ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGIA

LICENCIATURA EN SISTEMAS
CON ENFASIS EN REDES Y SISTEMAS TELEMÀTICOS

“MODELO DE SEGURIDAD PARA REDES DE EMPRESAS FINANCIERAS CON SU PROPIA PÁGINA WEB TRANSACCIONAL”

Nota de aprobación: 91

Tutor: Jorge Mejía Suárez

Sustentante: Álvaro Jiménez Castro
Cédula 1-0870-0531
Teléfono 388-6438
Correo electrónico ajimenezca@bncr.fi.cr

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE
LICENCIATURA EN SISTEMAS
CON ENFASIS EN REDES Y SISTEMAS TELEMÀTICOS

San José – Costa Rica
MAYO 2005

Dedicatoria

Esta tesis se la dedico en este orden a Dios, mi familia y a todos los que en estos momentos también están por terminar su proyecto de graduación y en su momento creyeron que por algún motivo no podrían llegar a cumplir con esta meta propuesta. A Dios en especial le agradezco con todo el corazón por haberme permitido terminar este trabajo a pesar de los muchos problemas de salud que sufrí a lo largo de tres años y sobretodo el inconveniente en la sala de operaciones el día 30 de junio del 2004, donde estuve a punto de no volver a ver a mis seres queridos en especial a mi esposa y mi hija.

Agradecimientos

Quiero agradecer a todas las personas que me ayudaron a terminar esta tesis; en especial, a las personas a quienes hasta ese momento no conocía y que sacaron un momento de su tiempo para contestar el cuestionario. También agradezco a las personas que, dada su experiencia, me ayudaron con sus observaciones y correcciones para poder realizar un buen documento que estoy seguro será de mucho provecho para las personas que el día de mañana lo requieran y deseen consultar para ayudarse en la universidad.

Agradezco además al personal docente y administrativo de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), por su excelente trato humano y profesional hacia los estudiantes.

Presentación

El presente constituye el trabajo de investigación requerido para optar por el grado de Licenciatura en Ingeniería Informática en la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT).

La investigación se realizó con la finalidad de poder brindar a empresas financieras tales como bancos, mutuales, puestos de bolsa, etc., una guía que sirva de modelo de seguridad a nivel de redes de datos locales, así como la respectiva conexión externa de los clientes, proveniente de Internet.

Introducción

En la actualidad, se debe tener muy en cuenta que, si bien es cierto las redes de computadoras brindan una gran cantidad de ventajas, a la hora de compartir recursos y ahorro de costos, por sí solas no implementan una adecuada seguridad de la información de una empresa.
No se puede ignorar que vivimos en una sociedad en donde cada vez hay más hackers y crackers, y sus ataques son cada vez más frecuentes.

Desde los comienzos de la computación, los sistemas han estado expuestos a una serie de peligros o riesgos que han aumentado conforme se globalizan más las comunicaciones entre los sistemas.

Inicialmente, la seguridad fue enfocada al control de acceso físico, ya que para acceder a un computador, se requería la presencia física del usuario frente al sistema. Posteriormente empiezan a proliferar los sistemas multiusuario en los cuales un recurso computacional era compartido por varios usuarios. Surgen nuevos riesgos como la utilización del sistema por personas no autorizadas, manipulación de información o aplicaciones por suplantación de usuarios y surge un primer esquema de protección en códigos de usuarios y contraseñas (passwords) para restringir el acceso al sistema.

Siguen evolucionando los sistemas y se inicia la computación en red, en la cual además de los riesgos asociados a los sistemas multiusuarios, aparece un nuevo tipo de vulnerabilidad, básicamente en el proceso de transmisión de la información; aunque las primeras redes estaban aisladas del mundo exterior a la empresa, estaban expuestos a los posibles ataques internos. La evolución de la tecnología continúa y comienza el proceso de interconexión de las distintas redes aisladas de una empresa para configurar corporativas, donde aumentan considerablemente los riesgos, ya que es más difícil controlar la totalidad de la red.

El objetivo de realizar este trabajo es brindar un esquema de seguridad para empresas financieras, a nivel de comunicación entre redes e Internet y que consiste en prevenir,

impedir, detectar y corregir vulnerabilidades en la seguridad durante la transmisión de información.

CAPÍTULO 1 PROBLEMAS Y PROPÓSITOS

1.1 Justificación

Debido a la funcionalidad que tienen las redes de computadoras, de permitir la mayor conectividad entre equipos para acceder información, se podría presentar un problema por cuanto existe la posibilidad de que se accese información clasificada, sensible a ser observada, por personas ajenas y dentro de cualquier empresa de carácter financiero, y que se haga mal uso de esta información, o, en su defecto sea destruida.

El propósito de este trabajo consiste en hacer una recopilación de los aspectos de seguridad de redes que son más sensibles a ser vulnerados en una empresa financiera, evaluar las herramientas de hardware y software más adecuadas y hacer el análisis de la implementación de mecanismos de seguridad para redes LAN, WAN e Internet, con la intención de que los resultados obtenidos sean de gran utilidad para las personas encargadas de evaluar o diseñar estrategias de seguridad para la interconexión entre redes de computadoras.

1.2 Objetivos

1.2.1 Objetivo general de diagnóstico:

- Identificar un modelo de seguridad adecuado tanto de hardware como software que ayude a prevenir y corregir vulnerabilidades

1.2.2 Objetivos específicos de diagnóstico:

- Identificar las principales vulnerabilidades que afectan a las redes LAN y WAN
- Identificar las principales vulnerabilidades que pueden afectar a una empresa financiera con su propia página Web
- Identificar las principales técnicas de ataque por Internet
- Identificar software y hardware especializados en materia de seguridad para redes

1.2.3 Objetivo general de la propuesta:

- Establecer un modelo básico de seguridad para redes LAN, WAN e Internet para empresas financieras que desean tener página Web

1.2.4 Objetivos específicos de la propuesta:

- Generar políticas de seguridad que sean fundamentales para que una empresa financiera cuente con un adecuado plan de seguridad para sus datos
- Implementar una estrategia que contenga las posibles correcciones que se deben efectuar para prevenir las vulnerabilidades detectadas

1.3 Alcances

Esta propuesta servirá de base para el desarrollo de un modelo de seguridad a nivel de redes de Área Local, redes de Área Ancha y accesos a Páginas Web.
El trabajo se enfocará a empresas financieras que tienen su propia página Web, en la cuál los clientes podrán realizar transacciones de acuerdo a los diferentes servicios que la institución ofrezca a sus clientes.

1.4 Limitaciones

Se ha tratado de contactar a los oficiales encargados de seguridad informática de varias instituciones financieras del país, pero ha sido muy difícil que puedan brindar tiempo e información para este trabajo.
Además este será un trabajo de graduación universitario, y lo que se indica será una guía de seguridad basada en un trabajo de investigación, y no precisamente serán las políticas de seguridad internas que vayan a tener cada empresa financiera del país.

CAPÍTULO 2 MARCO TEÓRICO

2.1 Seguridad

Podemos definir seguridad como una característica de cualquier sistema que indique si ese sistema está fuera de peligro, daño o riesgo. Como ningún sistema, sea informático o no, es infalible, los sistemas deben de tener un grado considerable de fiabilidad, que represente la probabilidad de que un sistema se comporte tal y como se espera de él; por tanto se puede hablar de sistemas fiables más que de sistemas seguros.

Según Charles P. Fleeger (1997) se puede entender que mantener un sistema seguro o fiable consiste en garantizar básicamente tres aspectos: confidencialidad, integridad y disponibilidad.

La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por individuos autorizados, y que estos elementos no van a convertir esta información para hacerla disponible a otras entidades.

La integridad consiste en que los objetos solamente pueden ser creados, modificados o borrados por personas autorizadas y de una manera controlada.

La disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a las personas autorizadas y en el momento establecido. Generalmente tienen que existir los tres aspectos descritos anteriormente para que se considere que en un sistema haya seguridad.

2.2 Protección de la información

Los tres elementos principales a proteger en cualquier sistema informático son el hardware, el software y los datos. El hardware es el conjunto formado por todos los elementos físicos de un sistema informático. El software es el conjunto de programas lógicos que hacen funcional al hardware, tanto sistema operativos como aplicaciones.

Los datos son el conjunto de información lógica que manejan el hardware y el software. Generalmente los datos consisten el principal elemento de los tres a proteger, ya que es el más amenazado y algunas veces el más difícil de recuperar.
Tanto el hardware, software y los datos, podrían sufrir ataques en su contra, o sea, están expuestos a diferentes amenazas. Generalmente, estas amenazas se pueden dividir en cuatro grupos: interrupción, interceptación, modificación y fabricación.

Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.

Una interceptación se hace si un elemento no autorizado consigue acceso a un determinado objeto del sistema.

Una modificación se da cuando además de tener el acceso, se modifica el objeto. La destrucción es una modificación que deja al elemento inutilizable.

Un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al que se atacó, de forma que sea difícil distinguir entre el objeto real y el fabricado.

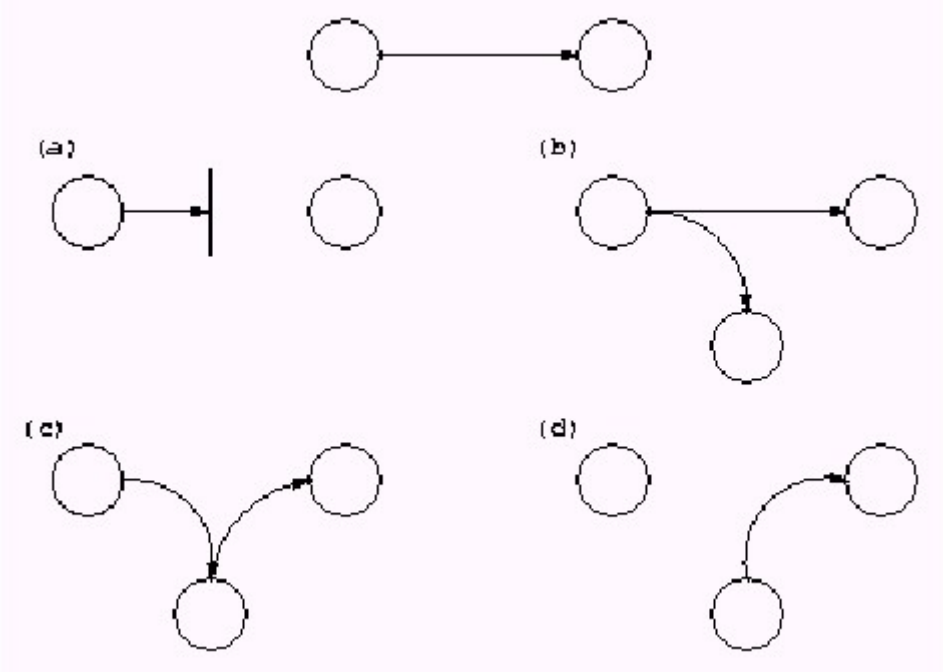


Figura 1
Flujo normal de información entre emisor y receptor y posibles amenazas:
(a) interrupción, (b) interceptación, (c) modificación y (d) fabricación

2.3 Elementos que pueden atentar contra la seguridad

En la gran mayoría de las publicaciones relativas a la seguridad informática en general, se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. A continuación se presenta una relación de tales elementos.

2.3.1 Personas

La mayoría de ataques a nuestros sistemas, van a provenir de personas que intencionadamente o no, pueden causar enormes daños y pérdidas. Generalmente se trata de piratas informáticos que intentan conseguir el máximo nivel de privilegio posible, aprovechando alguno o algunos de los riesgos lógicos, especialmente agujeros del software.

Las personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas, generalmente se dividen en dos grupos: los atacantes pasivos, que son los que husmean por el sistema pero no lo modifican o destruyen, y los atacantes activos, que son los que dañan el objeto atacado, o lo modifican en su favor.

Generalmente los curiosos y los hackers realizan ataques pasivos (que se pueden convertir en activos) mientras que los crackers y ex empleados realizan ataques activos puros, los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y atacantes activos en el caso contrario.

Las personas que pueden causar daños a nuestros sistemas se pueden clasificar en los siguientes grupos

2.3.1.1 Personal

Las amenazas a la seguridad de un sistema provenientes de la propia institución son muy pocas veces tomados en cuenta, ya que se supone que es un ambiente de confianza; por ello generalmente se pasa por alto el hecho de que casi cualquier persona de la institución, incluso el personal que no es del área de informática (secretarias, personal de seguridad, limpieza y mantenimiento), pueden comprometer la seguridad de los equipos.
Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son muy dañinos, debemos recordar que nadie conoce mejor los sistemas y sus debilidades que el propio personal de la empresa), lo normal es que más que de ataques, se trate de accidentes causados por un error o por desconocimiento o inexistencia de las normas básicas de seguridad.

2.3.1.2 Ex empleados

Otro grupo de personas potencialmente interesadas en atacar nuestros sistemas son los antiguos empleados de la institución, especialmente los que no la abandonaron por voluntad propia o los que pasaron a empresas de la competencia. Generalmente son personas descontentas con la empresa, que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por un hecho que no considera justo.

2.3.1.3 Hackers

Junto con los crackers, los hackers son los ataques más habituales a un sistema. Aunque en la mayoría de las situaciones se trata de ataques no destructivos, parece claro que no benefician en absoluto el entorno de fiabilidad que se pueda generar en un determinado sistema.

2.3.1.4 Crackers

Los entornos que tienen un nivel de seguridad que no es muy alto, son un objetivo típico de los intrusos, ya sea para husmear, para utilizarlos como enlace hacia otras redes o simplemente por diversión. Son por lo general redes abiertas y la seguridad no es un factor que se tiene muy en cuenta. De esta manera el atacante sólo tiene que utilizar un escáner de seguridad contra el dominio completo y luego atacar los equipos que presentan vulnerabilidades.

2.3.1.5 Intrusos remunerados

Este grupo de atacantes a los sistemas es muy peligroso, aunque es menos habitual en redes de empresas pequeñas y medianas en infraestructura y organización. Suelen afectar por lo general a las grandes empresas y organismos gubernamentales. Se trata de piratas con gran experiencia en problemas de seguridad y amplio conocimiento de sistemas, que son pagados por terceros generalmente para robar secretos o simplemente para dañar la imagen de la institución afectada.

2.3.2 Amenazas

Cualquier acción que comprometa la seguridad de la información que se encuentra en una red se considera una amenaza. Las amenazas se pueden clasificar en cuatro categorías: naturales, accidentales, activas deliberadas y pasivas deliberadas. Las naturales no están dirigidas a los elementos de la red ni sistemas de información, e incluyen principalmente cambios naturales que pueden afectar de una manera u otra el normal desempeño de la red; las accidentales se dividen en errores de: usuario,

administración, sistema, salida, datos mal preparados, entre otras; finalmente, las deliberadas son amenazas intencionales generalmente perpetuadas por hackers.

2.3.3 Amenazas Lógicas

Como amenazas lógicas se encuentran todo tipo de programa que de una u otra forma pueden dañar a nuestro sistema, creados de forma intencionada para ese fin, o simplemente por error.

Según Donn P. Baker (1981), las amenazas lógicas se pueden dividir en las siguientes clasificaciones:

2.3.3.1 Software incorrecto

Los errores más habituales en un sistema provienen de errores cometidos en forma involuntaria por los programadores de sistemas o aplicaciones. A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema se les llama *exploits*.
Estos programas representan la amenaza más común contra los sistemas, ya que un exploit es fácil de conseguir y utilizar contra una red, sin siquiera saber como funciona, incluso hay exploits que dañan seriamente la integridad de un sistema y están preparados para utilizarse desde MS-DOS, con lo que cualquier pirata novato, puede utilizarlos contra un servidor.

2.3.3.2 Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo, ya que de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o su red, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

2.3.3.3 Puertas traseras

Durante el desarrollo de aplicaciones grandes o sistemas operativos es habitual entre los programadores, insertar “atajos” en los sistemas actuales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ello se consigue mayor velocidad a la hora de detectar y depurar fallos.
Lo peligroso es que si un atacante descubre estas puertas traseras, va a tener un acceso global a datos que no debería poder leer, lo que representa un grave peligro para nuestro sistema.

2.3.3.4 Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas. La función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos archivos, la ejecución bajo un determinado comando o la llegada de una fecha concreta.

2.3.3.5 Canales cubiertos

Según la definición de Sheila Brand (Departament of Defense Trusted Computer System Evaluation Criteria) son canales de comunicación que permiten a un proceso transferir información de una forma que viole la política de seguridad del sistema, en otras palabras un proceso transmite información a otros que no están autorizados a leer dicha información.

2.3.3.6 Virus

Un virus es una secuencia de código que se inserta en un archivo ejecutable, de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

2.3.3.7 Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grave. Un gusano puede automatizar y ejecutar en unos segundos, todos los pasos que seguiría un atacante humano para acceder a nuestro sistema; mientras que una persona por muchos conocimientos y medios que posea, tardará como mínimo algunas horas en controlar nuestra red completa, un gusano puede hacer eso mismo en unos pocos minutos, de ahí su peligro.

2.3.3.8 Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las funciones que un usuario espera de él, pero que realmente ejecuta funciones ocultas sin el consentimiento del usuario.

2.3.3.9 Programas conejo o baterías

Son los programas que no hace nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema produciendo una negación del servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica el gran número de copias suyas en el sistema, que pueden llegar a provocar que un servidor se detenga.

2.3.3.10 Técnicas salami

Es el robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que una cantidad inicial sea extremadamente grande y la robada sea pequeña, hacen muy difícil su detección. Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios.

2.3.4 Catástrofes

Las catástrofes naturales o artificiales son la amenaza menos probable, simplemente por ubicación geográfica; nadie escapa a la probabilidad de sufrir un terremoto o una inundación que afecte los sistemas en producción.
El hecho de que las catástrofes son amenazas poco probables, no implica que no se tomen medidas básicas, ya que si se produjeran, se generarían graves daños.

2.3.5 Métodos de protección

Para proteger nuestros sistemas se debe hacer un análisis de las amenazas potenciales que pueden sufrir, las pérdidas que podrían generar y la probabilidad de que ocurra. A partir de este análisis se deben implementar las políticas de seguridad de tal manera que se definan responsabilidades y reglas por seguir para evitar las amenazas o minimizar el impacto en caso que se produzcan.
A los mecanismos utilizados para implementar estas políticas de seguridad se les denomina mecanismos de seguridad. Son la parte más importante de nuestro sistema de seguridad, y se convierten en una herramienta básica para garantizar la protección de nuestros sistemas y nuestra red.

Los mecanismos de seguridad se dividen en tres grupos:
Prevención: son aquellos que aumentan la seguridad de un sistema durante su funcionamiento, previniendo que ocurran violaciones a la seguridad; un ejemplo es el uso de cifrado en la transmisión de datos, ya que evita que un posible atacante escuche las conexiones hacia y desde un sistema en una red.

Detección: son aquellos que se utilizan para detectar violaciones de seguridad o intentos de violación, un ejemplo pueden ser programas que tengan la funcionalidad de hacer auditorías.

Recuperación: son aquellos que se aplican cuando una violación a la seguridad del sistema se ha dado. Se aplican con el objetivo de regresar al sistema a su funcionamiento

correcto. Dentro de este último grupo se encuentra un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es solamente retornar al sistema a su funcionamiento normal, sino averiguar el alcance del ataque, las actividades de un intruso dentro del sistema y la "puerta" utilizada para entrar, de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas en la red.

Según Tomas Olovsson (1992) los mecanismos de prevención más habituales en redes son:

- **Mecanismos de autenticación e identificación**

  Estos mecanismos hacen posible identificar entidades del sistema en una forma única, y luego de ser identificadas se autentican. Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que accesan a un objeto.

- **Mecanismos de control de acceso**

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

- **Mecanismos de separación**

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

- **Mecanismos de seguridad en las comunicaciones**

  Es importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esa seguridad en las comunicaciones se utilizan ciertos mecanismos, la mayoría de los cuales se basa en criptografía Una de las mayores amenazas a la integridad de las redes es el tráfico sin cifrar, que hace extremadamente fácil ataques destinados a robar contraseñas o suplantar la identidad de máquinas de la red.

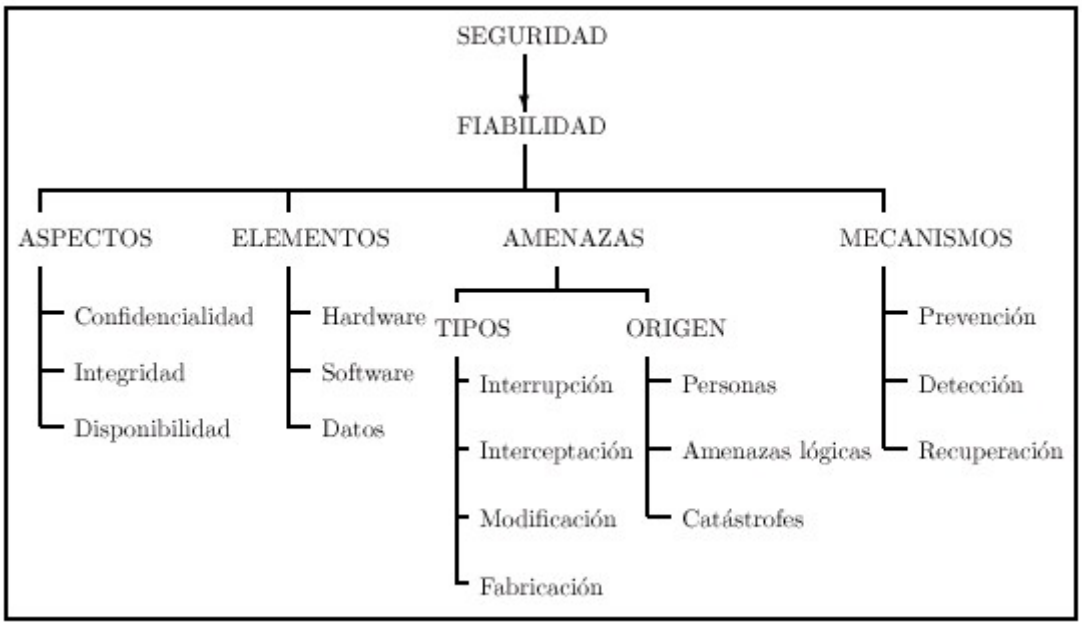


Figura 2 Visión de la seguridad informática

2.4 Ataques remotos

2.4.1 Escaneo de puertos

Una de las primeras actividades que un atacante realizará contra un objetivo será un escaneo de puertos (portscan), ya que esto le permitirá obtener información básica acerca de cuáles servicios se están ofreciendo en nuestras computadoras, y, además obtendrá detalles específicos, como por ejemplo, qué sistema operativo está instalado en cada host. Analizando cuáles puertos pueden estar abiertos en un sistema, el atacante podrá buscar agujeros en cada uno de los servicios que se están ofreciendo, ya que cada puerto abierto en una máquina es una potencial puerta de entrada a la misma.

Existen diferentes aproximaciones para clasificar los escaneos de puertos, tanto en la función de las técnicas seguidas en el ataque como su función sobre a qué sistemas o puertos debe ir dirigido. Por ejemplo se habla de un escaneo horizontal cuando el atacante busca la disponibilidad de determinado servicio en diferentes máquinas de una red.

Un escaneo vertical es cuando un atacante solamente escanea los puertos de una máquina en particular ya que solo muestra interés en ese host en concreto.

Según la técnica utilizada, los escaneos se pueden dividir en tres grupos: open, half-open y stealth.

Los escaneos **open** se basan en el establecimiento de una conexión TCP. Estos son muy sencillos de detectar y detener. El escaneador intenta establecer una conexión con un puerto específico del host atacado, y en función de la respuesta obtenida, conoce el estado de dicho puerto. Esta técnica es rápida, sencilla, fiable y no necesita de ningún privilegio especial en la máquina atacante.

En los escaneos **half-open** el atacante finaliza la conexión antes de que se complete el protocolo lo que dificulta la detección del ataque por parte de algunos detectores de intrusos muy simples.

La otra técnica de escaneo es el **stealth scanning**, en el cual se cumplen algunas de las siguientes condiciones:

- Elude cortafuegos o listas de control de acceso
- No es registrado por técnicas de detección de intrusos
- Simula tráfico normal de red para no levantar sospechas en un analizador de red

2.4.2 Spoofing

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada. La idea de este ataque es muy sencilla, desde su equipo un atacante simula ser otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basado en el nombre o en la dirección IP del host suplantado.

En el spoofing entran en juegos tres máquinas: un atacante, un atacado y un sistema suplantado que tiene cierta relación con el atacado; para que el atacante logre su objetivo, necesita por un lado establecer una comunicación falseada con su objetivo, y por otro que el equipo suplantado interfiera en el ataque.

Para evitar ataques de spoofing contra nuestros sistemas podemos tomar diferentes medidas preventivas; en primer lugar sería reforzar la secuencia de predicción de números de secuencia TCP.
Otra medida sencilla es la de eliminar las relaciones de confianza basadas en direcciones IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas. El cifrado y filtrado de conexiones que pueden aceptar nuestras máquinas también son unas medidas de seguridad importantes para evitar el spoofing.

2.4.3 Negaciones de servicio

Las negaciones de servicio (DoS, Denial of Service) son ataques dirigidos contra un recurso informático, con el objetivo de degradar total o parcialmente los servicios prestados por este recurso a sus usuarios legítimos. Constituyen uno de los ataques más sencillos y contundentes contra todo tipo de servicios. Un pirata puede interrumpir constantemente un servicio sin necesidad de grandes conocimientos o recursos, utilizando simplemente sencillos programas y un módem y una PC caseros.
Las negaciones de servicio más habituales consisten en la inhabilitación total de un determinado servicio o de un sistema completo, bien porque ha sido realmente bloqueado por el atacante o porque está tan degradado que es incapaz de ofrecer un servicio a los usuarios.
Una nueva modalidad de negación de servicio es la “negación de servicio distribuida” (DDoS Distribuited Denial of Service), en este ataque un pirata compromete en primer lugar un determinado grupo de máquinas, y en un determinado momento hace que todas ellas ataquen simultáneamente a su objetivo real enviándoles diferentes tipos de paquetes. La defensa ante una negación de servicio distribuida no es inmediata, pero se pueden tomar ciertas medidas preventivas que ayuden a limitar el alcance de uno de estos ataques. Un correcto filtrado de tráfico dirigido a nuestras máquinas es vital para garantizar nuestra seguridad, como por ejemplo:

- No responder a comandos ping externos a nuestra red
- Activar el antispoofing en el cortafuego
- Establecer correctamente límites de utilización de los recursos

- Limitar el ancho de banda dedicado a una determinada aplicación o protocolo, de forma que las utilizaciones por encima de ese margen sean negadas
- Limitar los recursos del sistema (CPU, memoria, disco) que puede consumir una determinada aplicación de tipo servidor

2.4.4 Interceptación

En las redes de difusión, cuando una máquina envía una trama a otra, indica en un campo reservado la dirección del host destino. Todas las máquinas del dominio de colisión ven esa trama, pero solo su receptora legítima la captura y elimina de la red. Este es el funcionamiento normal de TCP/IP; sin embargo es importante señalar que todas las máquinas ven esa trama. Existe un modo de funcionamiento de las tarjetas de red denominado **modo promiscuo**, en el cual la tarjeta lee todas las tramas que circulan por la red, tanto dirigidas a ella como a las otras máquinas. El leer estas tramas no implica eliminarlas de la red, por lo que el host destino legítimo las recibirá y eliminará sin notar nada extraño.

Para evitar que programas para hacer sniffing de este tipo capturen nuestra información, se recomienda sustituir los hubs de nuestra red por switches que aíslen nuestros dominios de colisión.

Implantar SSL (Secure Socket Layer) o túneles seguros es algo más costoso, pero que en la mayoría de las ocasiones es algo que vale la pena hacer.

El sniffing es el ataque de interceptación más conocido y utilizado, pero no es el único que se puede poner en práctica.

Otro ataque de interceptación menos utilizado pero igual de peligroso es el **keylogging**, el registro de teclas pulseadas por un usuario en su sesión.

2.4.5 Ataques vía web

Cualquier empresa, desde las más pequeñas hasta las más grandes organizaciones, tiene una página web en la que al menos trata de vender su imagen corporativa. En instituciones financieras, su misma página Web ofrece la oportunidad de realizar

transacciones financieras donde están involucrados sus servicios al cliente, donde está por demás indicar que la seguridad en estas instituciones debe ser de la mejor.

Cualquier analizador de vulnerabilidades que se pueda ejecutar contra nuestros sistemas (NESSUS, ISS Security Scanner, NAI CyberCop Scanner...) es capaz de revelar información que nos va a resultar útil al momento de reforzar la seguridad de nuestros servidores Web, incluso existen analizadores que están diseñados para auditar únicamente este servicio, como **whisker**.

Otra medida de seguridad básica es deshabilitar el Directory Indexing que por defecto muchos servidores incorporan. Se trata de una medida extremadamente útil u sencilla de implantar.

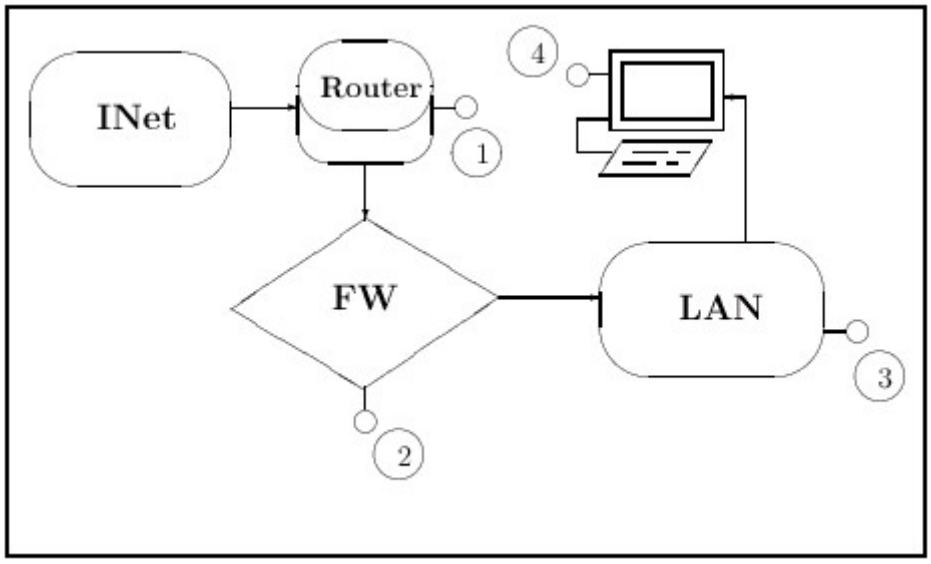


Figura 3 Puntos de defensa entre un atacante y su objetivo

2.5 Kerberos

Durante 1983, en el M.I.T (Massachussets Institute of Technology) comenzó el proyecto *Athena* con el objetivo de crear un entorno de trabajo educacional compuesto por estaciones gráficas, redes de alta velocidad y servidores; el sistema operativo para

implementar ese entorno era Unix 4.3BSD, y el sistema de autenticación utilizado se denominó *Kerberos.*

Hasta que se diseñó Kerberos, la autenticación en redes de computadoras se realizaba principalmente de dos formas: en la primera se aplicaba la autenticación por declaración, en la que el usuario era libre de indicar el servicio al que desea acceder, y en la otra se utilizaban contraseñas para cada servicio de red. El primer método proporcionaba un nivel de seguridad muy bajo, ya que se le otorgaba demasiado poder al cliente sobre el servidor. El segundo modelo tampoco era muy bueno ya que por un lado se obligaba al usuario a digitar continuamente su contraseña, de forma que se perdía mucho tiempo y además la contraseña estaba viajando continuamente por la red. Kerberos trata de mejorar estos esquemas intentando por un lado que un cliente necesite autorización para comunicarse con el servidor y por otro lado eliminando la necesidad de demostrar el conocimiento de información privada como lo es la contraseña del usuario.

El uso de Kerberos se produce principalmente en el login, en el acceso a otros servidores y en el acceso a sistemas de archivos en red. Una vez que un cliente está autenticado, o bien, se asume que todos sus mensajes son fiables, o si se desea mayor seguridad, se puede elegir trabajar con mensajes seguros (autenticados) o privados (autenticados y cifrados). Kerberos se puede implementar en un servidor que se ejecute en una máquina segura, mediante un conjunto de bibliotecas que utilizan tanto los clientes como las aplicaciones.

2.6 Criptología

La criptología es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicación. Esta ciencia está dividida en dos ramas: la **criptografía**, que se ocupa del cifrado de mensajes en clave y del diseño de criptosistemas y el **criptoanálisis**, que trata de descifrar los mensajes en clave rompiendo así el criptosistema.

Aunque el objetivo original de la criptografía era mantener en secreto un mensaje, en la actualidad no se persigue únicamente la privacidad o **confidencialidad** de los datos, sino que se persigue además garantizar la **autenticidad** de los mismos (el emisor del mensaje es quien dice ser y no otro), su **integridad** (el mensaje que se lee es el mismo que fue enviado) y su **no repudio** (el emisor no puede negar el haber enviado el mensaje)

2.7 Esteganografía

La esteganografía es la ciencia que estudia los procedimientos encaminados a ocultar la existencia de un mensaje en lugar de ocultar su contenido. Mientras que la criptografía pretende que un atacante que consigue un mensaje no sea capaz de averiguar su contenido, el objetivo de la esteganografía es ocultar ese mensaje dentro de otro sin información importante, de forma que el atacante ni siquiera se entere de la existencia de dicha información oculta.
No se trata de sustituir el cifrado convencional, sino de complementarlo, ocultar un mensaje reduce las posibilidades de que sea descubierto; no obstante, sí lo es, el que ese mensaje haya sido cifrado introduce un nivel adicional de seguridad.

2.8 Herramientas de software de seguridad

Ningún sistema operativo se puede considerar seguro tal y como se instala por defecto. Normalmente cualquier distribución de un sistema se instala pensando en proporcionar los mínimos problemas a un administrador que desee poner a trabajar la máquina inmediatamente, sin tener que preocuparse por la seguridad.

Algunas herramientas de seguridad que se pueden instalar en los sistemas operativos más conocidos son:

2.8.1 Titan

Es uno de los programas más fáciles de instalar, especialmente sobre SunOs o Solaris, al tratarse de un conjunto de shellscripts, el administrador no tiene por qué preocuparse por ningún proceso de compilación, ni conocer técnicas avanzadas de seguridad para poder utilizarlo.

2.8.2 TCP Wrappers

Existe una serie de servicios como telnet o ftp que habitualmente no se pueden cerrar, ya que los usuarios necesitarán conectarse al servidor para trabajar en él o para transferir archivos. En estos casos es peligroso permitir que cualquier máquina de Internet tenga la posibilidad de acceder a nuestros recursos, por lo que se suele utilizar un programa llamado TCP Wrappers para definir una serie de redes o máquinas autorizadas a conectarse al sistema.

2.8.3 SSH

El Secure Shell (SSH) es un software cuya principal función es permitir la conexión remota segura a sistemas a través de canales inseguros, aunque también se utiliza para la ejecución de órdenes en ese sistema remoto o para transferir archivos desde o hacia él de manera fiable.
SSH soporta el cifrado automático en sesiones X-Windows o modelos de seguridad más avanzados, como el cifrado NFS o la construcción de redes privadas virtuales. Su código fuente es libre para uso no comercial.

2.8.4 Tripwire

La herramienta Tripwire es un comprobador de integridad para archivos y directorios de sistemas Uníx. Compara uno de estos objetos con la información sobre los mismos almacenada previamente en una base de datos, y alerta al administrador en caso de que algo haya cambiado. La idea es simple, se crea un resumen de cada archivo o directorio importante para nuestra seguridad apenas se instala el sistema, y esos resúmenes se almacenan en un medio seguro, de forma que si uno de los archivos es modificado, Tripwire alertará la próxima vez que se realice la comprobación.

2.8.5 Nessus

Surge en 1998, como un analizador de vulnerabilidades gratuito, de código fuente libre y fácil de utilizar.
La distribución de Nessus consta de cuatro archivos básicos: las librerías de programa, las librerías NASL (Nessus Attack Scripting Languaje), el núcleo de la aplicación y sus plugins. Es necesario compilar en este orden cada una de esas partes. Además el programa requiere para funcionar correctamente pequeñas aplicaciones adicionales, como la librería GMP, necesaria para las aplicaciones de cifrado.

2.8.6 Crack

Crack, desarrollado por el experto en seguridad Alec Muffet, es el adivinador de contraseñas más utilizado en entornos Unix.

Este adivinador realiza una primera pasada sobre el archivo de claves intentado romper contraseñas en base a la información de cada usuario almacenada en el archivo. Se trata de unas comprobaciones rápidas pero efectivas, ya que aunque la cantidad de datos del archivo no es muy grande, se trata de información frecuentemente utilizada como password. Tras esa pasada, entran en juego los diccionarios para seguir adivinando contraseñas (un diccionario es un archivo con posibles contraseñas en él, generalmente uno por línea).

2.9 Herramientas de hardware de seguridad

2.9.1 Firewall (Cortafuego)

Un firewall o cortafuegos es un grupo de sistemas que hace cumplir una política de control de acceso entre dos redes.
Un firewall puede verse como un dispositivo que administra el acceso entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewall realiza la función de un filtro que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean, permite o deniega su paso. Para permitir o denegar una comunicación, el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo electrónico, etc. Dependiendo del servicio, el firewall decide si lo permite o no.
Cualquier firewall desde el más simple hasta el más avanzado, presenta dos graves problemas de seguridad, por un lado centralizan todas las medidas en un único sistema, de forma que si éste se ve comprometido y el resto de la red no está suficientemente protegido, un atacante conseguirá amenazar a toda la subred simplemente poniendo en jaque a una máquina.

El segundo problema, es la falsa sensación de seguridad que un firewall proporciona, generalmente un administrador que no disponga de un firewall, va a preocuparse por la integridad de todas las máquinas de la red, pero en el momento en que instala un firewall y lo configura, asume que toda su red está segura, por lo que se descuida la seguridad de los equipos de la red interna.

Además un firewall no protege contra ataques que no pasan por él, esto incluye todo tipo de ataques internos dentro del perímetro de seguridad, pero también otros factores que no deberían suponer un problema. El típico ejemplo de esto son los usuarios que sin permiso ni conocimiento del administrador de la red, y sin pensar en las consecuencias, instalan un módem en sus estaciones de trabajo.

2.9.2 Tipos de cortafuegos

2.9.2.1 Packet filter (filtrador de paquetes)

Limita la información de la red, basado en direcciones fuente y destino.

2.9.2.2 Proxy server

Solicita las conexiones entre un cliente en el lado interno del Firewall e Internet.

2.9.2.3 Stateful packet filtering

Limita la información de una red no sólo basado en la dirección fuente y destino, sino también basado en el contenido del paquete.

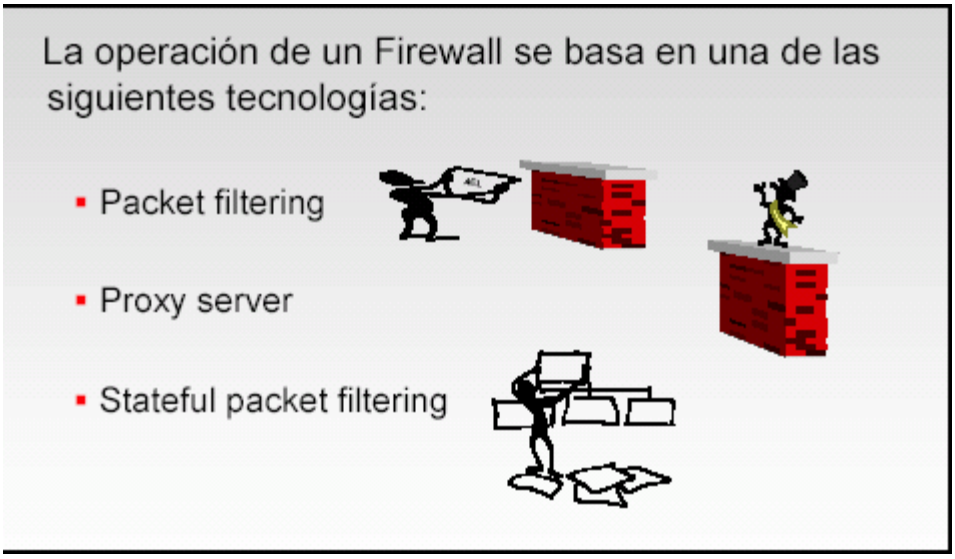


Figura 4: Operación de los Firewalls

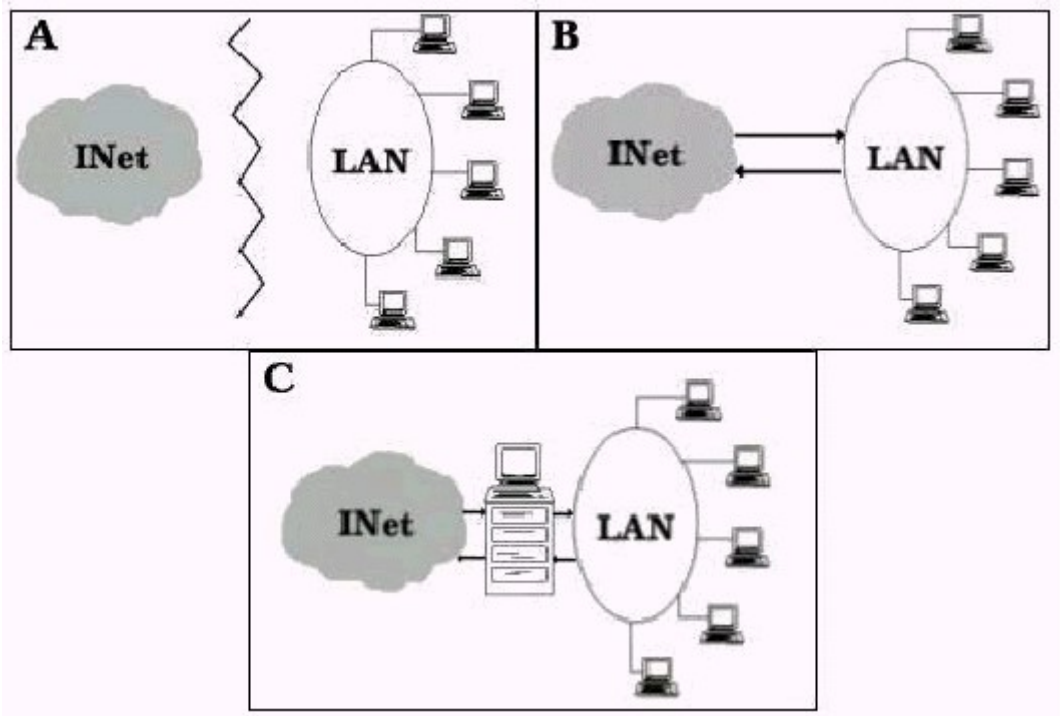


Figura 5: (A) Aislamiento, (B) Conexión total, (C) Firewall entre la zona de riesgo y el perímetro de seguridad

2.10 Redes

2.10.1 ¿Qué es una red?

Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, CD-Roms o impresoras y que son capaces de realizar comunicaciones electrónicas.

2.10.1.1 Objetivos de una red

- El objetivo principal de una red es lograr que todos sus programas datos y equipo estén disponible para cualquiera de la red que lo solicite, sin importar la localización física del recurso y del usuario.
- Otro de sus objetivos consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, es decir que todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias.
- El ahorro económico debido a que los ordenadores pequeños tiene una mejor relación costo / rendimiento, en comparación con la que ofrece las máquinas grandes.
- Proporciona un poderoso medio de comunicación entre personas que se encuentran en lugares distantes entre sí.

2.10.2 Clasificación de las redes

2.10.2.1 Redes de área local

Según Andrew Tanembaum (1997), las redes de área local, generalmente llamadas LAN (Local Area Network), son redes de propiedad privada dentro de un solo edificio o

campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos (por ejemplo impresoras) e intercambiar información. Las LAN se distinguen de otro tipo de redes por tres características:

1. su tamaño
2. su tecnología de transmisión
3. su topología

Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas, como las líneas compartidas de la compañía telefónica que solían usarse en áreas rurales. Las LAN tradicionales operan a velocidades de 10 a 100 Mbps, tienen bajo retardo (décimas de microsegundos) y experimentan muy pocos errores.

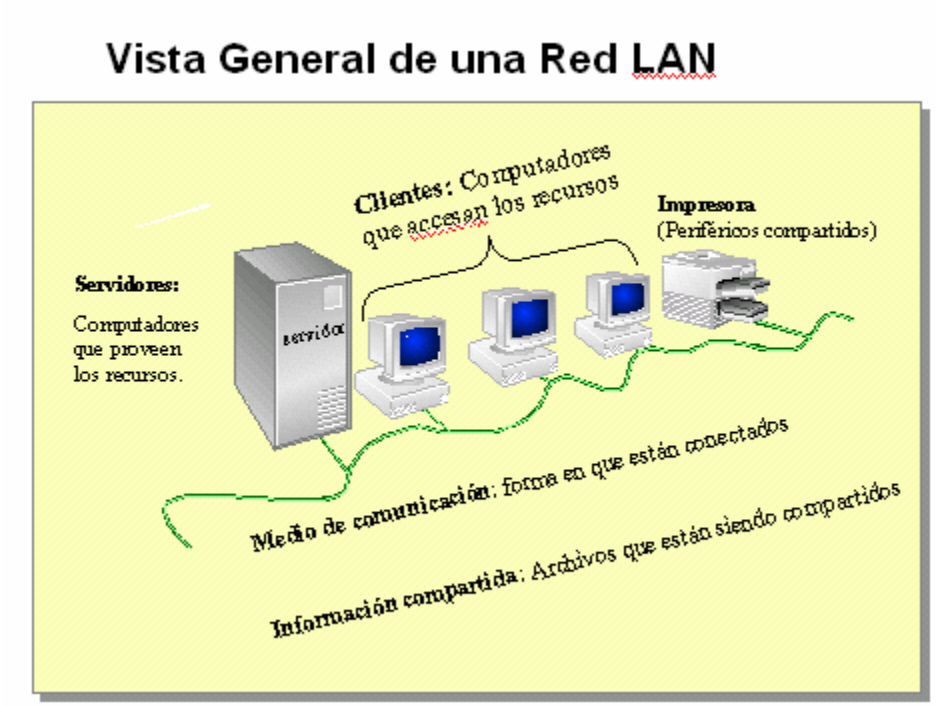


Figura 6. Vista de una red LAN

2.10.2.2 Redes de área ancha

Según Andrew Tanembaum (1997), una red de área amplia, o WAN (Wide Area Network) se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (es decir, de aplicación). Estos hosts están conectados por una subred de comunicación, o simplemente subred. El trabajo de la subred es conducir mensajes de un host a otro, así como el sistema telefónico conduce palabras del que habla al que escucha. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (los hosts), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos, canales o troncales) mueven bits de una máquina a otra.
Los elementos de conmutación son computadoras especializadas que conectan dos ó más líneas de transmisión.
Un término genérico para las computadoras de conmutación, se usa la palabra enrutador.
En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas, cada una conectada a un par de enrutadores. Cuando se envía un paquete de un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe completo en cada enrutador intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía.

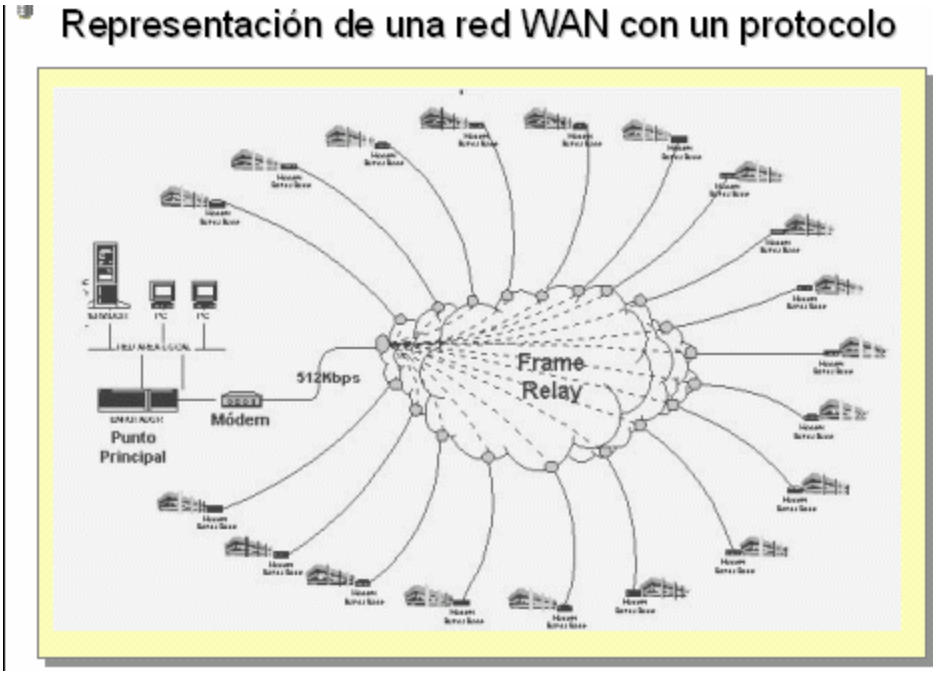


Figura 7 Red WAN con un protocolo

CAPÍTULO 3 METODOLOGÍA

Este capítulo describe la investigación realizada sobre los factores críticos de éxito que se deben de considerar para la implementación de una guía de seguridad para redes e Internet, que pueda ser aplicado en empresas financieras que tienen páginas Web en las cuáles los clientes puedan realizar diversas transacciones monetarias.
Para realizar esta investigación, se aprovechó el conocimiento y experiencia de personas que tienen asignado en su empresa, un puesto de encargado de seguridad informática.

3.1 TIPO DE INVESTIGACIÓN

En el presente estudio se utilizó el enfoque de investigación descriptiva, la cual es una herramienta fundamental para cumplir con los objetivos del proyecto, específicamente el objetivo de propuesta relacionado con los factores críticos de éxito que debe contemplar la formulación de una guía de seguridad.

Investigación Descriptiva

Los estudios descriptivos pueden especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis, según lo indican Hernández, Fernández y Baptista (1998).

Este tipo de investigación mide o evalúa diversos aspectos, dimensiones o componentes del fenómeno o fenómenos por investigar. Desde el punto de vista científico, describir es medir, por ello se relaciona con una serie de cuestiones y se mide cada una de ellas independientemente, para así, describir lo que se investiga con la mayor precisión posible.

La investigación descriptiva, en comparación con la naturaleza poco estructurada de los estudios exploratorios, requiere considerable conocimiento del área que se investiga para formular las preguntas específicas que busca responder, por lo que puede ser más o menos profunda pero en cualquier caso se basa en la medición de uno o más atributos del fenómeno descrito. (Hernández, Fernández y Baptista, 1998)

En este trabajo de investigación, se utilizó el tipo de investigación descriptiva para la recopilación de datos, con ello se permitió la interpretación de la información analizada con el fin de dar mejores resultados.

3.2 FUENTES DE INFORMACIÓN

Población y Muestra

Se entiende por población al conjunto de elementos que pueden ser personas, animales, empresas, organizaciones, objetos y otros. Así con el estudio se pretende conocer las características del conjunto y generalizar los resultados o conclusiones que se obtengan.

Una población puede ser finita o infinita. La población finita tiene un número limitado de elementos, mientras que una población infinita la forman un número ilimitado. Se procedió a definir una población finita, la cual consistió en aquellos sujetos por ser entrevistados o bien a los cuales se les aplicó un cuestionario.

La muestra seleccionada para ambos instrumentos es de tipo no probabilística o también conocida como muestra dirigida, donde según Hernández, Fernández y Baptista (1998), la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de investigación, donde la elección de sujetos depende del criterio del investigador.

Para el proceso de recolección de datos, el cuestionario fue contestado por 7 personas que trabajan en un departamento de seguridad informática, en instituciones financieras. Estos 7 oficiales de seguridad informática, tienen mucho conocimiento y experiencia en elaboración de manuales de seguridad informática y labores de monitoreo y soporte técnico de herramientas de seguridad.

Con el fin de obtener un mejor criterio de la totalidad de la población seleccionada, se van a tomar en cuenta todas las respuestas dadas por los sujetos en la contestación del cuestionario.

Documentación

Se dispuso de libros para consulta bibliográfica, artículos en Internet y se asistió a dos charlas de Seguridad Informática, la primera impartida en la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT) el día 14 de noviembre del 2003 con motivo de una charla organizada por la universidad válida por un sello verde, y la segunda en el Banco Nacional de Costa Rica el día 28 de noviembre del 2003 como parte de la celebración del día mundial de Seguridad Informática. Tanto las consulta bibliográficas, artículos de Internet y las charlas, proporcionaron datos teóricos para la investigación y con ello obtener la base para formular instrumentos de acuerdo con lo requerido por el objetivo planteado.

3.3 DESCRIPCIÓN DE LOS INSTRUMENTOS

Cuestionarios

El principal objetivo del cuestionario planteado consistió en recopilar datos en forma escrita para una fácil captura de información y análisis sobre los factores requeridos para el éxito de la implementación de una guía de seguridad y la formulación de un documento donde se expongan cuáles serán las mejores políticas de seguridad a seguir por una empresa financiera que tenga una página Web donde los clientes puedan realizar transacciones monetarias.

El cuestionario utilizado se aplicó a personal del departamento de seguridad informática de instituciones financieras públicas y privadas. Los nombres de las instituciones no se nombran a petición de las personas involucradas para no comprometerlas ni comprometer al empleado que contestó el cuestionario.

3.4 ANÁLISIS DE DATOS

Después de aplicar los cuestionarios se realizó un proceso de análisis de los datos recolectados.

Para la tabulación de los datos obtenidos se utilizó el software de Microsoft Excel 2000, esta herramienta permitió la elaboración de gráficas de acuerdo con el análisis de datos realizados.

Análisis del cuestionario

Después de la recopilación de datos con el fin de poseer y brindar a los clientes de instituciones financieras, un ambiente de seguridad adecuado en dónde hacer transacciones monetarias, se obtienen las siguientes conclusiones:

- La interrupción de los servicios provocada por virus informáticos y ataques tanto internos como externos, afecta a las empresas fundamentalmente en la pérdida de negocios, imagen y confiabilidad.

- El aseguramiento de la continuidad de los servicios críticos resulta imperativa para la operación de la organización.

- La falta de políticas de seguridad efectivas, de una adecuada infraestructura tecnológica y de una figura departamental que se encargue de la seguridad informática de una empresa, puede traer como consecuencia que la empresa no sólo se vea amenazada, sino que sea blanco de algún tipo de ataque que pueda comprometer la información real de los clientes.

Como factores críticos de éxito para la definición de políticas de seguridad efectivas, así como de la infraestructura tecnológica a utilizar, se destacan diversos aspectos los cuales se pueden agrupar en factores técnicos, de comportamiento y administrativos.

Según los datos obtenidos entre los factores podemos distinguir:

Factores Técnicos

Estos factores están relacionados con la tecnología, en aspectos propiamente de hardware o software.

- Requerimientos

Tener la visión y compresión de los requerimientos y objetivos de la solución por implementar, con ello se pueden cumplir las expectativas de la empresa en cuanto a la solución de seguridad.

Estos requerimientos y objetivos son fundamentales cuando se necesita de proveedores para la implementación de la solución y también para la definición de los perfiles de las personas que formarán parte de una unidad de seguridad informática.

- Características de las políticas de seguridad

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización. Por esta razón, las políticas de seguridad por definir, deben ser claras y de fácil compresión y cumplimiento para los empleados.

Las políticas de seguridad informática deben considerar los siguientes elementos:

- Se debe establecer claramente cuál será el alcance de las políticas, incluyendo los sistemas y el personal sobre los cuáles aplican
- Deben estar definidos claramente los objetivos de la política y la descripción clara de los elementos involucrados en su definición
- Deben indicar las responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización
- Debe tener la definición de sanciones en caso de no cumplirse las políticas
- Se deben definir las responsabilidades de los usuarios con respecto a la información a la que se tiene acceso
- Deben ofrecer explicaciones compresibles sobre por qué se deben tomar ciertas decisiones y explicar la importancia de los recursos
- Deben establecer las expectativas de la empresa en relación con la seguridad y especificar la autoridad responsable de aplicar las sanciones

- Las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan su compresión clara
- Deben seguir un proceso de actualización periódica con respecto a los cambios más relevantes dentro de la empresa, tales como aumento de personal, rotación de personal, cambios en la infraestructura computacional, desarrollo de nuevos servicios, etc.

- Infraestructura de hardware

La selección de hardware debe ser de acuerdo con las necesidades de la empresa específicamente a nivel de seguridad, para ello se debe contar con un modelo físico donde quede organizada de la mejor manera la topología de las redes internas de la empresa y su correspondiente enlace hacia las redes de datos exteriores.

- Software por utilizar

Las herramientas de software que se utilicen deben contar con una interfase amigable al usuario y una operación de menú estándar, con el fin de realizar una administración más eficiente. Deben ser, además, fáciles de operar. Antes de adquirir cualquier herramienta de software, es recomendable realizar un estudio de mercado para asegurarse de que la herramienta va a cumplir satisfactoriamente con las necesidades de la empresa.

Factores de Administración

Los factores de administración se refieren a las metodologías de trabajo, y a aspectos de gestión empresarial.

- Etapas para implantar un sistema de seguridad informática en la empresa

Para hacer un buen planeamiento de las soluciones de seguridad informática con que deberá contar la empresa, es necesario cumplir con los siguientes requisitos:

- Introducir el tema de seguridad en la visión y misión de la empresa

- Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes
- Designar y capacitar a los jefes, supervisores y operadores del departamento de informática
- Definir y trabajar sobretodo las áreas donde se pueden lograr mejoras relativamente rápidas
- Velar porque las comunicaciones internas sean efectivas
- Identificar las áreas de mayor riesgo para la empresa y trabajar en ellas planeando soluciones efectivas
- Capacitar a todos los empleados en los elementos básicos de seguridad y riesgo para el manejo de software, hardware y seguridad física

- Documentación

Es importante realizar la documentación técnica correspondiente a la información más relevante que se tenga con respecto a la experiencia en soluciones de seguridad tanto a nivel de hardware como de software.

También es muy importante documentar las experiencias que se tengan con relación a ataques informáticos que haya sufrido la empresa, sobretodo en como se logró identificar, como se corrigió, como se puede prevenir en el futuro y qué implicaciones tuvo para la empresa.

- Análisis costo / beneficio

Es importante realizar un estudio de costo/beneficio en función de la criticidad del servicio, la probabilidad de falla y el costo de proveer la solución, es decir, va en directa relación con el tipo de negocio, lo primero que se debe hacer es valorizar el costo del "no servicio".

Factores de Comportamiento

Los factores de comportamiento se refieren específicamente a las relaciones personales entre los miembros del equipo de trabajo y necesidades dadas por las personas para un mejor entendimiento de la solución, es decir factores de motivación.

Dentro de los beneficios que se pueden obtener, al tener un ambiente en el que los empleados trabajen en una plataforma de seguridad confiable, están los siguientes:

- Aumento de la productividad
- Aumento de la motivación del personal
- Compromiso con la misión de la compañía
- Mejora de las relaciones laborales
- Ayuda a formar equipos competentes
- Mejoramiento del clima laboral

Análisis de cuestionarios

El cuestionario aplicado permitió obtener datos importantes sobre la situación actual que están experimentando empresas financieras que le brindan a sus clientes la facilidad de realizar transacciones monetarias desde cualquier computadora con conexión a Internet. También ayudó a identificar algunos factores requeridos para el éxito de la implementación de soluciones de seguridad a nivel de redes LAN y WAN y además para bases de datos y sobre dificultades presentadas durante el proceso de implementación. Los diferentes factores evaluados corresponden a determinar:

- Identificación de la alta gerencia con el papel de un departamento de seguridad informática
- Herramientas más usadas con respecto a tráfico de información proveniente de Internet
- Figura de un departamento de seguridad informática
- Pruebas y análisis de vulnerabilidades
- Políticas de seguridad
- Ataques a la institución

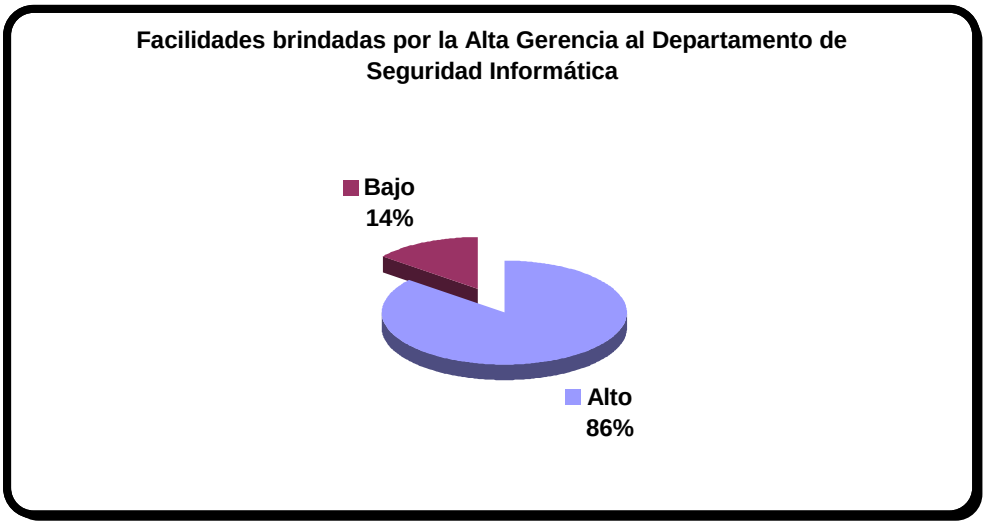
- Medidas de contingencia

El detalle de los aspectos evaluados se presenta a continuación mediante el uso de gráficas y tablas que interpretan los resultados obtenidos después de la aplicación del cuestionario.

Tabla # 1

Facilidades brindadas por la Alta Gerencia al Departamento de Seguridad Informática

Categoría	Frecuencias	%
Alto	6	85.71
Bajo	1	14.29
Total	**7**	**100**



Gráfica # 1: Facilidades brindadas por la Alta Gerencia al Departamento de Seguridad Informática

Fuente: Resultado de análisis de cuestionarios, Agosto 2004

En la tabla # 1 se presentan los datos que consideran los sujetos a los que se les aplicó el cuestionario, es el nivel de identificación que tiene la Alta Gerencia de la empresa, con respecto a las facilidades

La gran mayoría consideran que la Alta Gerencia de la empresa está bien identificada con la importancia de contar con una estructura tecnológica sólida, que le permita minimizar al máximo el riesgo de sufrir ataques por parte de hackers, virus, gusanos, etc, que puedan traer como consecuencia pérdidas de información de clientes, afectación del servicio al cliente y la consecuente afectación de la imagen de la empresa.

Solamente un sujeto consideró, que la empresa, al ser de carácter financiero y de bienes y servicio, la alta gerencia brinda un mayor apoyo a otras áreas ajenas a la seguridad informática. Esto sobretodo en relación con capacitación del personal, infraestructura y espacio físico del centro de cómputo.

Tabla # 2

Acceso a Internet

Categoría	**Frecuencias**	**%**
Servidor Proxy	7	100
MODEM	0	0
Total	7	100

Todos los sujetos a los que se les aplicó el cuestionario, indicaron que su empresa cuenta con un servidor Proxy para el acceso a Internet, y que el uso de módems está prohibido según lo indica una política interna.

Tabla # 3

Herramientas de seguridad

Categoría	**Frecuencias**	**%**
Detector de intrusos	7	100
Antivirus	7	100
Enrutador con filtrado de paquetes	5	71.42
Firewall (Hardware y/o Software)	7	100

Los resultados de la tabla # 3, indican que los sujetos aseguran contar en sus empresas con herramientas de hardware y software que les permiten minimizar al máximo posible un problema que pueda ocasionar una denegación de servicio o pérdida de datos.

Tabla # 4

Encargado de seguridad

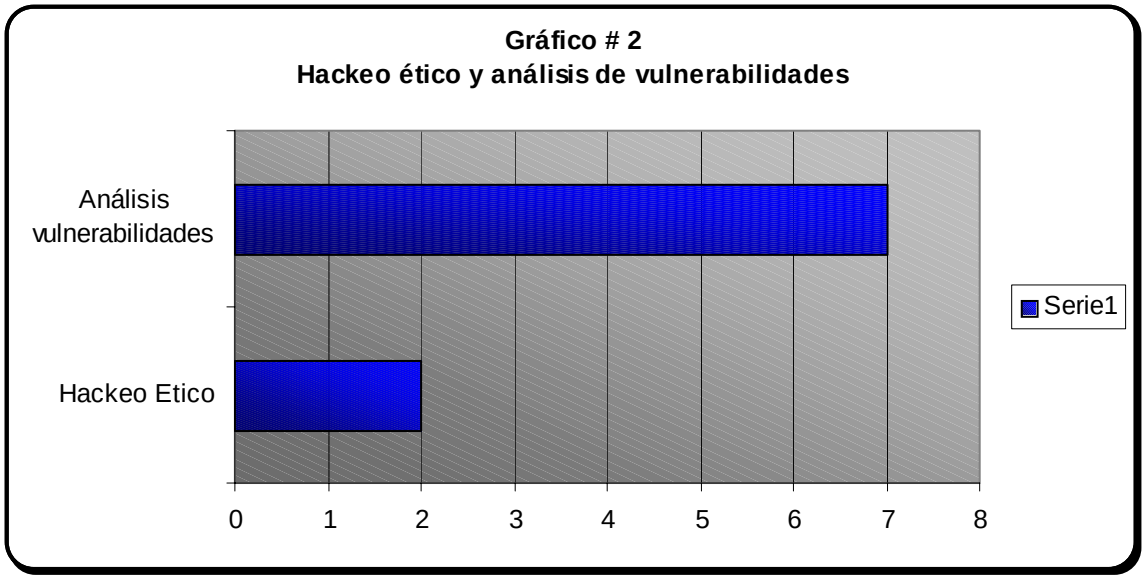
Categoría	**Frecuencias**	**%**
Existe una figura o departamento	7	100
No existe una figura o departamento	0	0

Los resultados de la tabla # 4, indican que en las empresas se cuenta con un encargado o departamento que vela por el control, cumplimiento e implementación de políticas de seguridad.

Tabla # 5

Pruebas de penetración y vulnerabilidades

Categoría	**Frecuencias**	**%**
Pruebas de penetración (Hackeo ético)	2	28.5
Análisis de vulnerabilidades	7	100



Fuente: Resultado de análisis de cuestionarios, Agosto 2004

Los resultados reflejados por la tabla # 5 y representados en el gráfico # 2, indican que solamente dos de los siete sujetos a los que se les aplicó el cuestionario, indican que en sus empresas se realizaron o se realizan pruebas de penetración o hackeo ético, aunque no se indica la periodicidad de las mismas.

Sin embargo, todos los sujetos aseguraron que en sus empresas, se hacen actualizaciones periódicas de los parches que corrigen vulnerabilidades detectadas en sus respectivos sistemas operativos. Además, aseguran contar con herramientas que les permiten detectar otras vulnerabilidades que no se corrigen con la aplicación de parches. En algunos casos se indicó que la corrección de las vulnerabilidades se hace de acuerdo con el nivel de peligro de la vulnerabilidad detectada.

Tabla # 6

Políticas de seguridad

Categoría	**Frecuencias**	**%**
Definidas	7	100
No definidas	0	0
Total	**7**	**100**

Todos los sujetos consultados indicaron que en sus empresas existen definidas políticas de seguridad. Dentro de las que más se mencionan están las siguientes:

- ***Seguridad del Personal*:** todo lo referente a los colaboradores de la organización, especialmente en lo que se refiere a sus responsabilidades. Incluyendo entre otros temas: confidencialidad, responsabilidad de los usuarios sobre los equipos (Hardware), responsabilidad de los usuarios sobre los programas (Software), Integridad física del personal, acceso a las áreas restringidas, acceso fuera de horas de oficina.

- ***Seguridad Física*:** normas establecidas para lograr minimizar las amenazas relacionadas con equipo computacional. Incluye entre otros temas: control de temperatura en el área de servidores, equipo de respaldo para el servidor de datos, capacitación en el uso de extintores, mantenimiento preventivo y correctivo, disponibilidad de equipo.

- ***Seguridad Lógica*:** normas establecidas para lograr seguridad a nivel de datos, de sistemas de información y de accesibilidad. Incluye entre otros temas: respaldo y recuperación de información, plan de contingencia, protección contra virus, seguridad en sistemas operativos, detección de intrusos, administración de usuarios y claves, estándar de claves de usuario, cambio periódico de claves, control de inactividad de estaciones de trabajo, control de acceso a la red y a las aplicaciones, inventario de software, procedimientos contra alteración de información, políticas para el uso de Internet.

- Claves de acceso a los diferentes sistemas reguladas por puesto y horario de trabajo.
- Restricción de accesos a sistemas
- Restricción de accesos al Web
- Administración de recursos informáticos

Tabla # 7

Conocimiento de las políticas de seguridad

Categoría	**Frecuencias**	**%**
Conocimiento de todo el personal	7	100
Desconocimiento por parte de algún departamento	0	0
Total	**7**	**100**

Todos los sujetos indicaron que las políticas de seguridad son del conocimiento de todo el personal de la empresa.

Tabla # 8

Distribución de las políticas de seguridad

Categoría	**Frecuencias**	**%**
Publicadas en la Intranet de la Empresa	7	100
Difundidas mediante correos electrónicos	7	100
Publicadas en boletines informativos o manuales	4	57.14

Existen diferentes medios de distribución del conocimiento de las políticas internas de seguridad de las empresas. En algunos casos se indicó, que por problemas en las líneas de transmisión de algunas sucursales, el uso del protocolo “http”, está limitado pues consume mucho ancho de banda. A estas sucursales se les hace llegar las políticas mediante un manual y dicho manual debe ser leído por todo el personal de la sucursal. Hay empresas que periódicamente publican boletines informativos en los cuales una sección de dicho boletín, está destinada a la publicación de políticas internas de riesgo.

El control del cumplimiento de dichas políticas, es básicamente el mismo entre las empresas. Periódicamente, se nombra a uno o a varios empleados de cada departamento para que verifique el debido cumplimiento por parte de todos los demás compañeros del departamento. En algunos casos, esta evaluación se hace escogiendo empleados al azar y cuando el tiempo lo permite, la evaluación se hace para todos los empleados. Además, la Auditoría Interna de cada empresa, debe hacer observaciones y recomendaciones en

caso de que algún aspecto o política de seguridad no se esté cumpliendo, y estas recomendaciones deben ser atendidas con la mayor brevedad posible.

Tabla # 9:

Herramientas de Software para administrar seguridad

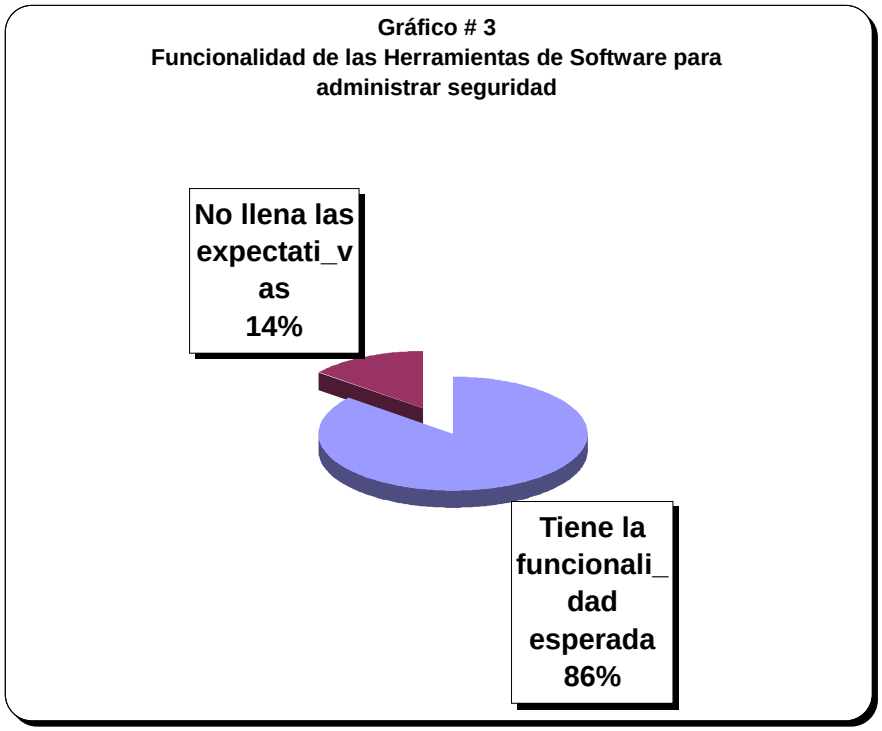
Categoría	**Frecuencias**	**%**
Cuenta con herramientas de software	7	100
No cuenta	0	0,0
Total	**7**	**100**

Todos los sujetos consultados indicaron que en su empresa cuentan con una o más herramientas de seguridad a nivel de software, que les permite tener una mejor administración de la seguridad.

Tabla # 10:

Funcionalidad de las Herramientas de Software para administrar seguridad

Categoría	**Frecuencias**	**%**
Tiene la funcionalidad que la empresa necesita	6	85.71
No llena las expectativas	1	14.29
Total	**7**	**100**



Fuente: Resultado de análisis de cuestionarios, Agosto 2004

La gran mayoría de los sujetos consideran que las herramientas de software cumplen las expectativas de funcionalidad esperadas con respecto a ayudar en la administración de la seguridad. Sin embargo, uno de los individuos considera que la herramienta no llena las expectativas, ya que sufrieron el ataque de un hacker, y provocó varios problemas que por razones obvias no fueron mencionados.

Como complemento a la información anterior, la mayoría de las empresas hicieron un estudio de mercado que les permitiera comparar las propiedades de varias herramientas antes de adquirir una para la empresa. Esto por cuanto en la empresa existe un comité que se encarga de supervisar las compras, sobretodo en las instituciones públicas.

Un sujeto indicó que la empresa no realizó un estudio de mercado, sino que se hizo un estudio de las herramientas que en ese momento había disponibles para las necesidades propias de la empresa.

Tabla # 11

Contrato para las herramientas de seguridad

Categoría	Frecuencias	%
Cuentan con contrato	6	85.71
No cuentan	1	14.29
Total	**7**	**100**

La mayoría de los sujetos indicó que sus empresas tienen contratos que les permiten realizar actualizaciones al software de las herramientas de seguridad. Solamente un sujeto indicó que su empresa no posee un contrato de mantenimiento que le permita realizar actualizaciones al software de la herramienta de seguridad utilizada en ella. No se indicaron las razones del caso.

Tabla # 12

Conocimiento de técnicas de ataque

Categoría	Frecuencias	%
Todas	0	0
Algunas	4	57
Las más utilizadas	3	43

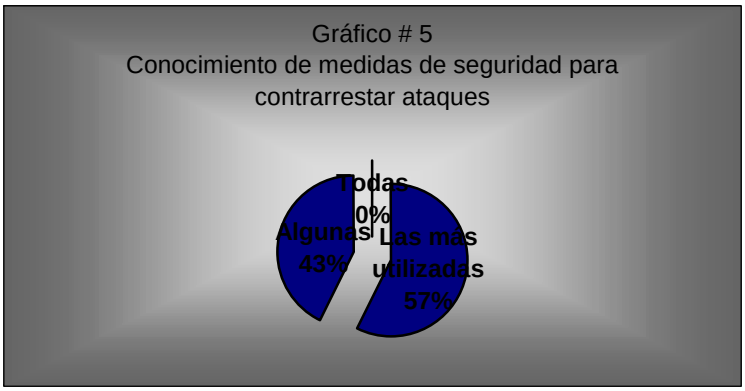
Fuente: Resultado de análisis de cuestionarios, Agosto 2004

Tal como se muestra en la tabla # 12 y el gráfico # 4, los sujetos a los cuales se les aplicó el cuestionario, no aseguraron tener el conocimiento de todas las técnicas de ataque utilizadas por hackers o crackers. Unos reconocieron que tienen el conocimiento de algunas y otros indicaron que tienen conocimiento de las más utilizadas.

Tabla # 13

Medidas de seguridad que contrarrestan ataques

Categoría	**Frecuencias**	**%**
Todas	0	0
Algunas	3	43
Las más utilizadas	4	57



Fuente: Resultado de análisis de cuestionarios, Agosto 2004

Tal como se muestra en la tabla # 13 y el gráfico # 5, los sujetos a los cuales se les aplicó el cuestionario, no aseguraron tener el conocimiento de todas las medidas de seguridad que contrarrestan los ataques indicados en la tabla # 12. Unos reconocieron que tienen el conocimiento de algunas y otros indicaron que tienen conocimiento de las más utilizadas.

Tabla # 14

Ataques sufridos por virus, gusanos o troyanos

Categoría	Frecuencias	%
No han sufrido ataques	0	0
Sí han sufrido ataques	7	100
Total	7	100

Todos los sujetos indicaron que sus empresas han sufrido ataques de virus, gusanos o troyanos, tales como SQL-Slammer, Blaster, Sobig, Red Code, Nimda, etc.

Tabla # 15

Control documentado de ataques sufridos

Categoría	Frecuencias	%
Se documentan sucesos sufridos	7	100
No se documentan	0	0
Total	7	100

Todos los sujetos indicaron que sus empresas han documentado los inconvenientes provocados por ataques de virus, gusanos, troyanos o intrusiones.

Tabla # 16

Actualización de conocimientos

Categoría	Frecuencias	%
Se actualizan los conocimientos	7	100
No se actualizan	0	0
Total	7	100

Los sujetos involucrados aseguraron que el personal encargado de la seguridad informática, está en constante actualización de conocimientos. Esta actualización es muy variada entre las que más se mencionaron están:

- Inscripción a sitios de Internet de reportes y contratos de mantenimiento
- Asistencia a seminarios
- Asistencia a capacitaciones
- Proveedores expertos
- Noticias
- Inscripción en revistas especializadas en informática

Tabla # 17

Medidas de respaldo y recuperación

Categoría	**Frecuencias**	**%**
Se cuentan en la empresa	7	100
No se cuenta	0	0
Total	7	100

Los sujetos involucrados aseguraron que en sus empresas, se tienen medidas de respaldo y eventuales recuperaciones, en caso que la empresa sufra algún inconveniente. Entre los más señalados están:

- Respaldos y replicación a nivel de base de datos
- Respaldos de información de usuarios
- Contingencia de equipos
- Contingencia geográfica

Tabla # 18

Ventanas de tiempo estimados ante problemas en la página Web

Categoría	**Frecuencias**	**%**
Se cuentan en la empresa	7	100
No se cuenta	0	0
Total	7	100

Los sujetos involucrados aseguraron que en sus empresas, se tienen estimadas ventanas de tiempo máximo en las cuáles la página Web podría estar fuera de servicio ante una eventualidad. El tiempo estimado ha sido calculado por 2 factores:

- Estimaciones (1 sujeto)
- Realizando pruebas y simulacros (6 sujetos)

Análisis de la aplicación del cuestionario

Después de aplicado el cuestionario y de realizar un análisis de los resultados obtenidos, se pueden concluir los siguientes aspectos:

- La alta gerencia de las empresas, está conciente de la importancia de contar actualmente con una infraestructura tecnológica y personal capacitado, que permita tener lo más segura posible la página Web y los datos de la empresa, ante un eventual ataque
- Las políticas de seguridad de cada empresa, tratan de ser lo más efectivas posibles y que sean del conocimiento y cumplimiento del personal
- Las empresas realizan distintas pruebas de vulnerabilidades en sus equipos, con el fin de tener corregidos los problemas más críticos que puedan ocasionar un daño grave al equipo o a la información contenida en ellos
- Las empresas cuentan con distintas herramientas de seguridad que les permite tener una administración más segura y eficiente de sus recursos tecnológicos. Según la información suministrada por los sujetos en estudio, la gran mayoría de estas herramientas llenan o cumplen con las expectativas de funcionalidad que la empresa necesita o para la que fueron adquiridas
- En general, las empresas poseen contratos sobre sus herramientas de seguridad, que les permiten realizar actualizaciones sobre las mismas con el fin de minimizar al máximo el riesgo
- El conocimiento de todas las técnicas de ataque por parte de crackers o hackers no es del total conocimiento de los oficiales de seguridad informática, sin embargo, aseguraron que tienen el conocimiento de las técnicas más utilizadas por los atacantes. De igual manera, el conocimiento de las medidas que contrarrestan los

ataques, son las más utilizadas y efectivas dentro de las que los oficiales de seguridad tienen conocimiento

- Todos los sujetos indicaron que sus empresas han sufrido algún problema ocasionado por virus, gusanos o troyanos y que estos ataques han sido documentados con el fin de prevenir al máximo futuros problemas
- Los sujetos indicaron que en sus respectivas empresas se cuenta con distintas medidas de respaldo y recuperación de datos, en caso de sufrir algún inconveniente
- El tiempo máximo que puede estar fuera de servicio la página Web de la empresa está contemplado por estimaciones y realización de pruebas y simulacros

CAPÍTULO 4 DIAGNÓSTICO

El uso de herramientas de seguridad, debe ser complementado con políticas de seguridad efectivas. Los usuarios de los distintos equipos deben ser responsables de cumplir y hacer cumplir las políticas y procedimientos que la empresa determine.

Algunas políticas de seguridad que siempre se deben tener en cuenta son las siguientes:

4.1 Políticas de Software

- Se considera como Software autorizado, tanto los sistemas operacionales como aquellos paquetes de usuario final y de sistemas aplicativos, que el Departamento de Informática ha instalado, previo visto bueno para su adquisición y con la Autorización legal del proveedor para su uso

- No practique el pirateo de software, ya que es ilegal y en diversos grados, peligroso. El uso de Software no autorizado o adquirido ilegalmente, se considera como pirata y una violación a los derechos de autor

- Se debe asegurar de que la instalación del software de la red, se realiza correctamente

- Se podrá utilizar únicamente el software que el departamento de Informática haya instalado y oficializado

- Tanto el software como los datos, son propiedad de la empresa. La copia o sustracción o daño intencional o utilización para fines distintos a las labores propias de la empresa, será sancionada de acuerdo con las normas y reglamento interno de la empresa

- El Departamento de Informática llevará el control del software instalado, basándose en el número de licencia que contiene cada uno

- Periódicamente, el Departamento de Informática deberá efectuar visitas para verificar el software utilizado en cada dependencia. Por lo tanto, el detectar

software no instalado por esta dependencia, será considerado como una violación a las normas internas de la empresa

- Toda necesidad de software adicional debe ser solicitada por escrito al Departamento de Informática, quien justificará o no dicho requerimiento, mediante la realización de un estudio de evaluación

- El Departamento de Informática instalará el software en cada computador y entregará a los usuarios los manuales correspondientes, los cuales quedarán bajo la responsabilidad del Jefe del departamento respectivo

- Los disquetes, discos compactos o cualquier medio de almacenamiento que contienen el software original de cada paquete, serán administrados y almacenados por el departamento de informática

- El Departamento de Informática proveerá el personal y una copia del software original en caso de requerirse la reinstalación de un paquete determinado

- El departamento de informática actualizará el software comprado cada vez que una nueva versión salga al mercado, a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización

- Se debe realizar cuando menos, una auditoría anual a los sistemas
- Si el sistema operativo de la empresa es de red, muy probablemente vendrá incluido algún utilitario de auditoría. Este utilitario se debe aprovechar para realizar auditorías internas parciales con más frecuencia

- Si un experto descubre agujeros en el sistema, no se debe suponer que es difícil que alguien los descubra. Estos problemas no se pueden dejar sin solución

4.2 Políticas sobre Seguridad física de los equipos y usuarios

- Deben estar claramente delimitadas y restringidas las diferentes áreas de accesos a los equipos de cómputo más críticos de la empresa

- El equipo de cómputo deberá estar ubicado en un área con baja posibilidad de inundación, incendio, robo y demás riesgos

- Todo el equipo de cómputo debe estar conectado a una U.P.S.

- Únicamente los equipos de cómputo pueden estar conectados a la UPS

- Se podrá utilizar únicamente el hardware y que el Departamento de Informática haya instalado y oficializado

- El hardware utilizado por el usuario es propiedad de la empresa. La sustracción o daño intencional o utilización para fines distintos a las labores propias de la empresa, será sancionada de acuerdo con las normas y reglamento interno de la empresa

- El Departamento de Informática llevará el control del hardware instalado, basándose en el número de serie que contiene cada uno

- Toda necesidad de hardware adicional debe ser solicitada por escrito al departamento de informática, quien justificará o no dicho requerimiento, mediante la realización de un estudio de evaluación

- La prueba, instalación y puesta en marcha de los equipos y/o dispositivos, serán realizadas por el Departamento de Informática, el cual, una vez se compruebe el correcto funcionamiento, deberá oficializar su entrega al área respectiva mediante un documento oficial o acta

- Ubicar el equipo en un área donde no exista mucho movimiento de personal

- No trasladar ningún equipo de cómputo sin la autorización y asesoría del departamento de informática

- Instalar los equipos de computo sobre escritorios o muebles estables o especialmente diseñados para ello

- Ubicar los equipos de cómputo más críticos para la empresa lejos de la luz del sol y de ventanas abiertas

- No conectar otros aparatos (Radios, maquinas de escribir, calculadoras, etc.) en la misma toma del computador

- Cada usuario, al momento de terminar las labores diarias, deberá apagar los equipos (Computadora , Impresoras, Escanners)

- Evitar la colocación, encima o cerca de la computadora ganchos, clips, bebidas y comidas que se pueden caer accidentalmente dentro del equipo

- No fumar cerca de los equipos. El alquitrán se adhiere a las piezas y circuitos internos del equipo

- Mantener libres de polvo las partes externas del computador y de las impresoras. Para esto se debe utilizar un paño suave y seco. Jamás usar agua y jabón. Solicitar al técnico de mantenimiento una tarea total de limpieza de estos equipos

- Mantener la pantalla y el teclado cubiertos con fundas plásticas cuando no haga uso de ellos por el tiempo considerable o si planea el aseo o reparaciones de las áreas aledañas al computador

- No se debe destapar y tratar de arreglar los equipos por cuenta propia. En todos los casos es necesario asesorarse del departamento de informática o del encargado de esta operación

- No prestar los equipos o asegurarse que la persona que los utilizará conoce su correcta operación

- Todas las pantallas de los equipos deberán contar con filtros antirreflectivos

- Se debe contar con sistemas de vigilancia (en buen estado) en las áreas críticas

- Se debe contar con un sistema que permita controlar la humedad relativa del ambiente, así como de la temperatura ambiental

- Al menos las áreas críticas del centro de cómputo, deben contar con detectores de humo

- Se debe contar con extintores de incendio que ayuden a combatir los diferentes tipos de fuego

4.3 Políticas de seguridad a nivel de red

- Se debe considerar la posibilidad de que ciertos equipos, como los enrutadores, switches y servidores, estén fuera del alcance de usuarios no autorizados

- Se deben configurar correctamente los protocolos de seguridad en sistemas de red. Si se desconoce como hacerlo, se debe recurrir a un experto para que le diseñe uno e incluso para que sea él mismo el que realice las instalaciones

- Se deben utilizar cortafuegos tanto de hardware como de software
- La instalación de la red LAN, debe ser hecha por especialistas
- De ser necesario, se debe contratar a una empresa especializada para que haga un test de la red. Existen aparatos especiales que pueden detectar degradaciones en los cables. Esto podría hacerse cada dos años o el tiempo que se considere necesario

- Se debe utilizar un sistema de cifrado en sus comunicaciones
- Oculte los archivos del sistema
- Si la empresa puede, se debe contratar a un administrador de red con un alto grado de competencia y experiencia. También se puede optar por contratar los servicios de una consultora de mantenimiento

- Asegúrese de que el protocolo de seguridad es correcto y que los permisos y grupos están bien creados y definidos. En una red, es recomendable que solamente una o dos personas tengan derecho “a todo”

4.4 Políticas de Respaldos

- Se deben hacer copias de seguridad y almacenarlas en lugares seguros

- Se debe verificar que los respaldos una vez generados, se hayan efectuado correctamente

- Los respaldos una vez realizados, se deben proteger contra borrados o alteraciones accidentales de la información (aplicar el seguro que cuentan los distintos medios de almacenamiento)

- Es importante establecer una frecuencia de respaldos (diario, mensual, semanal, etc), así como que haya el tiempo prudencial para la respectiva custodia

- Es importante mantener en lugar seguro y externo al sitio de trabajo, copias actualizadas de la información más importante de cada dependencia, con el fin de garantizar la oportuna recuperación de datos y programas en caso de perdidas o daños en el computador

- Cada respaldo debe contar con una copia, la cuál deberá ser guardada en un lugar estratégico, con el fin de proporcionar una custodia alterna en caso de que alguna situación especial (incendio, inundación, catástrofe natural, etc), haya destruido el lugar donde se resguardan los respaldos

- Debe mantenerse un inventario actualizado de los medios magnéticos existentes en la Cintoteca primaria y la Cintoteca alterna, indicando el estado de los mismos (nuevos, activos, para reutilizar u otros)

- Las siguientes pautas determinan una buena política de Backups aplicable en cada dependencia de la compañía.
    a. Determinar el grado de importancia de la información que amerite copias de seguridad
    b. Comunicar al departamento de informática para que este elabore copias periódicas a través de la red
    c. Indicar cuanto tiempo se debe conservar esta información

4.5 Políticas de Antivirus

- El antivirus instalado, debe ser capaz de realizar limpiezas y escaneos en estaciones de trabajo de la red, no solamente en el servidor

- El Virus por computadora puede definirse como un: “programa con capacidad de reproducir un error (infección) e insertarlo en las áreas de datos, de programas y en otras del mismo sistema y alterar su normal funcionamiento”. Ataca destruyendo la integridad de la información contenida en los medios de almacenamiento magnético llegando incluso a dañar partes físicas de la máquina

- Los componentes que más comúnmente son afectados por los virus son los siguientes:
    a. Las tablas de localización de archivos (FATS) que al modificarse ocasionan la perdida total del contenido del disco duro
    b. La asignación de discos, que al ser modificados graban la información en el volumen equivocado
    c. Programas y archivos de datos que son removidos (borrados) del disco duro o del disquete
    d. Archivos de datos a los cuales se les altera su longitud y contenido
    e. Espacios libres de almacenamiento que se ven reducidos por la duplicación de programas y/o de archivos de datos
    f. Programas del sistema operacional residentes en memoria que son eliminados o modificados

g. Sectores del disco duro o de disquete que son declarados como defectuosos
h. Partes lógicas de tarjetas inteligentes las cuales pueden verse afectadas en sus funciones preprogramadas

- Aunque existen tratamientos “vacunas”, lo primordial es prevenir el contagio mediante la adopción de una política de “sano” procesamiento que el usuario debe seguir:
    a. Utilizar únicamente software original legalmente adquirido y autorizado e instalado por el departamento de informática
    b. No instalar en la computadora software “pirata” ni de “juegos”
    c. No instalar “vacunas” sin la autorización de sistemas. Estas aunque parezca irónico, pueden estar infectadas
    d. Estar atentos a los mensajes de alerta emitidos por el computador. El departamento de informática aplicará el detector de virus periódicamente

4.6 Políticas de Mantenimiento de equipos

- Se debe brindar mantenimiento preventivo al equipo de cómputo de la oficina (UPS, Servidores, equipos de comunicación, baterías auxiliares u otros)

- Se debe contar con personal encargado de dar seguimiento al mantenimiento preventivo suministrado al equipo de cómputo, dejando evidencia del mismo

4.7 Políticas de Seguridad de la información

- La información, como recurso valioso de una organización, esta expuesta a actos tantos intencionales como accidentales de violación de su confidencialidad, alteración, borrado y copia, por lo que se hace necesario que el usuario, propietario de esa información, adopte medidas de protección contra accesos no autorizados

- Las siguientes pautas o recomendaciones, ofrecen la posibilidad de habilitar cierto grado de protección con los medios actualmente disponibles en la compañía.
  Clave de autorización de encendido
    1. Este es un recurso de protección disponible en todos los computadores, se habilita al momento de configurar el equipo y es una clave que será solicitada como primer paso de inicialización después de encendido el computador
    2. Todo computador, será entregado por el departamento de informática con este medio de protección activado, previa autorización del usuario
    3. Cuando se activa esta protección se debe tener presente las siguientes consideraciones:
        a. No olvidar la clave. Su desactivación puede gastar tiempo valioso durante el cual el computador no puede ser utilizado
        b. Esta clave deberá ser guardada en un sobre, el cuál deberá estar resguardarse en un lugar seguro al que tengan acceso solo el personal autorizado

- Se debe contar con una Bitácora manual en la cuál se registren las actividades que afectan la operación de los equipos y sistemas

- Dicha bitácora deberá ser revisada periódicamente por un encargado y dejar evidencia de esta revisión

4.8 Políticas de Contratos

- Los tramites para la compra de los equipos aprobados por el departamento de informática, así como la adecuación física de las instalaciones serán realizadas por la dependencia respectiva

- Con el fin de garantizar un correcto funcionamiento de los equipos de computación (computadores, impresoras y cualquier dispositivo anexo) se debe contar con un contrato de mantenimiento tanto preventivo como correctivo con firmas

especializada que presten de una manera rápida y efectiva este tipo de servicio o en su defecto por el departamento interno de servicios

- El departamento de informática controlará y supervisará la garantía de los equipos y dispositivos existentes en todas las dependencias y el contrato de mantenimiento de estos

- En el caso de existir un mantenimiento contratado debe cubrir, tanto en el tipo preventivo como en el correctivo, el reemplazo de piezas y/o tarjetas defectuosas y pierde validez cuando se comprueba que el usuario ha abierto el equipo o tratado de reparar por su cuenta el daño presentado

- El departamento de informática mantendrá un control de cada equipo, que contemple las revisiones efectuadas, cambios de piezas y modificaciones realizadas y las estadísticas de su rendimiento

- Se debe dar seguimiento a las condiciones establecidas en los contratos (Outsorcing, Mantenimiento u otros) por parte de los funcionarios designados para tal fin

4.9 Políticas de Control de accesos

- Se debe cambiar con frecuencia las claves de acceso, sobretodo si se es usuario privilegiado y dejar evidencia del mismo

- Se debe ocultar los archivos donde se guardan encriptadas las claves de acceso

- Si se desconfía del uso que se le puede dar al correo electrónico de la empresa, por parte de los empleados, es recomendable usar algún programa de filtro

- Los funcionarios o servicios de la oficina, deberán accesar Internet en forma segura, por medio de un Proxy y no por medio de Modems

- El uso de códigos de acceso debe ser personalizado y no compartido

- Cuando por alguna razón el usuario deba ausentarse momentáneamente de sus labores, su equipo debe quedar desactivado o bloqueado

- Debe quedar registrados los intentos de acceso fallidos o no autorizados y ser revisados por algún departamento o funcionario encargado

4.10 Principales vulnerabilidades detectadas en sistemas operativos Windows y Unix

SANS Institute, conjuntamente con el FBI y el NIPC, han actualizado el documento “Las 20 vulnerabilidades más críticas en Internet” donde explican cuáles son las vulnerabilidades en seguridad más críticas. Según indica el propio documento, estas son las habitualmente utilizadas en la mayoría de incidentes de seguridad. Por tanto, eliminarlas se convierte en un factor crítico.

Actualmente está vigente la tercera revisión del documento desarrollado conjuntamente por SANS Institute, el FBI (Policía Federal de los Estados Unidos) y el NIPC (Centro de Protección de la Infraestructura Nacional de los Estados Unidos). La primera versión salió en el año 2000, cuando SANS Institute reunió en un documento las diez vulnerabilidades de seguridad más críticas. Se entiende, dentro del concepto de estos estudios, que la criticidad viene dada por lo habitual en que las vulnerabilidades se utilizan en los ataques contra los sistemas informáticos conectados a Internet.

En octubre del 2001, se publicó la segunda versión del documento “Las 20 vulnerabilidades más críticas” desarrollado ya conjuntamente con SANS Institute y el FBI. Este documento ampliaba la base de estudio, ya que se recopilaban un gran número de vulnerabilidades específicas para los sistemas Windows y Unix

Es importante señalar que solucionar estas 20 vulnerabilidades (o las que afecten a nuestros sistemas) no es sinónimo de garantía de seguridad. Solucionar estos 20 problemas solo garantiza estar a salvo de cualquier atacante o gusano que intente aprovecharse de uno de estos problemas. Solucionar estos problemas no significa que se

debe bajar la guardia ante cualquier otra vulnerabilidad que vaya apareciendo y que pueda afectar a cualquier sistema.

La nueva edición del documento es mucho más práctica que las anteriores. No solo describe las vulnerabilidades, sino también explica cómo determinar si un sistema es vulnerable y, en caso que lo sea, las medidas de protección a tomar.

4.10.1 Principales vulnerabilidades en sistemas Windows

1) **Servicios del Internet Information Services (IIS)**

IIS tiene un gran número de vulnerabilidades que básicamente son de tres tipos:

- Error al tratar peticiones inesperadas
- Desbordamientos de memoria intermedia
- Aplicaciones de ejemplo incluidas en el IIS

2) **Microsoft Data Access Components (MDAC) – Remote Data Services**

Las versiones antiguas de los servicios de datos remotos (RDS) permiten a un usuario remoto ejecutar órdenes en el sistema infectado con privilegios de administrador.

3) **Microsoft SQL Server**

SQL Server tiene un buen número de importantes agujeros de seguridad que pueden ser utilizados para revelar información sensible, alterar el contenido de las bases de datos y comprometer los servidores de bases de datos.

4) **NETBIOS – Unprotected Windows Networking Shares**

Una configuración errónea de los recursos de red de Windows puede permitir el acceso a los archivos críticos de un sistema o bien ofrecer un mecanismo para que un atacante pueda controlar el computador de la víctima.

5) **Anonymous Logon – Null Sessions**

A través de conexiones de usuario anónimo o sin usuario, un atacante puede obtener información sobre la configuración de la máquina, los usuarios definidos y los recursos compartidos. Es el primer paso del ataque contra una máquina con Windows.

6) **LAN Manager Authentication – Weak LM Hashing**

Debido a la necesidad de ofrecer compatibilidad descendente, Windows utiliza un mecanismo de cifrado de contraseñas muy ineficiente. Una vez capturada la contraseña, utilizando la fuerza bruta (todas las combinaciones posibles) es posible descifrarla en períodos de tiempo muy cortos.

7) **General Windows Authentication – Accounts whit No Passwords or Weak Passwords**

Una de las vulnerabilidades más frecuente es la existencia de usuarios sin contraseñas (que pueden ser identificadas muy fácilmente si se permite conexiones nulas al sistema) o con contraseñas débiles.

8) **Internet Explorer**

Internet Explorer es el navegador por defecto incluido en todas las versiones de Windows. Todas las versiones publicadas hasta la fecha, sin los últimos parches publicados, tienen importantes vulnerabilidades de seguridad.

9) **Remote Registry Access**

Una configuración errónea del sistema puede permitir el acceso remoto al registro del sistema, el cuál es una base de datos jerárquica donde están definidos todos los parámetros del sistema: configuración de programas, dispositivos y usuarios.

10) **Windows Scripting Host**

Este es un componente presente en Windows 98, ME, 2000 y XP (así como en 95 y NT si se ha instalado Internet Explorer 5 o posterior) que permite la ejecución de scripts en Visual Basic.

Algunos de los últimos gusanos (como el “I love you”) utilizan este componente para su ejecución.

4.10.2 Principales vulnerabilidades en sistemas Unix

1) **Remote Procedure Calls (RPC)**

RPC permite que los programas de una computadora ejecuten procedimientos en otra computadora, enviando datos y recibiendo los resultados. No obstante, el servicio fue diseñado hace muchos años y la seguridad no era entonces un factor clave. Así, muchos procedimientos RPC se ejecutan con privilegios de root y no realizan ningún tipo de comprobación.

2) **Apache Web Server**

A pesar que Apache no tiene el mismo número de problemas de seguridad que el IIS, no es un producto invulnerable. Por tanto se debe verificar que se está usando la última versión, no únicamente del servidor Web, sino también de los diferentes módulos.

3) **Secure Shell (SSH)**

El protocolo SSH1 se ha demostrado como potencialmente vulnerable a la posibilidad de interceptar y descifrar una comunicación, por lo que no se aconseja su utilización.

Si se utiliza OpenSSH, se debe considerar que algunas bibliotecas de funciones utilizadas (como OpenSSL) tienen sus propias vulnerabilidades que pueden afectar a la seguridad de las comunicaciones.

4) **Simple Network Manager Protocol (SNMP)**

Según la versión del protocolo SNMP utilizada, los mecanismos de autenticación son extraordinariamente simples. Esto, unido a la posibilidad de modificar la configuración de los dispositivos de red, lo convierte en un importante agujero en la seguridad corporativa.

5) **File Transfer Protocol (FTP)**

El protocolo FTP transmite las contraseñas de los usuarios por la red sin ningún tipo de protección. Por otra parte, algunos de los programas servidores de FTP más utilizados en los sistemas Uníx tienen un buen número de importantes vulnerabilidades.

6) **R-Services – Trust Relantionships**

Se trata de una serie de servicios que permiten el acceso a sistemas remotos, sin necesidad de volver a autenticarse en los mismos. No obstante, cuando se diseñaron estos mecanismos, la seguridad no era un factor clave por lo que el sistema de autenticación es muy débil y fácilmente suplantable. Se desaconseja su utilización en cualquier entorno.

7) **Line Printer Daemon (LPD)**

Muchas implementaciones del servicio LPD tienen serios problemas de seguridad que permiten a un atacante remoto ejecutar código con privilegio de root.

8) **Sendmail**

Sendmail ha sido históricamente, uno de los servicios más atacados. No obstante, en los últimos dos años no se ha descubierto ningún problema especialmente grave. Por tanto es importante verificar que se esté utilizando una versión moderna.

9) **BIND/DNS**

Se han descubierto recientemente nuevas versiones de vulnerabilidades en el servicio de resolución de nombres de dominio que pueden ser utilizadas para ejecutar código en las máquinas vulnerables o bien utilizarlas como plataformas para atacar a otros sistemas. Por tanto, es importante verificar que se esté utilizando una versión moderna.

10) **General Unix Authentication – Accounts with No Passwords or Weak Passwords**

Al igual que sucede en los sistemas Windows, muchos sistemas Uníx tienen cuentas de usuario sin contraseñas o con contraseñas débiles. También la instalación por defecto de algunos programas crea cuentas de usuario con contraseñas conocidas.

4.11 Modelo de interconexión en una red LAN corporativa

Es importante que cada empresa antes de plantear un modelo de seguridad, primera se efectúe un análisis de riesgos potenciales. Este estudio le permitirá a la empresa, valorar qué es lo más crítico que se desea proteger, además de plantearse a sí mismos, cuánta importancia tiene la página Web para la institución. Puede tenerse para dar información a los clientes, o bien, para que los clientes desde su casa u oficina puedan ingresar a la página y realizar diversos tipos de transacciones monetarias.

Si se trata del segundo caso, el modelo de seguridad que adopte la institución debe ser muy seguro y efectivo, ya que se trata de transacciones en las que los saldos de las cuentas personales de los clientes se ven afectados de acuerdo con el tipo y cantidad de transacciones que el cliente realice.

El modelo de seguridad puede ser tan simple o tan complejo como se quiera. En el mercado se pueden encontrar tantas soluciones como proveedores, por lo que no se puede afirmar que una solución específica es la mejor.

Dentro de los objetivos propuestos para este trabajo, está proponer un modelo de seguridad que sea efectivo y que pueda servir de guía para cualquier empresa financiera (bancos, mutuales, puestos de bolsa, etc.) que quiera tener una página Web donde sus clientes puedan hacer transacciones. El modelo propuesto trata de abarcar los principales componentes que se deben tomar en cuenta para hacer un diseño seguro y que pueda ser complementado con políticas de seguridad efectivas.

Aunque el modelo propuesto tiene duplicación de algunos de sus dispositivos y eso podría encarecer la solución, considero importante que existan equipos redundantes ya que una posible falla de alguno de ellos, podría llegar a comprometer la seguridad de la información y la continuidad del servicio, que es precisamente lo que se quiere evitar.

Además, una solución de seguridad debe ser complementada con una serie de políticas y procedimientos como los que se expusieron anteriormente, que ayuden a reforzar la seguridad que se quiere obtener mediante la solución física del modelo de seguridad.

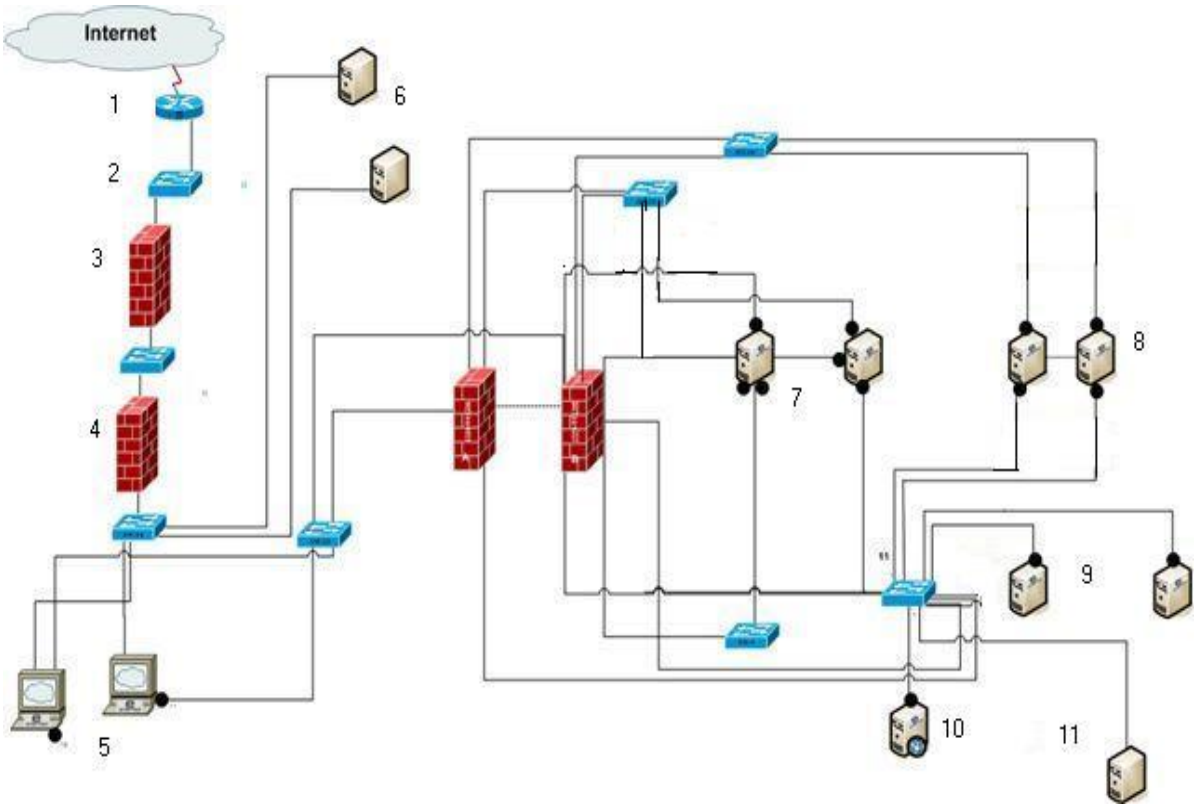


Figura 8 Red corporativa de seguridad

1) Enrutador: Es el equipo que se encarga de conectar la red corporativa de la empresa con la Internet. Su función es la de interconectar dos o más redes y reenviar paquetes de acuerdo con la información encontrada en su tabla de enrutamiento.

2) Switch: Son los dispositivos centrales en redes con topología en estrella que identifican el ordenador que va a recibir en ese momento el paquete de datos. En otras palabras, permiten la intercomunicación entre los equipos en una misma subred.

3) Firewall a nivel de hardware: También se conocen como Packet-Filtering Gateways.

Estos firewall son los más económicos. Las capacidades de filtro suelen estar presentes en el software del router, y como probablemente se va a necesitar un router para conectarse a Internet no hay ningún costo adicional.

Los network firewall operan despreciando paquetes en base a sus direcciones de origen o destino o sus puertos. En general no se detiene información de contexto, las decisiones son tomadas solo en base a la información del paquete en cuestión. En función del router, el filtrado se puede hacer a la entrada, a la salida o en ambos lados. El administrador realiza una lista de máquinas aceptables y servicios, y una lista de máquinas y servicios a denegar.

4) Firewall a nivel de software: Un firewall a nivel de software, representa el diseño opuesto en el diseño de un firewall. En vez de usar un mecanismo de propósito general para permitir diversos tipos de tráfico, puede utilizarse un código de propósito específico para cada aplicación deseada. Estos firewalls poseen además otra característica apreciada, pueden registrar (archivos .log) y controlar todo el tráfico de entrada y salida.
Estos firewalls tienen la responsabilidad de tomar los paquetes de una red y llevarlos a otra. Previamente abren el paquete, examinan el contenido y se aseguran de que no tengan ningún riesgo potencial. Una vez chequeados dichos paquetes, y son seguros, el firewall construye unos nuevos con el mismo contenido. Con esto se asegura que sólo los paquetes para los cuáles hay un código de construcción pueden atravesar el firewall. No se pueden enviar paquetes no autorizados porque no hay código para generarlos.

5) Servidor Web: Este es uno de los servidores críticos que requieren redundancia. Un servidor Web es un programa que implementa el *protocolo HTTP* (hypertext transfer protocol). Este protocolo está diseñado para transferir hipertextos, páginas Web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Sin embargo, el hecho de que HTTP y HTML estén íntimamente ligados, no debe dar lugar a confundir ambos términos. HTML es un formato de archivo y HTTP es un protocolo.

Cabe destacar el hecho de que la palabra *servidor* identifica tanto al programa como a la máquina en la que dicho programa se ejecuta. Existe, por tanto, cierta ambigüedad en el término.

Un servidor Web se encarga de mantenerse a la espera de *peticiones HTTP* llevada a cabo por un *cliente HTTP* que se conoce como *navegador* o browse. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla. El cliente es el encargado de interpretar el código HTML, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de la misma.

6) Servidor DNS: Este es uno de los servidores críticos que requieren redundancia. Un servidor DNS (Domain Name System) se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando éste está bien configurado.

7) Servidor de componentes: Este es uno de los servidores críticos que requieren redundancia, debido a que en él estarán los componentes que requiere la aplicación.

8) Servidor de Base de datos: Este es uno de los servidores críticos que requieren redundancia, ya que en estos servidores, estarán preferiblemente replicadas las bases de datos.

9) Domain controlers (controladores de dominio): Este es uno de los servidores críticos que requieren redundancia. Su principal función es la de servir de repositorio para

el Directorio Activo (Active Directory) el cuál es una base de objetos que se pueden identificar en una red.

10) Servidor de Parches: Para este tipo de servidores, no se va a contar con un servidor redundante, ya que en caso de que algún equipo de la red, necesite un parche y el servidor de parches por alguna razón esté fuera de servicio, la aplicación de parches se puede realizar en forma manual en cada equipo.

11) Servidor de Antivirus: Es un caso similar al del servidor de parches, ya que en caso de que algún servidor ocupe la actualización de la versión del antivirus, este se podría ejecutar de forma manual en cada equipo, por lo que no es necesario que tenga redundancia.

4.12 ¿Qué es el ISO 17799?

Es un estándar genérico de seguridad reconocido internacionalmente. Básicamente es un set de controles que incluye las mejores prácticas en seguridad de la información.

4.12.1 ¿Por qué es necesario el ISO 17799?

Su intención es servir como punto de referencia único para identificar los controles necesarios en la mayoría de las situaciones en que los sistemas de información se ven involucrados en la industria y el comercio. Sirve para facilitar el comercio en un entorno confiable.

Existe como BS7799 desde 1995, aunque no se popularizó su utilización debido a que fue criticado como simplista, poco flexible y debido a que había asuntos más importantes que atender, como por ejemplo el Y2K.

Sin embargo, en 1999 se publica una segunda versión revisada y empezaron a desarrollarse herramientas para facilitar su aplicación y las certificaciones empezaron de manera formal. Este paso le permitió evolucionar rápido a un ISO, o sea, un Estándar Internacional.

4.12.2 El ISO 17799 en la actualidad

Actualmente se está dando una adaptación. Muchas organizaciones han declarado su intención de certificarse o están alineando sus procesos, principalmente instituciones financieras que ya habían adoptado el BS7799 o British Standard. Se podría decir que desde los eventos del 11 de setiembre del 2001 en Nueva York, se presentó una gran reconsideración hacia la seguridad informática.

4.12.3 ¿Por qué es importante certificarse?

Sobretodo por competitividad. Surge la pregunta de ¿qué pasaría si una empresa de la competencia se certifica primero que nosotros? Sencillamente esto podría ser un diferenciador en el mercado.

Claramente se ve la necesidad de la certificación en cuestiones de e-Bussines. Pero igual de importante puede ser para una firma consultora que ejecuta auditorias o un despacho de abogados que lleva a cabo la fusión de dos empresas. Ellos tendrán que garantizar que la información de sus clientes se encuentra protegida y que no habrá fugas o pérdidas de información. Y ni hablar de instituciones financieras.

4.12.4 ¿Qué podemos hacer con respecto al ISO 17799?

1- Ignorarlo.

2- Al implementar políticas de seguridad en las empresas, tomar el ISO como una guía e intentar cubrir todos sus puntos.
3- Desarrollar todas las políticas del ISO 17799 y continuamente verificar que se cumplan.
4- Buscar la certificación completa.

4.12.5 ¿En qué consiste el ISO 17799?

El ISO17799 esta organizado en 10 secciones principales, cada una cubre áreas o tópicos diferentes.

4.12.5.1 Planeación de la continuidad del negocio

Los objetivos son: Contrarrestar las interrupciones de las actividades productivas críticas del negocio. Evitar fallas mayores o desastres.

4.12.5.2 Sistemas de Control de Acceso

Objetivos:

1.- Controlar el acceso a la información

2.- Prevenir los accesos no autorizados a sistemas de información.

3.- Garantizar la protección de servicios de red.

4.- Prevenir los accesos no autorizados a los computadores.

5.- Detectar actividades no autorizadas.

6.- Garantizar la seguridad de la información cuando se utilice equipo de cómputo móvil o remoto.

4.12.5.3 Desarrollo y Mantenimiento de Sistemas

Asegurarse que la seguridad del sistema esta construida dentro de la aplicación para prevenir perdidas, abusos, modificaciones de los datos. Debe de proteger la

confidencialidad, autenticidad e integridad de la información. Los proyectos informáticos y sus actividades de soporte deberán de ser conducidos de forma segura.

4.12.5.4 Seguridad Física y Ambiental

El objetivo de esta sección es prevenir el acceso no autorizado a las instalaciones para prevenir pérdida, robo, daño de los bienes y evitar la interrupción de las actividades productivas. Prevenir el robo de información y de los procesos de la empresa.

4.12.5.5 Cumplimiento

Objetivos

1) Evitar la infracción de cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.

2) Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.

3) Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoria del proceso.

4.12.5.6 Seguridad del personal

Objetivo: Reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse de que el personal este conciente de las amenazas a la información y sus implicaciones.

Deberán apoyar la política corporativa de seguridad en contra de accidentes y fallas. A la vez, deberán aprender de estos incidentes.

4.12.5.7 Seguridad de la organización

Los objetivos de esta sección son:

1) Administrar la seguridad de la información dentro de la compañía.

2) Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos accesados por terceros, (proveedores, clientes, etc.)

3) Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros (outsourcing)

4.12.5.8 Administración de las Operaciones y Equipo de Cómputo

Objetivos:

1- Asegurar la correcta operación de las instalaciones de procesamiento.
2- Minimizar el riesgo de fallas en el sistema.
3- Proteger la integridad del software y la información
4- Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.
5- Asegurar la protección de la información en la red y de la infraestructura que la soporta.
6- Prevenir el daño a los activos y procesos críticos del negocio.
7- Prevenir la perdida, modificación o mal uso de la información intercambiada entre empresas.

4.12.5.9 Clasificación y Control de Activos

Los objetivos son mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

4.12.5.10 Políticas de Seguridad

Objetivo: Proveer la directriz y el soporte de la Dirección General de la empresa para la seguridad de la información.

4.12.6 Conclusión

Alinearse con la ISO17799 no es una tarea fácil, incluso para las organizaciones con más conciencia en la seguridad.

Por eso, se recomienda que la ISO17799 sea implementada bajo un esquema "paso a paso". El mejor punto de partida es realizar un análisis de la posición y situación de la organización, seguido de una identificación de los cambios necesarios para alinearse con

la ISO17799. A partir de este punto, el proceso de planear e implementar deben ser emprendidos metódicamente y abierta al cambio.

Figura 9 Certificaciones BS7799

4.13 Infraestructura de llave pública (PKI)

Anteriormente, se había hecho la propuesta de la interconexión física que debería tener un modelo de seguridad. Este modelo brinda seguridad a los equipos que forman parte de la red y a sus respectivas aplicaciones o funciones. Ahora bien, los clientes también necesitan contar con la seguridad de que su información personal no está siendo interceptada, modificada o destruida. Para esto, las instituciones financieras deben contar con una infraestructura de llave pública o PKI (Public Key Infrastructure) que le permita brindar esa seguridad a sus clientes.

De un modo sencillo, se puede decir que una infraestructura de llave pública es el conjunto de componentes y políticas necesarias para crear, gestionar y revocar certificados digitales que pueden ser utilizados para autenticar cualquier aplicación, persona, proceso u organización de una red de empresa, extranet o Internet.

La idea básica de una infraestructura de llave pública es que los datos sensibles sean protegidos mediante técnicas de encriptación. Cada dispositivo de usuario final posee software de encriptación y dos llaves; una pública para distribuirla a otros usuarios, y otra privada, guardada y protegida por su propietario. El usuario encripta un mensaje utilizando la llave pública del receptor; cuando el mensaje se recibe, el destinatario lo desencripta con su llave privada.

Se pueden tener múltiples pares de llaves para mantener comunicaciones distintas con grupos diferentes. Pero, dado el elevado número de llaves que intervienen en las comunicaciones, resulta crucial contar con algún método para administrarlas y controlar su utilización. Aquí es donde una PKI entra en juego, permitiendo la creación, distribución, seguimiento y revocación centralizada de llaves.

4.13.1 Componentes de una PKI

Una infraestructura de llave pública consiste en la interrelación de objetos, aplicaciones y servicios. Estos conceptos trabajan de manera conjunta para distribuir y validar certificados. Un modelo de PKI incluye los siguientes componentes:

- **Herramientas de administración de Certificados y Autoridad Certificadora:** Provee herramientas tanto para interfase gráfica para el usuario como de línea de comando para administrar certificados emitidos, publicar autoridades certificadoras y CRLs (Certificate Revoke List), configurar autoridades certificadoras (CAs), importar y exportar certificados y llaves y recuperar llaves privadas archivadas
- **Autoridades certificadoras (CAs):** Emite certificados a usuarios, computadoras y servicios y administra certificados. Cada certificado que un CA emite es firmado con el certificado digital de ese CA.
- **Puntos de distribución de certificados y CRL:** Publica el sitio donde los certificados y CRLs son publicados, dentro o fuera de una organización. Los publicadores pueden usar cualquier tipo de servicio de directorio, incluyendo X.500, Lightweight Directory Access Protocol (LDAP) o directorios en un sistema operativo específico.

- **Plantillas de certificados:** Define el contenido y propósito de un certificado digital. Una plantilla de certificados define los requerimientos de emisión, propósito del certificado, extensiones implementadas tales como políticas de aplicación o uso de llave extendida y permisos de matrícula para los certificados que una CA emite.
- **Certificados digitales:** Provee la fundación de un PKI. Los certificados digitales son credenciales electrónicas que están asociadas con una llave pública y una llave privada que una organización utiliza para autenticar usuarios.
- **Listas de revocación de certificados (CRL):** Despliega la lista de certificados que un CA ha revocado antes que el certificado llegue a su fecha de expiración.
- **Aplicaciones y servicios de llave pública habilitada:** Soporta encripción de llave pública. Se puede implementar una vez que se haya configurado la PKI para emitir, publicar y controlar certificados.

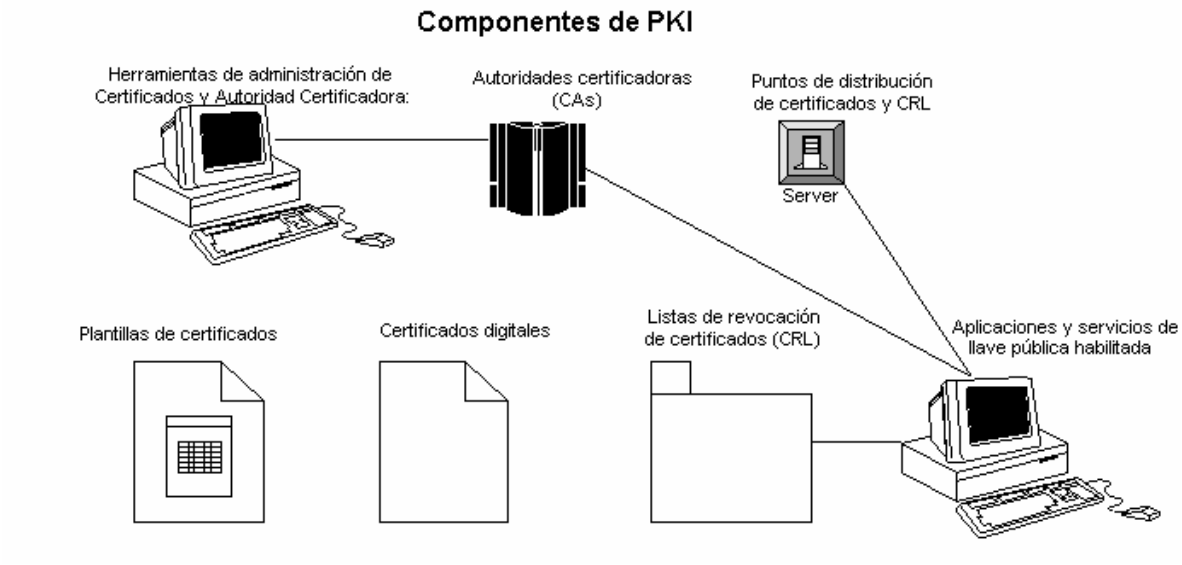


Figura 10. Componentes de PKI

4.13.2 Encripción de llaves

La encripción involucra tanto encripción simétrica como asimétrica de datos en un formato encriptado y el proceso de desencripción debe devolver el formato original de los datos.

Se usa en cada una la misma llave o se puede usar dos llaves diferentes para los procesos de encripción y desencripción.

4.13.2.1 Tipos de llaves

- Llave simétrica: La misma llave es usada tanto para encripción como desencripción. Cuando se encriptan los datos la persona o proceso que envía usa la llave simétrica para asegurarse que personas o procesos no autorizados no puedan inspeccionar los datos originales. La persona o proceso utiliza la misma llave simétrica para desencriptar los datos.

- **Llave asimétrica:** Este tipo de llave es una combinación de dos llaves relacionadas matemáticamente; una llave pública y una privada, las cuales a menudo son referidas como un par de llaves. Ambas llaves son usadas para encriptar y desencriptar datos.

    - Si la llave pública encripta los datos, la llave privada asociada desencripta los datos
    - Si la llave privada encripta los datos, la llave pública asociada desencripta los datos

La llave privada nunca debe ser expuesta a los usuarios en una red. Debe ser protegida en un perfil de usuario o computadora o en un dispositivo físico, tal como un smart card.

La llave pública, la cuál es un atributo del certificado digital, es ampliamente distribuida en localidades tales como el Active Directory ®, directorio de servicio que asegure que otros usuarios puedan obtener la llave pública para encripción y firma digital de datos.

4.13.2.2 ¿Cómo trabaja la encripción simétrica?

La encripción simétrica usa la misma llave para encriptar y desencriptar. Por su velocidad, se usa típicamente la encripción simétrica para encriptar grandes cantidades de datos. La encripción simétrica es también conocida como *encripción gruesa*.

Cuando se usa la encripción simétrica, el emisor de los datos originales, encripta los datos usando la llave simétrica. El resultado es un texto cifrado el cual es transmitido al receptor.
Cuando el receptor ya ha recibido el texto cifrado, desencripta los datos con la misma llave simétrica para obtener el dato original.

4.13.2.3 ¿Cómo trabaja la encripción de llave pública?

Cuando se implementa la encripción de llave pública, el par de llaves del receptor protege los datos originales de inspección encriptando los datos originales durante la transmisión.

Los pasos siguientes explican el proceso de cómo la encripción de llave pública es aplicada al texto de datos original:

1. El remitente recupera la llave pública del receptor. En un ambiente de Active Directory, el remitente recupera la llave pública recuperando el certificado de Active Directory del receptor y después recupera la llave pública del certificado.
2. El remitente genera una llave simétrica y usa esta llave para encriptar los datos originales.
3. La llave simétrica es encriptada con la llave pública del receptor para evitar que la llave simétrica sea interceptada durante la transmisión.
4. La llave simétrica encriptada y los datos encriptados son enviados al receptor.
5. El receptor usa su llave privada para desencriptar la llave simétrica encriptada.
6. Los datos encriptados son desencriptados con la llave simétrica, dando como resultado que el receptor obtenga el dato original.

4.13.3 ¿Qué es un certificado digital?

Un certificado digital provee información sobre el sujeto del certificado, la validez del certificado y cuales aplicaciones y servicios puede usar el certificado. Un certificado digital también brinda una manera de identificar el receptor del certificado. Los certificados usan técnicas de criptografía para solventar el problema de la falta de contacto físico entre las dos entidades que llevan a cabo una transacción. Una organización en lugar de identificar

el receptor del certificado “cara a cara”, una aplicación o servicio verifica cada receptor de certificado validando el certificado de cada receptor presente.

Es difícil para un usuario o computadora hacerse pasar por alguien más, porque los certificados son firmados digitalmente por la autoridad certificadora (CA) que entrega el certificado. Un atacante no puede modificar un certificado sin el conocimiento de la autoridad certificadora. Un atacante no puede asumir la identidad del usuario o computadora que está listada en el sujeto del certificado sin tener acceso a la llave privada que está asociada con el certificado.

Un certificado digital contiene lo siguiente:

- La llave pública criptográfica del certificado del sujeto
- Información sobre el sujeto que solicitó el certificado
- Información sobre la autoridad certificadora que emitió el certificado

Antes de que un CA emita un certificado, el CA verifica la identidad del solicitante. Esta verificación puede incluir un chequeo manual en segundo plano del solicitante o un examen del *Discretionary Access Control List* (DACL) de la plantilla del certificado del solicitante para asegurar que el usuario solicitante o computadora tiene los permisos requeridos para matricular el certificado solicitado.

Tomando como ejemplo una página Web de un banco estatal de Costa Rica, se podrían obtener las siguientes ilustraciones sobre lo referente a la conexión vía Web de un cliente contra el respectivo Banco.

1- Se accesa a la página Web digitando la respectiva dirección:

Figura 11. Presentación de una página WEB

2- Si se desea conocer más información sobre la empresa que brinda el servicio de seguridad a la entidad financiera se le debe dar doble clic en el ícono de la empresa que brinda el servicio de certificados digitales, en donde nos debe aparecer la siguiente información:

- la Autoridad Certificadora que emite el certificado digital
- el URL o nombre del sitio que nos brindará los servicios financieros
- el estado de la certificación
- el período de validez del certificado
- el nombre de la compañía u organización a la que se le emitió el certificado

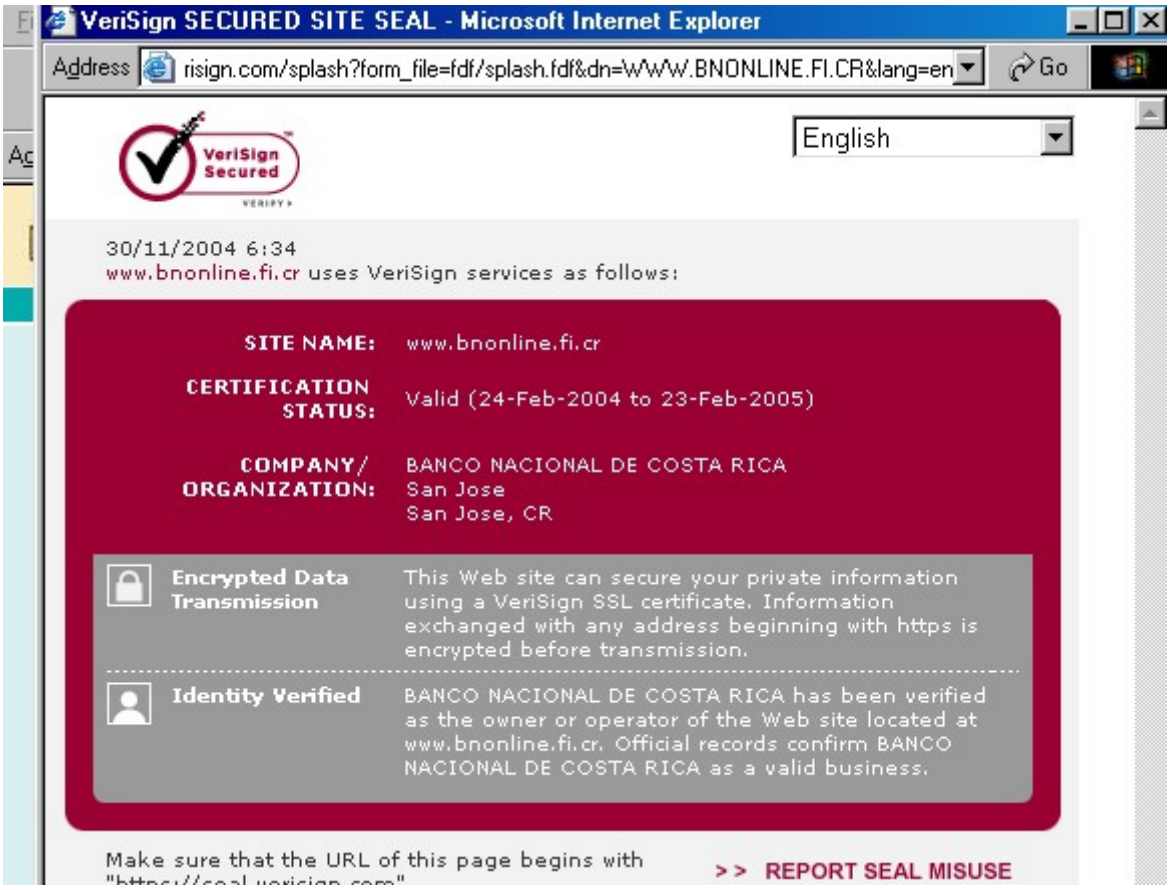


Figura 12. Información de la empresa que brinda el servicio de seguridad

3- Posteriormente podemos retornar a la pantalla donde podremos ingresar nuestra información y clave personal para ingresar a la página de servicios tal como se presenta a continuación.

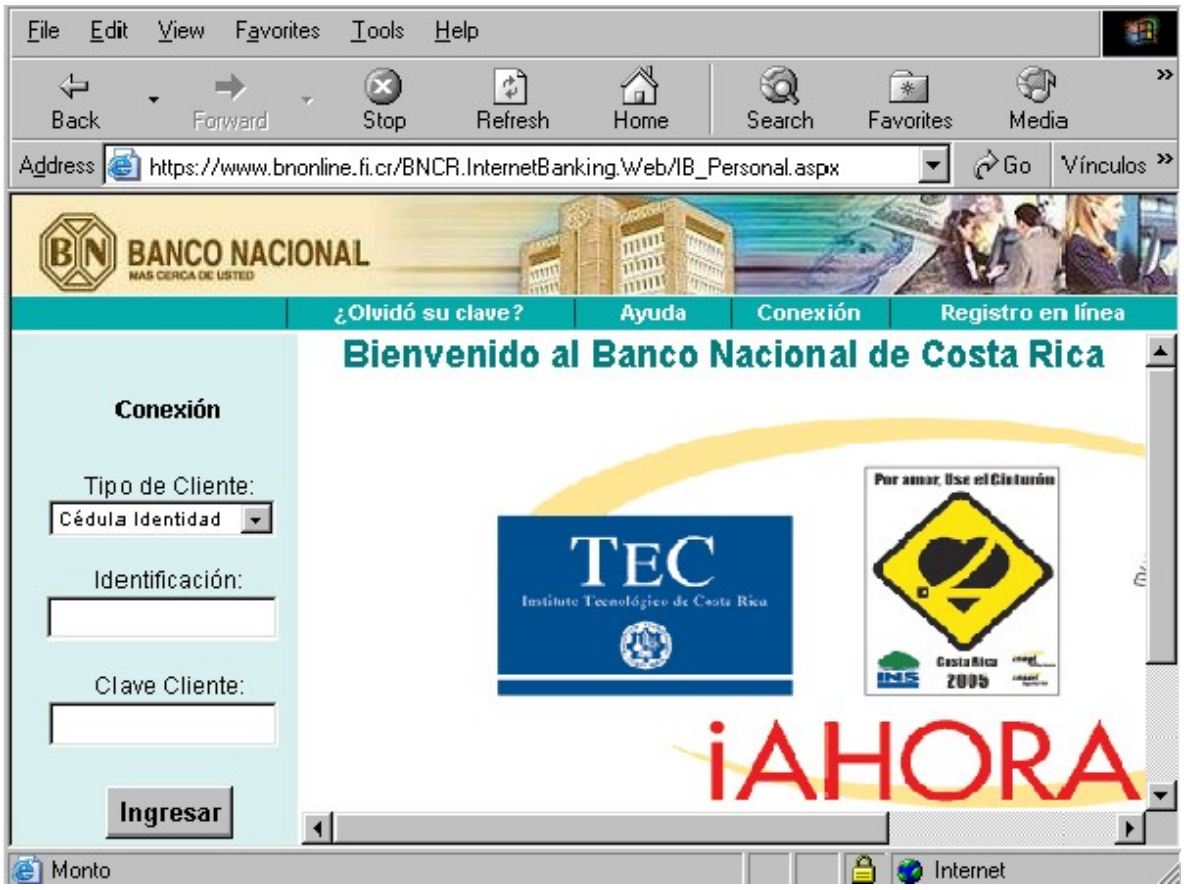


Figura 13. Presentación de la página WEB para servicios en línea

4- Antes de ingresar la información de nuestra identificación y clave, es muy importante que se verifique la verdadera identidad de la empresa, ya que se podría estar accesando a una página Web alterada. Esto se hace dando doble clic sobre el ícono del candado que generalmente aparece en la parte inferior de la pantalla. Es importante señalar que el ícono o imagen del candado se puede falsificar, pero no así la emisión del certificado digital de la empresa que nos provee el servicio de banca por Internet. Al dar doble clic sobre el candado debe aparecernos la siguiente información:

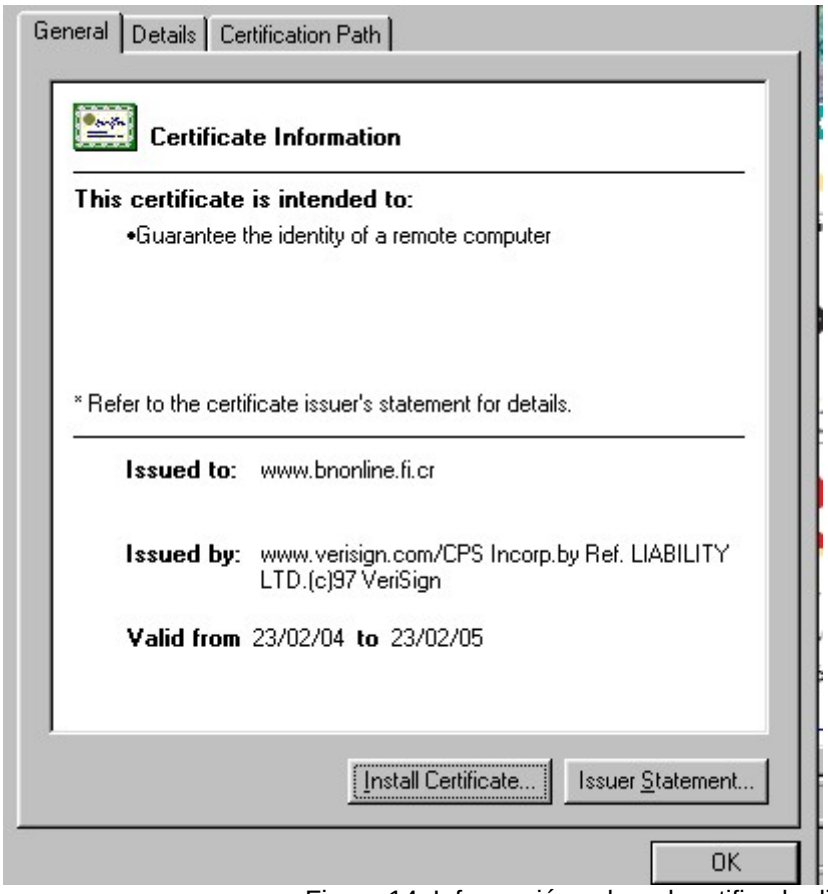


Figura 14. Información sobre el certificado digital

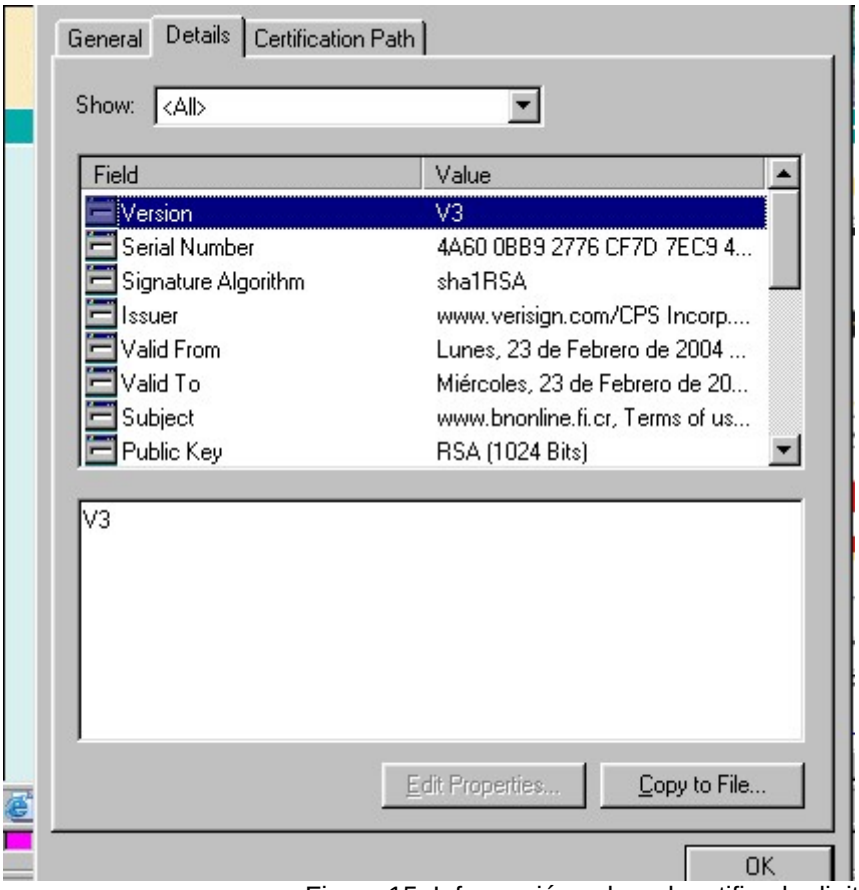


Figura 15. Información sobre el certificado digital

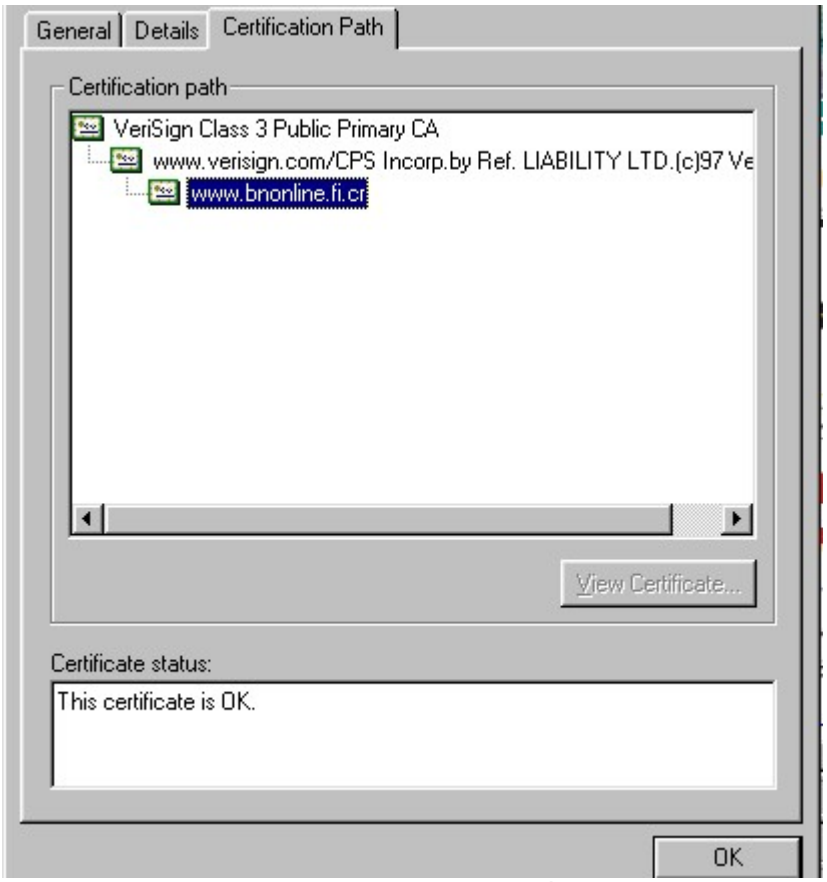


Figura 16. Información sobre el certificado digital

CAPÍTULO 5 RESULTADOS

5.1 Conclusiones

Después de realizado este trabajo, es importante indicar que para una institución financiera, de cuyas ganancias depende mucho la prestación de bienes y servicios, es casi una obligación evolucionar paralelamente con las nuevas tendencias tecnológicas respecto de la materia de seguridad informática. Incidentes lamentables como los atentados del 11 de setiembre del 2001 en Estados Unidos y los efectos tan negativos debido a los ataques de virus, gusanos y troyanos, han hecho conciencia en las personas para que se tomen la seguridad de la información como una prioridad.

Actualmente, el uso de páginas Web para realizar transacciones financieras desde la casa u oficina es una tendencia que cada día crece gracias a la necesidad de las instituciones financieras de bajar costos administrativos y operativos; además de ser una buena publicidad y propaganda de los beneficios que el cliente podría recibir al utilizarlas.

Como consecuencia de lo anterior, las entidades financieras deben hacer una mayor inversión para garantizarles a sus clientes dos variables muy importantes, la seguridad de los datos y el mejor tiempo de respuesta y eficacia de los sistemas, siguiendo los estándares internacionales que existen en la actualidad.

Cada institución financiera debe ser consciente de que, por la naturaleza de su existencia, son uno de los blancos preferidos de un atacante, tanto externa como internamente, por lo que debe contar con una adecuada plataforma tecnológica, procedimientos y políticas de seguridad efectivas, que pueda hacerle frente a un eventual ataque. Además, se debe tomar en cuenta que el problema de virus, gusanos y troyanos, es un problema mundial y se le debe combatir de la mejor manera posible.

Para que una institución financiera pueda ofrecer a sus clientes un sistema confiable, debe tener definidas políticas de seguridad, claras de entender y consistentes en su acción. Esto implica tener equipos y programas de seguridad instalados, darles el uso adecuado a los mismos, revisar en forma permanente los archivos de eventos y alarmas, y mantenerse al día en todo lo relacionado con los problemas de seguridad que se vayan descubriendo, y responder de acuerdo con las necesidades.

Un gran beneficio para las entidades financieras de contar con un sistema de seguridad confiable, es que le permite fortalecer su imagen, dando como resultado la tranquilidad a sus clientes de que la institución es segura para invertir su dinero.

Un entidad financiera que no cuente con los elementos de seguridad de datos, probablemente tenga costos menores de operación e inversiones; pero las consecuencias de ser víctimas de pérdidas de dinero, producto de fallas en sus sistemas de seguridad o peor aún, por falta de ellos, se puede traducir simplemente a una percepción tal de desconfianza por parte del mercado, que lo obligue a cerrar sus puertas.

Es importante indicar que un riesgo no se elimina, sólo se minimiza; por lo que hay que ser conscientes de que no se puede bajar la guardia en cuanto a la seguridad de la información.

5.2 Recomendaciones

La inversión que implica una plataforma de seguridad confiable para proteger los datos de los clientes, es inferior al costo que generaría para una institución no invertir en seguridad informática; ya que el proceso de corregir e implementar la seguridad después de un ataque, podría resultar mucho más caro, si se toman en cuenta los clientes que perdería la institución.

Considero que todas las empresas financieras deben contar con un mecanismo de gestión de vulnerabilidades, de los existentes en el mercado, que les permita la identificación de vulnerabilidades, la reparación con parches y el análisis de la configuración de la solución de seguridad que se administra.

La falta de información y el desconocimiento son el principal inconveniente cuando se debe planear la seguridad en un sistema informático. Es por eso que considero que en las universidades de Costa Rica, se hacen necesarias dos o tres materias dedicadas a ver temas importantes sobre seguridad informática y leyes contra el delito informático, que sirvan de apoyo y refuerzo a la materia de Auditoría en Sistemas. Estas materias también deben tener como objetivo establecer un perfil de conocimientos para que el futuro

profesional en informática, pueda cotizarse en el campo laboral, tanto como lo puede hacer en Análisis y Diseño de Sistemas, Sistemas Operativos, Telecomunicaciones, Bases de datos, etc. También podría ser un nuevo énfasis para optar por un postgrado. Esto le permitiría a las empresas contratar a profesionales con conocimientos en seguridad informática, es decir, un personal más capacitado y con una visión actualizada sobre la diversidad de aspectos que podrían comprometer uno de los activos más importantes de la empresa, el cuál es la información.

Además es importante que la empresa se guíe bajo los estándares de la norma de seguridad ISO-17799, los cuáles le ayudarán a identificar los mejores controles aplicables para la seguridad informática de la institución. Además, certificarse en esta norma puede convertirse en un punto a favor para atraer la mayor cantidad de clientes posible, tomando en cuenta que la empresa aparte de ofrecerle al público servicios financieros, también le debe ofrecer seguridad para sus inversiones.

Otra recomendación es que la empresa debe contar con un proveedor de servicios de certificados digitales, esto con el fin de que el cliente pueda tener seguridad de que está entrando a un sitio seguro, verificando que la página donde va a ingresar su clave y contraseña para hacer alguna transacción o consulta, sea realmente la de la institución.

Glosario

Ancho de banda: cantidad de datos que se pueden transmitir en determinado periodo de tiempo por un canal de transmisión; así considerado, el ancho de banda se expresa en bits por segundo (bps). Por ejemplo, un módem de 56 Kbps es capaz, en teoría, de enviar alrededor de 56.000 bits de datos por segundo, mientras que una conexión de red Ethernet con un ancho de banda de 100 Mbps (cien millones de bits por segundo), puede enviar casi 1.800 veces más datos en el mismo periodo de tiempo.

Bit: acrónimo de Binary Digit (dígito binario), que adquiere el valor 1 o 0 en el sistema numérico binario. En el procesamiento y almacenamiento informático un bit es la unidad de información más pequeña manipulada por el ordenador, y está representada físicamente por un elemento como un único pulso enviado a través de un circuito, o bien como un pequeño punto en un disco magnético capaz de almacenar un 0 o un 1. La representación de información se logra mediante la agrupación de bits para lograr un conjunto de valores mayor que permite manejar mayor información. Por ejemplo, la agrupación de ocho bits compone un byte que se utiliza para representar todo tipo de información, incluyendo las letras del alfabeto y los dígitos del 0 al 9

Bug: Se le denomina a errores de programación.

Cracker: usuario y programador informático que tiene amplios conocimientos y crea código malicioso capaz de romper los sistemas de seguridad, para acceder a otros ordenadores o computadoras y así poder recabar o destruir información. En ocasiones se utiliza como sinónimo de hacker, aunque este último tiene como finalidad su propia satisfacción o vencer retos tecnológicos, sin ánimo de realizar daño u obtener información de forma ilegal.

Una actividad especialmente dañina es el logro de la caída de los servidores de red, como los servidores de Internet, mediante lo que se ha dado en llamar ataques DoS (Denial of Service, ‘denegación de servicio’), cuya metodología es saturar su capacidad de procesamiento, mediante peticiones de servicio masivas, de manera que se bloquee todo el sistema y no admita peticiones de otros usuarios.

Otras actividades típicas de un cracker son la obtención de datos confidenciales, como números de tarjetas de crédito, la destrucción de bases de datos de los servidores o las interferencias en la mensajería electrónica.

E-Bussines: modo de gestionar empresas y realizar transacciones comerciales en red, fundamentalmente a través de Internet. En inglés se designa con los términos e-commerce, e-business o I-commerce. Existen empresas que operan exclusivamente a través de Internet, otras que tienen en la red una sección complementaria de su comercio tradicional y otras que utilizan Internet sólo para determinadas actuaciones, como las publicitarias, que dan a conocer la empresa o sus productos.

Aunque las tarjetas de crédito permiten transacciones electrónicas desde la segunda mitad del siglo XX, el auge del comercio electrónico se produjo a la par que la implantación de Internet. Importantes compañías de software han desarrollado aplicaciones para gestionar las tiendas virtuales donde se realizan estas operaciones comerciales. Estas aplicaciones deben permitir el mantenimiento de un catálogo, la elección de productos, un sistema seguro de pagos y, si es posible, elaborar perfiles de clientes. Todo ello con las adecuadas garantías de protección de la información sensible que manejan, para evitar que sea accesible a personas o entidades ajenas.

Exploits: programas utilizados para aprovechar fallos o errores de programación con el fin de atacar al sistema

Hacker: Originalmente fue un término utilizado para referirse a un aficionado a los ordenadores o computadoras, totalmente cautivado por la programación y la tecnología informática. En la década de los 80s, con la llegada de los computadores personales, y posteriormente con la posibilidad de conexión a los grandes sistemas de ordenadores a través de Internet, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar, alterar o eliminar los programas o los datos almacenados en las mismas, aunque a eso es a lo que dedican su atención los denominados crackers. También se utiliza para referirse a alguien que, además de programar, disfruta desensamblando

sistemas operativos y programas para entender su lógica de funcionamiento, para lo que utiliza programas que desensamblan el código y realizan operaciones de ingeniería inversa.

Hardware: Es la parte física, tanto interna como externa de un Computador. La selección del modelo y capacidades del hardware requerido por determinada dependencia, debe ir de acuerdo con el plan estratégico de sistemas y sustentado por un estudio elaborado por el departamento de informática, en el cual se enfatizan las características y volumen de información que ameritan sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias.

Host: Computadora de usuario final conectada a una red. En una interred, todas las computadoras se clasifican como hosts o enrutadores.

Internet: Red de carácter planetario que permite a un ordenador particular conectarse directamente a cualquier otro ordenador que también esté conectado a esta red.

IP: Internet Protocol

Mbps: Mega Bits por segundo, lo cuál representa una velocidad de transmisión.

Paquete: Fragmento de datos pequeño y autocontenido enviado por una red de cómputo. Cada paquete contiene una cabecera que identifica al transmisor y al receptor, así como los datos a entregar.

Ping: Protocolo de alto nivel que permite comprobar si los paquetes TCP/IP llegan a otro ordenador y el camino que siguen.

Sniffer: Sinónimo de monitor de red.

Software: En términos generales se puede definir que el Software es un conjunto de programas para llevar a cabo un objetivo específico y a su vez un programa es un

conjunto de instrucciones que realizan una tarea para cumplir dicho objetivo. El software para Computadores se puede clasificar en los siguientes tipos:

- Sistema operacional: Es el conjunto de programas que controla las actividades operativas de cada Computadora y de la Red.
- Paquete de Usuario Final: Mediante los cuales el usuario de un manera sencilla elabora sus procesos, por ejemplo, hojas de calculo, manejadores de bases de datos, procesadores de palabras, etc.
- Paquete de Sistemas Aplicativos: En los que a diferencia de los anteriores, el usuario es simplemente quien los usa. La programación y el desarrollo es compleja, realizada por el Departamento de informática o adquiridos a proveedores externos, por ejemplo, sistema de nomina, sistema de Contabilidad, sistemas de Inventarios, etc.

TCP: Transport Control Protocol

Bibliografía

Páginas de Internet consultadas:

www.sans.org/top20

www.cisco.com/go/security

www.cisco.com/securitypartners

www.cert.org/archive/pdf/attack_trends.pdf

www.carsoft.com.ar/Firewall.htm

http://www.networkassociates.com/us/about/press/sniffer_technologies/2003/20030904_083302.htm

http://www.networkassociates.com/us/about/press/sniffer_technologies/2003/20030501_152511.htm

http://www.networkassociates.com/us/about/events/seminars/mcafee/20031016_100817.htm

http://www.networkassociates.com/us/about/events/seminars/mcafee/20031017_100331.htm

http://seguridad.internautas.org/artesp.php

http://idg.es/comunicaciones

http://hispasec.com

http://www.virustotal.com

http://www.seguridadcorporativa.org

http://www.criptored.upm.es/paginas/docencia.htm

http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm

http://www1.7a69ezine.org/

http://www.marianistas.org/comunidad_64.htm

http://www.lawebdelprogramador.com/results.php?page=2&keyword=Seguridad%20Informatica

http://www.symantec.com/region/mx/enterprisesecurity/content/security_articles.html

http://www.symantec.com/region/mx/enterprisesecurity/content/risks/LAM_1398.html

http://www.cisco.com/global/LA/LATAM/sne/bancos.shtml

http://www.hispasec.com/unaaldiacom.asp

Bibliografía consultada:

Villalón Huerta, Antonio. Seguridad en Unix y Redes, 2002

De Marcelo Rodao, Jesús. Piratas cibernéticos. Grupo Editor Alfaomega, 2002

Enciclopedia Didáctica de Computación. Editorial Océano, 2002

Charles P. Fleeger. Security in computing. Prentice Hall, 1997.

Donn P. Baker. Computer Security Management. Prentice Hall, 1981

Tomas Olovsson. A structured approach to computer security. Technical Report 122, Chalmers University of Technology, 1992

Tanenbaum, Andrew S. Redes de Computadoras. Prentice-Hall 1997.

Hernández Sampieri Roberto, Fernández Collado Carlos, Baptista Lucio Pilar. Metodología de la Investigación (Segunda Edición). McGraw-Hill, 1998

Manual de configuración de Cisco PIX Firewall, elaborado por la empresa Unisys 2003

Charlas asistidas:

“Seguridad Informática”. Impartida en la ULACIT el 14 de Noviembre del 2003, válida por un sello verde.

“Día mundial de la Seguridad Informática”. Impartida en al Banco Nacional de Costa Rica el día 28 de Noviembre del 2003.

“Segundo Foro Internacional sobre Seguridad Informática”. Impartida en el hotel Radisson organizado por Microsoft de Costa Rica, el día 25 de Noviembre de 2004.

Software consultado:

Enciclopedia Microsoft Encarta 2004

Curso CCNA, certificación de la empresa Cisco.

Anexos

Índice