos de las empresas y es muy difícil tener un sistema 100% seguro y es por eso que damos las siguientes recomendaciones para minorizar las posibles amenazas en la que puede estar inmersa la Universidad de Sotavento.

En primer punto es crear estándares de todos los procesos informáticos. Implementar estándares nacionales e internacionales para lograr una buena estructura dentro de la organización.

En segundo término podemos considerar programas que se encuentran en el mercado para contrarrestar puntos muy específicos dentro del sistema de la Universidad de Sotavento:

- CryptoForge.
- MySQL (Manejo de usuarios y password).
- Firma Digital USB.
- Antivirus McAfee.
- Firewall.
- GFI Network server monitor.
- GFI Events Manager 7.1.

Y por ultimo crear una cultura informática para todos los usuarios de la Universidad de Sotavento, esta puede estar integrado por una cultura energética, el buen uso de los equipos y de la información que se transmite.

ANEXO

TABLAS

- **Tabla 2.1 – Porcentaje de Vulnerabilidades por tipo de sitio. Fuente**: *http://www.trouble.org/survey*
- **Tabla 2.2. Detalle de Ataques. Fuente:** HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org*. Capítulo 6–Página 71

GRÁFICOS

- **Gráfico 1.1 – Amenazas para la Seguridad**
- **Gráfico 1.2 – Tipos de Intrusos. Fuente:** CybSec S.A. *http://www.cybsec.com*
- **Gráfico 1.3 – Tipos de Ataques Activos. Fuente:** HOWARD, John D. Thesis: An Analysis of security on the Internet 1989–1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org*. Capítulo 6–Página 59.
- **Grafico 2.1 - Intrusiones Fuente:** *http://www.cybsec.com*
- **Gráfico 2.2 – Porcentaje de Ataques. Fuente:** *http://www.disa.mil*
- **Gráfico 2.3 – Ataque Smurf**
- **Gráfico 2.4 – Modelo de un Antivirus**

GLOSARIO

A

ActiveX: Lenguaje desarrollado por Microsoft para la elaboración de aplicaciones exportables a la red y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo. Véase también Root y SysOp.

Antivirus: Programa que es encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

Applet: Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente.

Archivo: Conjunto bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

Ataque: Intento de traspasar un control de seguridad de un sistema.

B

Backdoor: Puerta trasera de entrada a una computadora, programa o sistema en general. Es utilizado para acceder sin usar un procedimiento normal.

Bit: En informática, unidad mínima de información.

BroadCast: Difusión. Tipo de comunicación en que todo posible receptor es alcanzado por una sola transmisión. Véase también **Multicast.**

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo.

Byte: Combinación de **Bits**. En la representación más común 8 bits forman un byte.

C

Caballo de Troya: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño. Véase también **Troyano.**

CERT/CC (Computer Emergency Response Team/Coordination Center): Grupo establecido en diciembre de 1988 por Defense Advanced Research Projects Agency (DARPA) para manejar los problemas concernientes a la Seguridad Informática. El CERT es dirigido por expertos en diagnostico y resolución de problemas de

seguridad. Para la resolución de estos problemas están en permanente contacto con usuarios de todo el mundo y las autoridades gubernamentales apropiadas. Por más información *http://www.cert.org – http://wwww.acert.gov.ar*

Ciberespacio: "(...) alucinación consensual experimentada diariamente por millones de legítimos operadores en todas las naciones... una representación gráfica de información proveniente de todas las computadoras del sistema humano. Una complejidad inimaginable (...)". GIBSON, William. Neuromante.

Cifrar: Ver **Criptografía**

Clave, Contraseña (Password): Palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc.

Cliente: Sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una computadora que solicita el contenido de un archivo a otra (**Servidor**) es un cliente de la misma.

Código Fuente: Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" (**Compilar**) a código máquina para ser interpretad por esta última.

Compilador: Programa que toma el **Código Fuente** de un programa y lo convierte a un ejecutable.

Cookie: Es un pequeño trozo de información enviado por un servidor de Web al sistema de un usuario.

Correo Electrónico: Aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado **E-mail.**

Cracker: Persona que quita la protección a programas con sistemas anticopia. Hacker maligno que se dedica a destruir información.

Criptografía: Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de **claves**, que solo el emisor y receptor conocen.

Datagrama: Conjunto de datos que se envían como mensajes independientes. Unidad utilizada por el protocolo **IP.**

Denial of Service (DoS): Negación de Servicio. Acciones que impiden a cualquier sistema funcionar de acuerdo con sus propósitos.

Detección de Intrusos: Sistemas que agrupan un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

Decoy (Señuelo): Programa diseñado para vigilar el comportamiento de un usuario.

Diccionarios: Conjunto de palabras almacenadas en un archivo. Su fin es utilizar cada palabra para ser probada como posible **Password** de un sistema que se quiere violar. Véase también **Fuerza Bruta.**

DNS (Domain Name Server): Servicio que proporciona una dirección IP a partir de un nombre de dominio proporcionado. Este protocolo evita tener que recordar las complicadas combinaciones de números que forman una dirección IP.

E

E-mail: Ver **Correo Electrónico.**

Encriptar: Ver **Criptografía.**

Ethernet: Protocolo de comunicación. Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel, y Digital Equipment Corporation.

F

Firewall: Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información.

FTP (File Transfer Protocol): Protocolo del nivel de usuario (protocolos de aplicación) para la transferencia de archivos entre computadoras. También pueden hacer referencia a la aplicación que permite transferir archivos de una computadora a otra usando el mismo protocolo.

Fuerza Bruta: Se basan en aprovechar **Diccionarios** para comparar las palabras almacenadas en él con las **Passwords** del sistema y obtenerlos.

G

Gusano: Programa ilegitimo que es capaz de reproducirse a sí mismo infinitas veces hasta colapsar el sistema, ene l que se esta ejecutando por falta de recursos.

H

Hacker: Una persona que disfruta explorando los detalles de la computadoras y de cómo extender sus capacidades.

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

Host: Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el **Correo Electrónico, Telnet** y **FTP.**

ICMP (Internet Control Message Protocol): Protocolo utilizado para gestionar la comunicación de mensajes de error entre distintos puntos de la red.

ID: Identificación.

Internet: Sistema de redes de computación ligadas entre sí, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

Intruso: Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

IP (Internet Protocol): Protocolo de comunicación sin conexión, que por si mismo proporciona un servicio de datagramas. Es el Protocolo que proporciona el servicio de envío de paquetes para los protocolos soportados **TCP, UDP** e **ICMP.** Protocolo de capa de red de la pila **TCP/IP** que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad.

IP Spoofing: Método para falsear la IP en una conexión remota.

ISP (Internet Service Provider): Compañía o individuo dedicado a vender acceso (servicio) a Internet.

J

Java: Lenguaje de programación desarrollado por **SUN** para la elaboración de pequeñas aplicaciones exportables a la red (**Applets**) y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

L

Lamer: Termino aplicado por los **Hackers** a las personas con pocos conocimientos.

Login: Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

Log: Archivo de registro de actividades.

M

Mail Bomber: Consiste en el envío masivo de mails a una dirección de la victima.

MultiCast (MultiDifusión): Modo de difusión de información, que permite que esta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios. Véase también **BroadCast**.

N

Negación de Servicio: Ver **DoS.**

Newbie: Termino aplicado por los **Hackers** a los novatos en el hacking.

Network (Red): Red de computadoras es un sistema de comunicación de datos. Conecta entre si sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

P

Password (Clave): Ver **Clave, Contraseña.**

Patch (Parche): Modificación de un programa ejecutable para solucionar un problema, corregir un **Bug** o para cambiar su comportamiento.

PC (Personal Computer): Computadora Personal

Phreaker: Persona que usa los medios de comunicaciones sin pagarlos o pagando menos de lo que corresponde.

Pirata Informático: Persona que copia software, con derecho de autor, ilegalmente sin que medie el permiso expreso del desarrollador. No confundir con el término **Hacker** o **Cracker.**

PIN (Personal Identification Number): Número de Identificación Personal.

Promiscuo (Modo): Normalmente interfaz. **Ethernet** que permite leer toda la información sin importar su destino, aplicable a un segmente de **Red.**

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Puerto: Proceso de capa superior que esta recibiendo información de capas más bajas.

Red: Conjunto de computadoras, impresoras, **Routers, Switches**, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

RFC (Request For Comment): Documentos especiales escritos y publicados por individuos comprometidos en el desarrollo y mantenimiento de Internet. Tienen el importante propósito de servir de documentación para nuevos desarrollos tecnológicos y ofrecer los estándares sobre los cuales se identificara la nueva tecnología.

Root: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo.

Rootkit: Software que permite a los intrusos depositar **Puertas Traseras, Caballos de Troya** y diversos mecanismos para asegurar su regreso al sistema atacado, y al mismo tiempo esconderse del resto de los usuarios del sistema, en particular del Administrador.

Router: Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviara el tráfico de la red. Los routers envían paquetes de una red a otra base de información de capa de red. Ocasionalmente llamado Gateway (aunque esta definición d gateway esta cayendo en desuso).

S

SATAN (Security Administrador Tool For Analyzing Networks): Herramienta para el Análisis de Administradores de Seguridad de Redes. Aplicación realizada por el informático norteamericano Dan Farmer y el gurú americano-holandés Wietse Venema. Es capaz de establecer el nivel de vulnerabilidad de un **Host** y de todas las máquinas conectadas a él vía Internet (su dominio).

Server (Servidor): Máquina que ofrece servicios a otras dentro de una red. También llamado **Host.**

Shoulder Surfing: Espiar por detrás de un hombro para tratar de ver información interesante. Es un método comúnmente usado para acceder a cuentas de otras personas.

Sniffer: Es un programa que permite "escuchar furtivamente" en redes de medios de comunicación compartidos (tales como **Ethernet**). Se ejecuta en una máquina que esta conectada a la red, en modo **Promiscuo** y captura el tráfico de todo el segmento de red.

Software: Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de máquina.

Spam: Correo electrónico que se recibe sin haberlo solicitado (llamados "e-mail basura"). Un envío masivo de Spam puede provocar un colapso en el sistema que los recibe, en este caso se les denomina MailBombing.

SysOp: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo.

T

TCP (Transmisión Control Protocol): Este Protocolo de Control de Transmisión es un protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de estos.

TCP/IP (Transfer Control Protocol/Internet Protocol): Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundido en la actualidad, por ser la base de **Internet.**

TELNET: Protocolo estándar utilizado para realizar un servicio de conexión desde una terminal remota.

Terminal: Acceso a una computadora o sistema. Puede tratarse de monitor y teclado o de una computadora completa.

Trasching: Arte de revolver la basura para encontrar información útil.

Troyano: Programa legitimo que ha sido alterado de alguna forma y que contiene funciones desconocidas (y generalmente dañinas). Generalmente no contienen código reproductor. Véase también **Caballo de Troya.**

UseNet: Red que contiene cientos de foros electrónicos de discusión (**Newgroups**), las computadoras que procesan los protocolos, y finalmente, las personas que leen y envían las noticias.

Username (Usuario): Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

Virus: Programa de actuar subrepticio para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan reproducirse y ser susceptibles de mutar; resultando de dicho proceso

ANEXO

TABLAS

- **Tabla 2.1 – Porcentaje de Vulnerabilidades por tipo de sitio. Fuente**: *http://www.trouble.org/survey*
- **Tabla 2.2. Detalle de Ataques. Fuente:** HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org*. Capítulo 6–Página 71

GRÁFICOS

- **Gráfico 1.1 – Amenazas para la Seguridad**
- **Gráfico 1.2 – Tipos de Intrusos. Fuente:** CybSec S.A. *http://www.cybsec.com*
- **Gráfico 1.3 – Tipos de Ataques Activos. Fuente:** HOWARD, John D. Thesis: An Analysis of security on the Internet 1989–1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org*. Capítulo 6–Página 59.
- **Grafico 2.1 - Intrusiones Fuente:** *http://www.cybsec.com*
- **Gráfico 2.2 – Porcentaje de Ataques. Fuente:** *http://www.disa.mil*
- **Gráfico 2.3 – Ataque Smurf**
- **Gráfico 2.4 – Modelo de un Antivirus**

GLOSARIO

A

ActiveX: Lenguaje desarrollado por Microsoft para la elaboración de aplicaciones exportables a la red y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo. Véase también Root y SysOp.

Antivirus: Programa que es encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

Applet: Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente.

Archivo: Conjunto bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

Ataque: Intento de traspasar un control de seguridad de un sistema.

B

Backdoor: Puerta trasera de entrada a una computadora, programa o sistema en general. Es utilizado para acceder sin usar un procedimiento normal.

Bit: En informática, unidad mínima de información.

BroadCast: Difusión. Tipo de comunicación en que todo posible receptor es alcanzado por una sola transmisión. Véase también **Multicast.**

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo.

Byte: Combinación de **Bits**. En la representación más común 8 bits forman un byte.

C

Caballo de Troya: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño. Véase también **Troyano.**

CERT/CC (Computer Emergency Response Team/Coordination Center): Grupo establecido en diciembre de 1988 por Defense Advanced Research Projects Agency (DARPA) para manejar los problemas concernientes a la Seguridad Informática. El CERT es dirigido por expertos en diagnostico y resolución de problemas de

seguridad. Para la resolución de estos problemas están en permanente contacto con usuarios de todo el mundo y las autoridades gubernamentales apropiadas. Por más información *http://www.cert.org – http://wwww.acert.gov.ar*

Ciberespacio: "(...) alucinación consensual experimentada diariamente por millones de legítimos operadores en todas las naciones... una representación gráfica de información proveniente de todas las computadoras del sistema humano. Una complejidad inimaginable (...)". GIBSON, William. Neuromante.

Cifrar: Ver **Criptografía**

Clave, Contraseña (Password): Palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc.

Cliente: Sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una computadora que solicita el contenido de un archivo a otra (**Servidor**) es un cliente de la misma.

Código Fuente: Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" **(Compilar)** a código máquina para ser interpretad por esta última.

Compilador: Programa que toma el **Código Fuente** de un programa y lo convierte a un ejecutable.

Cookie: Es un pequeño trozo de información enviado por un servidor de Web al sistema de un usuario.

Correo Electrónico: Aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado **E-mail.**

Cracker: Persona que quita la protección a programas con sistemas anticopia. Hacker maligno que se dedica a destruir información.

Criptografía: Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de **claves**, que solo el emisor y receptor conocen.

Datagrama: Conjunto de datos que se envían como mensajes independientes. Unidad utilizada por el protocolo **IP.**

Denial of Service (DoS): Negación de Servicio. Acciones que impiden a cualquier sistema funcionar de acuerdo con sus propósitos.

Detección de Intrusos: Sistemas que agrupan un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

Decoy (Señuelo): Programa diseñado para vigilar el comportamiento de un usuario.

Diccionarios: Conjunto de palabras almacenadas en un archivo. Su fin es utilizar cada palabra para ser probada como posible **Password** de un sistema que se quiere violar. Véase también **Fuerza Bruta.**

DNS (Domain Name Server): Servicio que proporciona una dirección IP a partir de un nombre de dominio proporcionado. Este protocolo evita tener que recordar las complicadas combinaciones de números que forman una dirección IP.

E

E-mail: Ver **Correo Electrónico.**

Encriptar: Ver **Criptografía.**

Ethernet: Protocolo de comunicación. Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel, y Digital Equipment Corporation.

F

Firewall: Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información.

FTP (File Transfer Protocol): Protocolo del nivel de usuario (protocolos de aplicación) para la transferencia de archivos entre computadoras. También pueden hacer referencia a la aplicación que permite transferir archivos de una computadora a otra usando el mismo protocolo.

Fuerza Bruta: Se basan en aprovechar **Diccionarios** para comparar las palabras almacenadas en él con las **Passwords** del sistema y obtenerlos.

Gusano: Programa ilegítimo que es capaz de reproducirse a sí mismo infinitas veces hasta colapsar el sistema, ene l que se esta ejecutando por falta de recursos.

Hacker: Una persona que disfruta explorando los detalles de la computadoras y de cómo extender sus capacidades.

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

Host: Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el **Correo Electrónico, Telnet** y **FTP.**

ICMP (Internet Control Message Protocol): Protocolo utilizado para gestionar la comunicación de mensajes de error entre distintos puntos de la red.

ID: Identificación.

Internet: Sistema de redes de computación ligadas entre sí, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

Intruso: Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

IP (Internet Protocol): Protocolo de comunicación sin conexión, que por si mismo proporciona un servicio de datagramas. Es el Protocolo que proporciona el servicio de envío de paquetes para los protocolos soportados **TCP, UDP** e **ICMP.** Protocolo de capa de red de la pila **TCP/IP** que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad.

IP Spoofing: Método para falsear la IP en una conexión remota.

ISP (Internet Service Provider): Compañía o individuo dedicado a vender acceso (servicio) a Internet.

J

Java: Lenguaje de programación desarrollado por **SUN** para la elaboración de pequeñas aplicaciones exportables a la red (**Applets**) y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

L

Lamer: Termino aplicado por los **Hackers** a las personas con pocos conocimientos.

Login: Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

Log: Archivo de registro de actividades.

M

Mail Bomber: Consiste en el envío masivo de mails a una dirección de la víctima.

MultiCast (MultiDifusión): Modo de difusión de información, que permite que esta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios. Véase también **BroadCast**.

N

Negación de Servicio: Ver **DoS.**

Newbie: Termino aplicado por los **Hackers** a los novatos en el hacking.

Network (Red): Red de computadoras es un sistema de comunicación de datos. Conecta entre si sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

P

Password (Clave): Ver **Clave, Contraseña.**

Patch (Parche): Modificación de un programa ejecutable para solucionar un problema, corregir un **Bug** o para cambiar su comportamiento.

PC (Personal Computer): Computadora Personal

Phreaker: Persona que usa los medios de comunicaciones sin pagarlos o pagando menos de lo que corresponde.

Pirata Informático: Persona que copia software, con derecho de autor, ilegalmente sin que medie el permiso expreso del desarrollador. No confundir con el término **Hacker** o **Cracker.**

PIN (Personal Identification Number): Número de Identificación Personal.

Promiscuo (Modo): Normalmente interfaz. **Ethernet** que permite leer toda la información sin importar su destino, aplicable a un segmente de **Red.**

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Puerto: Proceso de capa superior que esta recibiendo información de capas más bajas.

Red: Conjunto de computadoras, impresoras, **Routers, Switches**, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

RFC (Request For Comment): Documentos especiales escritos y publicados por individuos comprometidos en el desarrollo y mantenimiento de Internet. Tienen el importante propósito de servir de documentación para nuevos desarrollos tecnológicos y ofrecer los estándares sobre los cuales se identificara la nueva tecnología.

Root: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo.

Rootkit: Software que permite a los intrusos depositar **Puertas Traseras, Caballos de Troya** y diversos mecanismos para asegurar su regreso al sistema atacado, y al mismo tiempo esconderse del resto de los usuarios del sistema, en particular del Administrador.

Router: Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviara el tráfico de la red. Los routers envían paquetes de una red a otra base de información de capa de red. Ocasionalmente llamado Gateway (aunque esta definición d gateway esta cayendo en desuso).

S

SATAN (Security Administrador Tool For Analyzing Networks): Herramienta para el Análisis de Administradores de Seguridad de Redes. Aplicación realizada por el informático norteamericano Dan Farmer y el gurú americano-holandés Wietse Venema. Es capaz de establecer el nivel de vulnerabilidad de un **Host** y de todas las máquinas conectadas a él vía Internet (su dominio).

Server (Servidor): Máquina que ofrece servicios a otras dentro de una red. También llamado **Host.**

Shoulder Surfing: Espiar por detrás de un hombro para tratar de ver información interesante. Es un método comúnmente usado para acceder a cuentas de otras personas.

Sniffer: Es un programa que permite "escuchar furtivamente" en redes de medios de comunicación compartidos (tales como **Ethernet**). Se ejecuta en una máquina que esta conectada a la red, en modo **Promiscuo** y captura el tráfico de todo el segmento de red.

Software: Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de máquina.

Spam: Correo electrónico que se recibe sin haberlo solicitado (llamados "e-mail basura"). Un envío masivo de Spam puede provocar un colapso en el sistema que los recibe, en este caso se les denomina MailBombing.

SysOp: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo.

T

TCP (Transmisión Control Protocol): Este Protocolo de Control de Transmisión es un protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de estos.

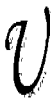
TCP/IP (Transfer Control Protocol/Internet Protocol): Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundido en la actualidad, por ser la base de **Internet.**

TELNET: Protocolo estándar utilizado para realizar un servicio de conexión desde una terminal remota.

Terminal: Acceso a una computadora o sistema. Puede tratarse de monitor y teclado o de una computadora completa.

Trasching: Arte de revolver la basura para encontrar información útil.

Troyano: Programa legitimo que ha sido alterado de alguna forma y que contiene funciones desconocidas (y generalmente dañinas). Generalmente no contienen código reproductor. Véase también **Caballo de Troya.**



UseNet: Red que contiene cientos de foros electrónicos de discusión (**Newgroups**), las computadoras que procesan los protocolos, y finalmente, las personas que leen y envían las noticias.

Username (Usuario): Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

Virus: Programa de actuar subrepticio para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan reproducirse y ser susceptibles de mutar; resultando de dicho proceso

la modificación, alteración y/o daño de los programas, información y/o hardware afectados.

Vulnerabilidad: Hardware, firmware, o **Software** que contiene **Bugs** que permiten su explotación potencial.

Web Sites (Sitio Web): Sistema dedicado al intercambio de información **On-Line.**

Windows: Sistema Operativo de la empresa Microsoft.

WWW (Word Wide Web): Gran red de servidores de Internet que brinda servicios de hipertexto y otros a las terminales que corren aplicaciones cliente como por ejemplo un explorador WWW.

BIBLIOGRAFÍA

Libro: Redes
Autores: Jesús Sánchez Allende / Joaquín López Lérida
Editorial: McGraw Hill

Libro: Tecnologías Emergentes para Redes de Computadoras
Autores: Uyless Black
Editorial: Pretince Hall 2da. Edición

Libro: Informática Presente y Futuro
Autores: Donald H. Sanders
Editorial: McGraw Hill 3ra. Edición

Libro: Computación & Informática Hoy
Autores: George Beekman
Editorial: Pearson

Libro: Seguridad en Centros de Cómputo
Autores: Leonard H. Finc
Editorial: Trillas

Libro: Comportamiento Humano en el Trabajo
Autores: David Keith / Newstrom Johnn W.
Editorial: McGraw Hill 2da. Edición

Libro: Dirección de Relaciones Laborales
Autores: Muller de la Lama Enrique
Editorial: Trillas Edición 2003

Libro: Las Organizaciones: Comportamiento, Estructura y Procesos
Autores: Gibson James L. / Ivancevich John M. / Dannelly James H.
Editorial: McGraw Hill Edición 2003

Libro: Redes de Área Local
Autores: Thomas W. Madron
Editorial: Grupo Noriega Edición 1992

Libro: Sistemas Operativos Modernos
Autores: Andrew S. Tanenbaum
Editorial: Pearson Educación Addison Wesley, Edición 1993

www.microsoft.com
http://es.mcafee.com/
www.gfi.com
www.cryptoforge.com.ar/
www.mysql.com
www.superscan.softonic.com/
www.symantec.com/es/mx/index.jsp
http://docs.hp.com/es/B2355-90957/ch08s06.html
http://www.nist.gov
http://www.kriptopolis.com
www.delitosinformáticos.com/tesis.htm
http://www.cybsec.com
http://www.cert.org.
http://www.disa.mil
http://www.trouble.org/survey

ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997.

HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000.

CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio 2001.

SCHNEIER, Bruce. Secrets & Lies.

HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU.

HUERTA, Antonio Villalón. "Seguridad en Unix y redes". Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000.