UNIVERSIDAD AMERICANA DE ACAPULCO

FACULTAD DE INGENIERÍA EN COMPUTACIÓN

INCORPORADA A LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
Clave: 8852-16

SEGURIDAD EN LA GESTIÓN REMOTA DE SERVIDORES

TESIS

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A :
ALFREDO NICOLÁS ESCALANTE REYES

DIRECTOR DE TESIS:

ING. JOSÉ MARIO MARTÍNEZ CASTRO

ACAPULCO GRO. **MAYO 2010**

ÍNDICE

A mis padres que sin su guía y cuidados no sería quien soy el día de hoy, Katia por ofrecerme su apoyo y amor incondicional y correspondido en los momentos de flaqueza, mi hermana Daniela por el simple hecho de ser la mejor hermana del mundo. Gracias abuelito Trinidad por ofrecerme tu ejemplo desde que tengo uso de razón y por seguir ofreciéndome un ejemplo a seguir. Muchas gracias a todos aquellos que me han jalado las orejas cuando tuvieron que hacerlo, de verdad, no sé qué haría sin ustedes.

1. Introducción

A lo largo de la historia siempre ha habido necesidad de ocultar cierta información para que no pueda ser accesible para cualquier persona.

Aunque hoy en día las cosas siguen siendo básicamente las mismas, conforme fue pasando el tiempo, la información y su contenido han cambiado en forma, por lo que los métodos de ocultación fueron evolucionando a la par de los mismos, adaptándose a la era informática contemporánea.

En la actualidad la manera de almacenamiento y procesamiento de información por excelencia son las computadoras; y son las mismas computadoras las que representan el mayor desafío para la protección y/o resguardo de la información que contienen.

Como se verá más adelante, la información consta de 4 principios básicos:

- ✓ Confidencialidad.
- ✓ Autenticidad.
- ✓ Integridad.
- ✓ Disponibilidad

Así mismo existen características y herramientas que ayudarán a garantizar un nivel de seguridad óptimo, como pueden ser el control de acceso, no repudiación de la información y criptografía.

En este trabajo de redacción se procura dar una idea un tanto general y especifica al mismo tiempo, la cual pueda ayudar al lector a ubicar las zonas débiles en cuanto a seguridad y también poder garantizar un nivel óptimo de seguridad para el cumplimiento de las funciones de sus sistemas.

Con base en la experiencia personal y laboral, en la utilización de equipos caseros Ubuntu Linux/Debian, en la operación de varios tipos de servidores (Solaris, entre otros), administración de redes, así como algunos servicios de clúster para redundancia, se explican las fortalezas y debilidades más comunes en las empresas actuales, así como se planten recomendaciones para el mejor ejercicio de la seguridad en las comunicaciones remotas para la gestión y administración de servicios informáticos.

Actualmente el autor del presente documento desarrolla actividades laborales en la empresa Radiomóvil DIPSA S.A. de C.V., la cual maneja en México la marca TELCEL, realizando funciones como analista de operación, mantenimiento y soporte en el centro de operaciones de red donde las funciones principales son el monitoreo y gestión de equipos,

así como soporte técnico para las plataformas y algunos casos de usuarios, todo esto de manera remota.

Las funciones generales son operar y mantener la infraestructura de red de la empresa, y dentro de estas funciones se desprenden algunas otras como la ejecución de modificaciones o mejoras en la infraestructura, coordinación de personal vía telefónica para resolver problemas físicos en los equipos, resolución de algunos problemas de usuarios, soporte a problemas con los servidores, servicio técnico de última línea para usuarios, entre otras.

1.1 Alcances

El enfoque de seguridad que se plantea se basa en la experiencia en el campo, combinándola con el Diplomado en Seguridad de la Información impartido por la UNAM en el CEM Polanco de la Ciudad de México.

El marco teórico que se presenta es un esquema general, y no da una explicación detallada de cada tema, sino una referencia para marcar las pautas de cada tema y sus inclinaciones particulares.

En general, el alcance de este trabajo es elaborar un documento que sirva como referencia para estructurar y dar forma al objetivo, es decir, no es un documento didáctico para niveles básicos ni intermedios de conocimientos en el tema, sino una guía avanzada para la gestión segura de sistemas informáticos.

1.2 Objetivos

Los objetivos principales que se quieren transmitir en el presente documento son:

Dar un marco de referencia para cualquier ingeniero, gerente de una empresa, administrador de red, técnico o persona en general con conocimientos avanzados de computación, que necesite mejorar y/u optimizar la seguridad en su red informática para una gestión más segura de sus sistemas, todo esto con el fin de lograrlo de la manera más imparcial y menos comercial posible.

Definir pros y contras de las aplicaciones más populares en el mercado profesional, planteando sus fortalezas y debilidades generales.

Ilustrar al lector acerca de las normas internacionales en seguridad informática para su mejor comprensión e implementación.

1.3 Hipótesis

Es posible implementar un esquema robusto y eficiente de seguridad informática en cualquier empresa, de forma independiente al tamaño de la infraestructura de tecnologías de la información con que se cuente.

1.4 Justificación

En las pequeñas y medianas empresas predomina una falta de estandarización en las áreas de TI en lo que respecta a la seguridad informática. Es necesario proponer un documento el cual ayude y

facilite el conocimiento a los responsables de estas áreas en cualquier empresa y con un nivel variado de especialización en el terreno de las tecnologías informáticas.

2. Marco Teórico

Entiéndase que en el presente documento no se plasma una bibliografía completa o básica, sino que se hace referencia a todas aquellas herramientas o disciplinas que sirven para el entendimiento rápido de los temas en cuestión, por lo que si el lector no posee al menos los conocimientos mínimos requeridos para la comprensión de esta redacción, es necesario que se referencie de otros trabajos más especializados en la didáctica antes de proceder.

2.1 Redes y protocolos

Como pieza principal en la comprensión de las telecomunicaciones y la seguridad inmersa, se debe entender todo lo que existe detrás, es decir, toda la teoría detrás de la implementación de la comunicación entre computadoras.

Las redes y los protocolos de comunicación, son las bases que hacen posible la comunicación entre equipos de cómputo, puesto que ponen orden en las transacciones de datos a través del medio físico en el que se encuentren.

2.1.1 ¿Qué es una red?

No debe enfocarse en los fundamentos de las comunicaciones entre computadoras, sin embargo, es imperativo comprender su lenguaje y sus componentes.

Una red, por definición, es la unión de elementos con el propósito de compartir información según la (Real Academia de la Lengua Española, 2001).

Una red informática es el conjunto de computadoras u ordenadores dispuestos de tal manera que permitan el intercambio de información entre ellos. Para lograr esto puede haber comunicación únicamente entre dos computadoras (conexión punto a punto), la cual ofrece todo el ancho de banda de una red para la comunicación entre estos dos

equipos, o también se pueden tener muchas computadoras conectadas entre sí, sin embargo, para lograr esta coordinación es necesaria la utilización de equipos intermedios.

Este trabajo se enfocará en las comunicaciones de red basadas en el protocolo TCP/IP, aunque se definirán también otros protocolos.

2.1.2 Modelo OSI

Existe un modelo de estudio y análisis para todas las redes llamado el **Modelo OSI** (Open System Interconnection, Sistema Abierto de Interconectividad). Este modelo fue desarrollado por la Organización Internacional de Estandarización a principios de los 80's, y fue lanzado en 1984. Este dispone ser un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones (CISCO SYSTEMS, 1999).

La propuesta de este modelo es dividir las redes en 7 capas, niveles o jerarquías, las cuales permiten entender mejor el funcionamiento de la red, así como facilitar la resolución de problemas.

La manera de interpretarlo es comenzando de las capas más bajas, y terminando con las capas de más alto nivel.

2.1.3 Protocolo TCP/IP

Aunque en realidad son dos protocolos, lo más usual es referirse a él como uno solo. TCP (Transfer Control Protocol – Protocolo de Control de Transferencia), e IP (Internet Protocol – Protocolo de Internet), fueron desarrollados como parte de la familia de protocolos de Internet, por la Agencia de Investigación de Proyectos Avanzados de Defensa, en EUA.

La familia de protocolos de Internet está conformada por alrededor de 100 protocolos distintos, de los cuales el TCP/IP es el más comúnmente utilizado para la conexión de computadoras.

Lo que lo hace tan especial es su capacidad para mantener conexiones estables entre varias computadoras en redes grandes, y aunque es relativamente lento para redes pequeñas, ofrece muchas ventajas contra otros protocolos en redes amplias (CISCO SYSTEMS, 1999).

2.2 ¿Qué es un servidor?

Un servidor es aquella entidad que permite procesar información con una finalidad específica, ayudando a realizar o controlar una o varias funciones, ya sea una manipulación por medio de actuadores físicos, o un control de información para brindar un servicio (ALEGSA, 1998).

Un servidor puede ser tanto una entidad física como una lógica, pudiendo haber varios servidores lógicos dentro de un solo servidor físico.

Para poder definir en su totalidad lo que es un servidor, se tiene que definir lo que es una comunicación. Según el diccionario de la Real Academia de la Lengua Española, una comunicación es aquel intercambio de señales mediante un código entre dos personas o entidades.

Esto es necesario para establecer que para que exista un servidor, se requiere tener alguna otra entidad que requiera de su servicio, a la que se le denomina cliente.

Existen muchos tipos de relaciones cliente - servidor, las cuales no siempre implican dos computadoras personales en ambos extremos, como puede ser con los servidores de impresión, servidores de correo, servidores web, servidores de archivos, de proxy, etc.

2.3 Sistemas operativos

Un sistema operativo (S.O.) es el conjunto de aplicaciones o software, el cual permite controlar un hardware o manipular información, de manera que el usuario pueda interactuar con él, mediante una aplicación y dispositivos de interfaz humana.

Un sistema operativo se conforma de varios subsistemas, cada uno con funciones distintas y específicas, tales como el uso del CPU, manejo de la memoria, control de periféricos, optimización de recursos, etc.

En función de lo que se tratará en esta investigación, es necesario enfocarse a los S.O. que aprovechen los recursos de red de la mejor manera posible.

Uno de los sistemas operativos más comúnmente utilizados, para realizar funciones de administración de aplicaciones, gestión de servicios, entre otros, es Solaris. Esta distribución de Unix ha sido la sucesora del desaparecido SunOS a partir de 1992, y actualmente soporta arquitecturas de hardware tan variadas como los clientes las requieran (SPARC, x86 y PowerPC).

En la actualidad las versiones y distribuciones de S.O. ya reflejan toda una historia de pruebas y errores que los han llevado a ser bastante estables y relativamente seguros.

Otras opciones comerciales para operación de sistemas son Ubuntu (Linux), Microsoft Windows Server, HP-UX (Unix), entre otros.

2.3.1 Unix

Este sistema operativo fue desarrollado por los laboratorios Bell de AT&T, y es derivado de un primer proyecto de investigación llamado MULTICS (Multiplexed Information and Computing Service – Servicio multiplexado de computación e información) en 1969, el cual pretendía

ofrecer una plataforma flexible para la utilización y migración de información de un equipo a otro más nuevo y potente, además de soporte multiusuario. En los inicios de la computación no existía la comunicación entre las computadoras, y los programas que corrían en una máquina habían sido escritos para ella, por lo que no podían ser ejecutados en otra. Dicho proyecto no obtuvo los resultados deseados y fue cancelado, sin embargo, gracias al trabajo independiente de Ken Thompson, Rudd Canaday, entre otros, dieron origen a otro sistema llamado UNICS (Uniplexed Information and Computing System – Sistema uniplexado de computación e información), el cual ofrecía lo que deseaban de Multics, pero teóricamente solo para un usuario.

Con el tiempo se le fueron agregando funcionalidades de seguridad, edición de textos, entre otras, las cuales garantizaron el financiamiento del proyecto por parte de los laboratorios Bell.

Todo sistema operativo que desee estandarizarse con los sistemas Unix, deberán acreditar la certificación UNIX 03 de la SUS o single UNIX specification (The Open Group, 2009). Actualmente, esta certificación solo la poseen 4 sistemas operativos: HP-UX (HP), IBM, Solaris (Sun) y Mac OS X 10.5 (Apple).

Tomando como base al nuevo UNIX, varias instituciones (como la universidad de Berkley y Sun Microsystem) desarrollaron sus

variaciones del mismo, las cuales, después de varios conflictos legales, lograron su independencia, alrededor del año 1975 (The Open Group, 2009).

2.3.2 Linux

Este es una variación indirecta de Unix, y es considerado como un sistema totalmente independiente a Unix.

Fue desarrollado por Linus Torvalds, basándose en el núcleo de Minix, desarrollando su núcleo propio, al que llamo Linux. Este ofrecía una mímica bastante fiel del núcleo de Unix, con compatibilidad para procesadores Intel x86.

En 1992 le fue concedida la licencia GLP (Licencia Pública General), y hasta la fecha, junto con Unix, son las versiones más usadas para servicios donde la estabilidad y confiabilidad, así como el rendimiento son importantes (Linux Online Inc., 2010).

2.3.3 Windows Server

Esta es una variante del Windows original, derivada de la familia NT, la cual esta meramente orientada al manejo y gestión de recursos de red.

Inicialmente las versiones estándar y NT eran familias totalmente paralelas de los productos de Microsoft, sin embargo, a partir de su versión XP, fue posible fusionarlas de manera relativamente estable, lo cual permitió una mucho mayor versatilidad y potencia para la ejecución y desarrollo de aplicaciones.

Las primeras versiones estándar de Windows eran solo interfaces gráficas de MS-DOS; posteriormente Microsoft reclutó a Dave Cutler, el cual fue pieza fundamental para el desarrollo de la nueva familia NT de Windows.

Actualmente, Windows en su versión más reciente está basada en la versión 6.0 del núcleo NT, que incluye aplicaciones de diagnostico y configuración de redes, así como un mejoramiento significativo en el manejo de memoria, reparación en 2do plano de particiones NTFS, cierre limpio de procesos, entre muchas otras características (Wikipedia, 2009).

2.4 Servicios de clúster y redundancias

Un clúster, por definición, es la aglomeración de entidades. En informática se entiende que un clúster es la unión de servidores mediante una red local de alta velocidad, que permite un mejor desempeño y aseguramiento de sus funciones.

Un servicio de redundancias no es lo mismo que un servicio de clúster, pero un servicio de clúster puede fungir como servicio redundante.

Entre los servicios de redundancias más populares y confiables se pueden encontrar Veritas Cluster Service y Service Guard de Red Hat.

Los servicios de redundancias en clúster son, básicamente, aplicaciones que se encargan del monitoreo de otras aplicaciones en 2 o más servidores. En caso de que exista algún problema que limite o impida la ejecución de una aplicación en un servidor, el servicio de clúster es el encargado de terminar dicha aplicación en el servidor afectado e iniciarla en algún otro servidor con los recursos disponibles para ello. (Programación en castellano, 2010)

2.5 Balanceadores de carga

Una vez que se tiene asegurada la buena operación de las aplicaciones y de las comunicaciones, mediante los servicios de clúster y redundancias, es necesario optimizar el desempeño de ambas. Esto se logra realizando un balanceo en la manera en que la carga de trabajo sea distribuida entre los servidores disponibles.

Existen balanceadores de carga físicos y lógicos.

Los balanceadores físicos son computadoras dedicadas al control del flujo de la información. La manera más usual para el balanceo de carga por este método es el Token Ring, la cual es mandar la carga a un equipo a la vez, sin verificar la cantidad de recursos disponibles en dichos servidores.

Los balanceadores lógicos son aplicaciones que pueden estar en un equipo dedicado o en cualquier otro servidor dentro del clúster, la cual tiene agentes dentro de todos los demás nodos, y monitoreando la carga de trabajo en cada nodo, direcciona la carga de trabajo hacia el equipo que garantice el procesamiento más rápido de la información (IDG COMMUNICATIONS, 2010).

2.6 Seguridad de la información

Debe entenderse por seguridad en la información a la disciplina para el resguardo de la información, cuando se requieran todos o alguno de los siguientes puntos:

- ✓ Confidencialidad
- ✓ Integridad
- ✓ Autenticidad
- ✓ Disponibilidad

En la medida que se conozcan las necesidades será la forma en que la información será protegida. Cabe recordar que la seguridad total no existe, y que se debe ser capaz de mantener un nivel deseado de resguardo (DSI, 2008).

También es necesario definir que la seguridad se basa en 4 principios o pilares principales:

- ✓ Criptografía.
- ✓ Control de acceso.
- ✓ Buenas prácticas.
- ✓ El proceso de aseguramiento.

2.6.1 ¿Qué es la criptografía?

La palabra criptografía viene del griego κρύπτω *krypto*, “oculto”, y γράφω *graphos*, “escribir”, o lo que es lo mismo “escritura oculta”.

En la historia de la información ha habido infinidad de métodos para ocultar información de los ojos de cualquier persona, y ha evolucionado de manera paralela en cada una de sus características.

Esta disciplina es de vital importancia en el aseguramiento de la información, ya que brinda las herramientas para poder entablar comunicaciones auténticas y confidenciales, dando pautas de control de acceso, esta herramienta ha permitido el nacimiento de las transacciones seguras en Internet.

Como se recuerda, los recursos en una computadora son limitados, y todo proceso extra que se tenga que aplicar a los datos, tendrá un impacto directo sobre el rendimiento de la misma.
Existen dos tipos principales de cifrado: simétrico y asimétrico.

El cifrado simétrico es muy eficiente en términos de ocupación de recursos, pero puede ser bastante problemático al momento de implementarse. Esto se debe a que este tipo de cifrado basa su seguridad en usar una misma llave de cifrado para codificar y decodificar la información, para esto, tanto el cliente como el servidor

deben poseer la misma llave y es esto lo que vuelve vulnerable a este tipo de cifrado durante el intercambio de dicha llave.

El cifrado asimétrico es más seguro y se implementa basándose en una infraestructura de llave pública (PKI), la cual hace que ahora se manejen al menos dos llaves durante el proceso de cifrado (el servidor). Aunque este esquema pueda parecer mejor que el anterior, este proceso de usar una llave para cifrar y otra para descifrar lo hace costoso en términos de recursos computacionales.

Existe un tercer tipo de cifrado que no siempre es considerado como tal, este se refiere a las funciones Hash o también conocidas como funciones de digestión (digest function).

Las funciones hash son implementadas en las firmas digitales y para el aseguramiento de la integridad de la información (DSI, 2008).

2.6.2 Algoritmos y métodos de cifrado

Desde la época de los Cesar (y antes), y en la actualidad, en la época de la información, siempre ha habido la necesidad de ocultar cierta información. Los primeros intentos de ocultarla fueron por oscuridad, es decir, aprovechando la ignorancia de quienes podían tener acceso a la información; esto fue al limitar el conocimiento de la lectura solo a las

personas que debían tener acceso a los datos preciados, entre otros métodos.

Conforme fue evolucionando la cultura popular, y los conocimientos promedio fueron creciendo, la manera de ocultamiento también evolucionó en otras medidas de seguridad. Podemos citar el ejemplo del algoritmo César, el cual consiste en sustituciones simples y mono alfabéticas sobre un texto plano. Otra opción un poco más sofisticada es la sustitución poli alfabética como en el cifrado Vigenère.

Actualmente existen estándares internacionales que no basan su seguridad en la oscuridad, sino en desafíos matemáticos que no tienen solución actualmente.

El algoritmo estándar en cifrado simétrico actualmente es el AES (Advanced Encryption Standard – Estándar Avanzado de Cifrado), el cual es sucesor del afamado DES (Data Encryption Standard – Estándar para Cifrado de Datos). Para cifrado asimétrico se debe utilizar una PKI (Public Key Infrastructure - Infraestructura de Llave Pública. Y para cuestiones de integridad, se debe analizar lo que conviene y definir cuando y como utilizar cada tipo de funciones para este propósito (DSI, 2008).

2.7 Métodos actuales para ocultar la información

La criptografía no es, hoy en día, la única manera de ocultar la información, y no siempre es la mejor opción para hacerlo.

Existen casos en los que quizá no se tendrá acceso a sistemas de descifrado, o quizá no sea necesaria una comunicación en 2 vías. En tales casos se pueden usar otros métodos para hacer privada la información, tales como la esteganografía, y métodos más antiguos como Vigenère, entre otros.

2.7.1 Esteganografía

Es la disciplina o conjunto de técnicas que permiten ocultar una información dentro de otra, para que la primera pase desapercibida y solo sea visible la segunda, y aún así se pueda recuperar la información original.

La esteganografía se puede clasificar en dos tipos: la analógica y la digital.

La analógica, como su nombre lo indica es la técnica de ocultamiento donde no interviene en ningún momento una computadora o sistema de computo digital.

Este subtema se orientará a la esteganografía digital, pues es la técnica que más concierne en el área de acción de la seguridad informática.

El ejemplo con más características didácticas es el de imágenes. Una imagen puede ocultarse dentro de otra imagen utilizando distintas técnicas. En las (figuras 2.1) y (figura 2.2) se ilustra como definiéndose un abecedario en base a diferencias entre los colores de los bits originales y los modificados, se modifica en cierta medida el tono del color de un pixel para denominar un 1 y se deja original para denominar al 0, de esta manera el producto terminado, con la información oculta, se apreciará a simple vista como la primer imagen (DSI, 2008).

126	127	129
126	127	128
125	126	128

Imagen Original

0	0.5	1
1	0	0.5
0.5	1	0.5

Marca de Agua

126	127	129
126	125	128
125	126	128

Imagen Marcada

Figura 2.1 Tabla de sustitución de pixeles

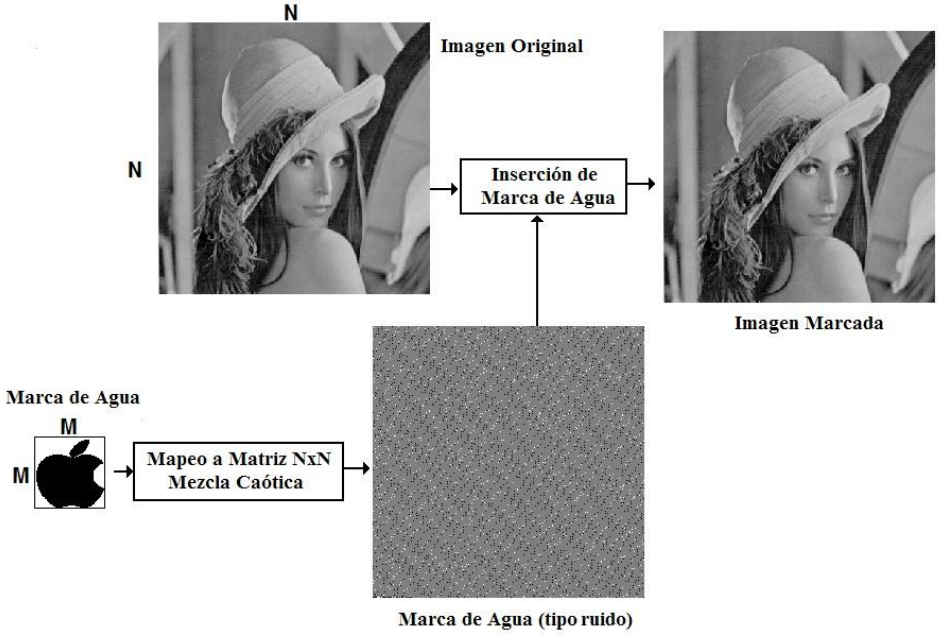

Figura 2.2 Diagrama de la implementación de una marca de agua

2.7.2 Criptografía en la era moderna

Aún cuando ya se tocó la definición de criptografía, ahora se define su importancia y campo de acción en la ocultación de la información en la era moderna.

Anteriormente se definió que la criptografía es una disciplina que ayuda a asegurar la información, aportando herramientas para varias funciones. Ahora establézcase que ésta es la piedra angular de la seguridad informática hoy en día, pues se basa en sus distintas variantes y/o disciplinas para poder implementar la seguridad en la información cotidiana y no tan habitual.

Para el establecimiento de una comunicación, es necesario el intercambio de llaves que permitan confidencialidad en el resto del intercambio (cifrado asimétrico). Para la comunicación consecuente solo es necesario utilizar una sola llave (cifrado simétrico). De esta manera se utilizan las funciones de cifrado en la información, todo esto basándose en principios básicos de las matemáticas.

Como se menciona en (Diffie Hellman, 2009), la seguridad informática se basa en desafíos matemáticos, los cuales no tienen solución hoy en día, así como en tamaños de palabra lo suficientemente grandes para poder evitar un ataque por fuerza bruta.

2.8 La seguridad en un equipo de cómputo

Este tema es introductorio para la implementación de mecanismos de seguridad, sin embargo, es necesario que se plantee para poder comprender mejor la implementación real.

Para poder asegurar la información mientras viaja en una comunicación, es recomendable que la información también esté segura de cada lado de la misma, es decir, es recomendable asegurar de la mejor manera posible la información en cada computadora.

Las maneras de realizar el aseguramiento de la información en una computadora o en cualquier otro equipo de computo será protegiendo los lugares donde reside, tanto de manera lógica como física.

Una manera de protegerla es usando hardware propietario, o hardware diseñado por un distribuidor en particular; otra manera es cifrando la información y la última y no menos importante manera de protegerla es físicamente. La combinación de todas estas da como resultado una seguridad óptima para el resguardo de la información.

2.8.1 Cifrado de la información

Todo proceso de cifrado debe ir acompañado de un descifrado, lo cual implica siempre, una carga de procesamiento extra al normal, por lo que se debe ser muy cuidadoso en definir cuán importante es la información a proteger así como las capacidades económicas y tecnológicas a disposición.

La información dentro de un equipo que puede asegurarse puede ser la información almacenada y la información en ejecución.

La información almacenada puede cifrarse de manera independiente o completa, es decir, pueden cifrarse un archivo o grupos de ellos, así como pueden cifrarse sistemas de archivos enteros (discos duros, particiones lógicas, etcétera).

La información en ejecución se protege generalmente a nivel de la programación de las aplicaciones, así como en la RAM que se utiliza. La primera manera se obtiene siguiendo todo un grupo de buenas prácticas que lleven a una utilización optimizada y segura de la memoria. La segunda generalmente se implementa con hardware especializado el cual garantiza, en la medida de lo posible, que la velocidad de I/O será la óptima, así mismo la información se mantendrá cifrada en todo momento.

2.8.2 Seguridad física

Se le conoce comúnmente como seguridad perimetral.

Un principio de la seguridad de la información es que, aunque se asegure la información de la mejor manera lógica posible, si el hardware donde está contenida cae en las manos incorrectas, eventualmente esa información será extraída del dispositivo. Por esto, la seguridad física es tanto o más importante que la seguridad lógica, aunque también puede ser la más costosa económicamente hablando.

Nuevamente debe hacerse la distinción en el costo/beneficio de la protección de la información objetivo. En base a este índice de medición se pueden establecer los mecanismos que realmente se necesitan para protegerla.

La seguridad física ha sido usada por siglos, ocasionando su perfeccionamiento o refinamiento constante, y en combinación con tecnología de última era, esta puede ser la estratagema más fuerte contra cualquier intrusión. Un ejemplo de esto puede ser la autenticación.

La autenticación de la persona que debe tener acceso a un perímetro o a cierta información siempre ha sido parte de la idea de seguridad. Históricamente las contraseñas han dado la solución, pero

recientemente este sistema de autenticación ha probado haber estado a punto de pasar a la obsolescencia. Actualmente contamos con varios sistemas que pueden autenticar algo que se posee, algo que se sabe o algo que se tiene, sea un dispositivo portátil, una contraseña de un solo uso o alguna biometría respectivamente.

La seguridad física también debe definirse como una seguridad por capas, la cual ofrece protección perimetral e interior, así como la autenticación al acceder directamente a la información o al equipo que la contiene.

2.9 Seguridad en redes informáticas

Recuérdese que la seguridad se puede implementar tanto en los datos como en la información.

Hasta ahora se ha enfocado en la protección de la información, tanto en el equipo de computo como en su transporte por medio de una red; sin embargo, en muchas ocasiones lo más eficiente es liberar de sobrecarga a las computadoras y servidores, quitándoles la tarea de cifrar la información y dejando esta tarea a hardware especializado que no cifrará toda la información, sino solamente los paquetes que son transmitidos por la red. Esto se puede implementar de más de una manera, las cuales se tratan más adelante.

2.9.1 Seguridad en las comunicaciones intercomputadoras

Como parte de la seguridad en la comunicación digital debe tomarse en cuenta todo el hardware que permitirá implementarla, así como el software que lo controla y el software que permitirá hacer cosas similares al hardware.

Firewalls o contrafuegos

Estos son por usos y costumbres los primeros equipos a los que se acude cuando pensamos acerca de seguridad informática, y efectivamente ofrecen cierta seguridad, siempre y cuando se empleen de la manera y el lugar adecuados.

Como se recuerda, un firewall solo filtrará tráfico que no se desee utilizar u otorgar acceso, y si la aplicación que está detrás no está debidamente actualizada o configurada, ésta puede convertirse en el principal punto débil, aún teniendo la mejor infraestructura montada. (Firewall, 2009)

IPv6

Aun cuando no se ha tenido experiencia directa con este nuevo sistema o estándar, se incluye ya que proporciona ventajas sobre el IPv4, las cuales ayudan a garantizar una mejor integración con el sistema de seguridad opcional de IPSec.

IPv6 permite definir prioridades a los tipos de flujos de datos, etiquetándolos como paquetes o como flujos (streamings), otorgándoles jerarquías a los distintos servicios que se brindan.

IPSec

Aquí se encuentra una suite de herramientas criptográficas que ayudan a maximizar la seguridad en las comunicaciones.

Este estándar es implementado de manera obligatoria con IPv6 y se mantiene optativo para el IPv4. Este dinamismo o flexibilidad se logra gracias a que IPSec actúa en el nivel 3 (capa de red) del modelo OSI, lo que lo hace implementable a cualquier comunicación segura o insegura actual (IPSec, 2006).

Wi Fi – IEEE 802.11

Esta es un área bastante polémica, ya que cualquier comunicación mediante ondas electromagnéticas es considerada como insegura, puesto que no se está tratando de medios de comunicación dirigidos, sino de difusión.

Toda la seguridad que se pueda implementar con la tecnología alámbrica puede ser aplicada a ésta, sin embargo, deben omitirse algunas propiedades y tomar en cuenta algunas ventajas y desventajas. Como se trata más adelante, la desventaja más importante es el medio en sí, así como sus limitaciones en ancho de banda y en algunos casos la distancia de transmisión. Así mismo, se deben considerar sus ventajas como puede ser la versatilidad, comodidad y practicidad.

Para mejores referencias, se acota toda mención de señales inalámbricas, al estándar emitido por la IEEE acerca de las comunicaciones inalámbricas entre equipos de cómputo. Dicho estándar es el IEEE 802.11b y 802.11g (IEEE, 2009).

3. Implementación y recomendaciones de la seguridad de bajo nivel

No existen recetas para la seguridad, pero si se logra tener un buen entendimiento de lo que se pretende realizar al proteger la información y el avalúo de la información misma, entonces podrán plantearse pautas para la ejecución de prácticas de seguridad informática que se acomoden lo mejor posible a las condiciones y ambientes particulares de cada empresa o individuo.

También merece la pena recalcar que la implementación de la seguridad junto con su planeación no garantizarán nada si no se cuenta con un programa de mantenimiento y monitoreo, así como una capacitación continua al personal involucrado con el monitoreo de los equipos, y al personal administrativo.

El término de seguridad a bajo nivel se refiere a todas aquellas políticas que permitan garantizar la seguridad a niveles no aplicativos o de SO, es decir, en las primeras capas del modelo OSI.

3.1 Seguridad física y su implementación

Tal y como ya se había mencionado acerca de la seguridad física, ésta es una pieza fundamental en el resguardo de la información, por lo que ésta definirá la seriedad con la que se está protegiendo la información.

Aunque el propósito de este documento es la implementación de la seguridad en el monitoreo de los equipos, también se debe contar con la seguridad física de los equipos como pilar de la estructura organizacional.

No tiene caso proteger la información en su transporte al equipo, si este está disponible para otros tipos de ataques menos sofisticados pero igualmente dañinos.

Como ejemplo de un tipo de ataque que puede ser de tipo lógico como físico, tenemos la suplantación de identidad. Esto puede ocurrir tanto por una desviación de la información hacia otro equipo, como por la suplantación física del mismo.

3.1.1 Control de Acceso (CA)

El primer tipo de control de acceso que se tratará, quizá sea el último que se deba considerar por su costo, es decir, la contratación de personal de seguridad.

Para llegar a la conclusión de contratar personal de seguridad es porque se ha realizado un análisis formal de costo/beneficio, ya que no se debe poner en manos de cualquier individuo ni persona la seguridad de la infraestructura de la empresa.

Tómese en cuenta que la empresa y su personal de seguridad deberán trabajar bajo las condiciones impuestas por la empresa a la que estarán protegiendo, claro está, permitiéndoles aportar su experiencia en la materia. Esto lleva de nuevo a la conclusión de que para poder mandar se debe saber qué es lo que se quiere, y para saberlo es porque ya se paso por etapas previas que ayudaran a acotar las necesidades y fortalezas informáticas, así como las vulnerabilidades y atributos en las instalaciones (debe saberse si de verdad es necesaria la seguridad física y no guiarse de tendencias ni recomendaciones informales).

Otra implementación del control de acceso es la verificación de la identidad del personal mediante la validación de algo que sabe, algo que tiene o algo que sea parte de el/ella.

Las validaciones se pueden llevar a cabo de las siguientes maneras:

Algo que se sabe. Esto puede ser mediante la utilización de una computadora o un teclado numérico al momento del acceso, donde se necesite el ingreso de una clave o contraseña.

Algo que se tiene. Ya sea la verificación de algún dispositivo electrónico o la posesión de una identificación.

Algo que sea parte de la persona. Esto se refiere a biometría. Cualquier dispositivo biométrico para la verificación de la identidad de la persona (DSI, 2008).

3.1.2 Monitoreo del perímetro

Esto puede llevarse a cabo nuevamente mediante la vigilancia de personal dedicado a esta función, así como mediante la utilización de circuitos cerrados de televisión, sensores de movimiento, sensores de presencia, etc.

Ambas implementaciones de la seguridad física deben ser combinadas para la optimización de la misma, ya sea acotando al menor número posible los accesos a las instalaciones, así como la vigilancia óptima de dichos accesos.

3.2 Aplicaciones emuladoras para línea de comandos

Aquí no se describirán las distintas aplicaciones en el mercado que permiten realizar esta función. Lo que se pretende es que se entienda que la seguridad en las aplicaciones que se utilicen estará en la compatibilidad que tengan dichas aplicaciones para la utilización de los estándares más altos de seguridad para el cifrado de la información, ya sea implementando el cifrado simétrico o asimétrico.

Como ya se había comentado anteriormente, y aquí aplica perfectamente, la seguridad en las aplicaciones no recae totalmente en la fortaleza de su programación, sino en lo bien que se tenga configurada para optimizar las funciones que requiere su cumplimiento. Como parte de la buena configuración de las aplicaciones se debe llevar un adecuado control de los certificados de los equipos a los que se requiere conexión por Secure Shell, el cual infiere la utilización de una PKI auto implementada. Siempre que sea posible debe evitarse la utilización del telnet, ya que ésta herramienta no ofrece ninguna protección contra el monitoreo de la conexión.

Casi todas las aplicaciones que se pueden descargar de manera gratuita desde Internet tienen la opción combinada de SSH y Telnet, las cuales pueden configurarse de manera independiente y permiten al usuario la personalización casi total de la manera en que se entablarán las comunicaciones (figura 3.1).

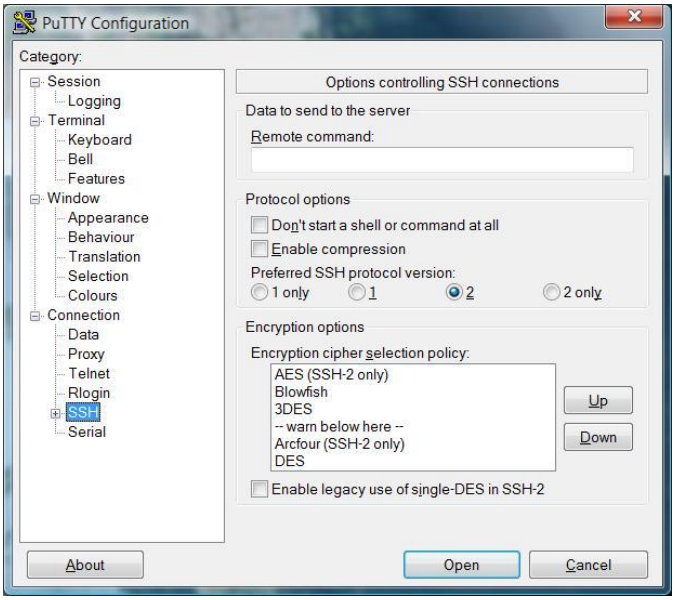

Figura 3.1 Ventana de configuración PuTTY

La utilización de certificados digitales confiables debe ser considerada seriamente para poder asegurar la autenticidad de las entidades en la comunicación, aunque sí deben tomarse en cuenta los certificados reconocidos por una autoridad certificadora, es algo que puede ser sumamente costoso y administrativamente laborioso.

3.3 Unix, Linux y Windows como S.O. de servicio

Ahora se debe comenzar a formalizar la relación costo/beneficio de las compras e implementaciones.

3.3.1 Linux

Ésta es la opción más económica, y no por eso debe entenderse como la menos potente o formal. Ésta ofrece generalmente una licencia de software libre y permite realizar implementaciones bastante más económicas en comparación con las otras opciones.

Fortalezas

- ✓ Reducción de costos
- ✓ Potencia y versatilidad
- ✓ Documentación en línea

Desventajas

- ✓ El soporte puede estar limitado
- ✓ Compatibilidad de hardware

Cabe destacar que existen distribuciones libres de Linux que están orientadas totalmente a los servidores y están optimizados sus

procesos. Así mismo, también existen distribuciones no libres las cuales requieren una cuota por su soporte y las cuales garantizan su estabilidad y su operación de una manera un tanto más formal. Un ejemplo de esta última es Red Hat.

Actualizaciones

Estas dependerán totalmente de la distribución de que se utilice y sus políticas de soporte. Por citar un ejemplo de un sistema de actualizaciones de Linux, revisemos el de Ubuntu (Ubuntu, 2009a).

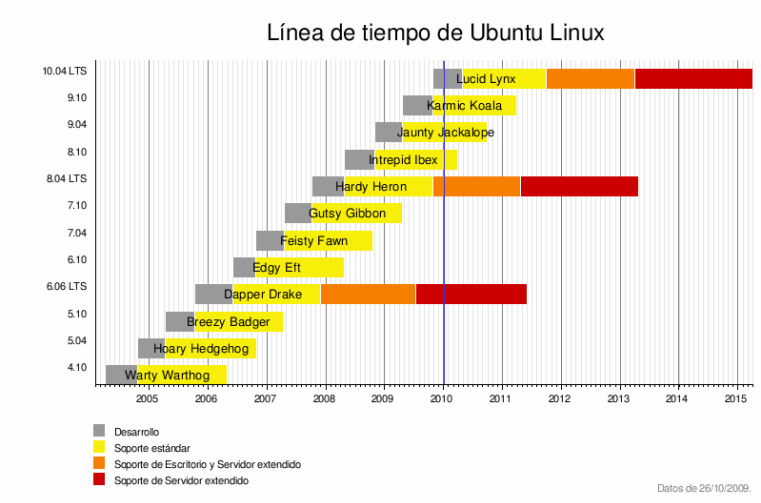

Figura 3.2 Esquema de actualizaciones de Ubuntu

Una de las más grandes fortalezas de Linux es su constante evolución, derivada de su política de software libre, la cual permite a cualquier usuario realizar modificaciones y mejoras a cada aplicación de manera

independiente. Una de las distribuciones que ha cobrado mucha fuerza es Ubuntu, la cual ofrece un sistema distintivo de actualizaciones vía Web de Debian GNU/Linux, así como un soporte continuo de sus aplicaciones dependiendo de la versión que se adquiera. Recientemente Ubuntu 8.04 Server Edition fue adoptada por Wikipedia como su S.O. para la operación de sus servidores en operación (Fernández, 2008). Así mismo se ha convertido en una competencia seria para otras distribuciones que dan estos servicios, tales como SuSE (SuSE, 2010) y Red Hat (Red Hat, 2010) /Fedora (Fedora, 2010)

Ubuntu maneja un esquema de actualización periódica cada seis meses, proporcionando soporte limitado para cada versión lanzada. Sin embargo, cada 2 años lanza una versión LTS (Log Term Support – Soporte de Tiempo Porolongado) (figura 3.2)

Independientemente de estas actualizaciones de distribución, constantemente se están realizando revisiones de actualizaciones del software ya instalado en el equipo. Esto aplica tanto para equipos de escritorio como para servidores, siempre y cuando sean configurados de manera correcta.

Requerimientos de hardware

Estos requerimientos recomendados son para la versión para servidores (Ubuntu, 2009b).

- ✓ Procesador x86 a 700 Mhz
- ✓ 384 Mb de memoria RAM
- ✓ 8 Gb de disco duro
- ✓ Tarjeta gráfica que soporte una resolución mínima de 1024 por 768 pixeles
- ✓ Tarjeta de sonido
- ✓ Interfaz de red (altamente recomendada con salida a Internet).

A continuación se muestran los requerimientos mínimos del sistema.

- ✓ Procesador x86 a 300 Mhz
- ✓ 64 Mb de memoria RAM
- ✓ 4 Gb de disco duro
- ✓ Trajeta gráfica VGA con resolución mínima de 640 por 480 pixeles.

3.3.2 Unix

El caso de Unix es algo muy distinto puesto que según su evolución, Unix se ha convertido en su gran mayoría, en un sistema operativo propietario, es decir, posee derechos de autor y no puede ser modificado sin autorización del mismo, y por consiguiente nunca se tendrá permitido ver su código fuente, aunque su núcleo y principios siguen siendo aquellos del software libre.

Para que un sistema operativo pueda ser considerado como perteneciente a los sistemas Unix, debe pasar por varios procesos de verificación y certificación (The Open Group, 2009).

Una de las aportaciones más significativas de estos sistemas, es la unificación de esfuerzos en una sola organización que se organiza de coordinar su compatibilidad y portabilidad entre plataformas.

Fortalezas

- ✓ Soporte extendido
- ✓ Aseguramiento de la versatilidad de sistemas, lo que permite cambiar de S.O. en el momento que se

considere oportuno por otro, dentro de los mismos estándares

- ✓ Bajos requerimientos de hardware
- ✓ Una amplia gama de posibilidades de capacitación y certificación para el personal encargado.

Desventajas

- ✓ Los costos pueden ser demasiado elevados para la mayoría de las PyMES
- ✓ Configuración puede llegar a ser bastante compleja, lo que hace necesaria en muchas ocasiones la capacitación o el soporte de especialistas en Unix.

Por estas características, los sistemas Unix están especializados, en su mayoría, en sistemas de carácter crítico y/o de alto rendimiento, con la excepción de Apple y su sistema Mac OS X. Sin embargo Apple, también cuenta con su sistema Xserve, el cual ofrece ventajas, como un número de licencias ilimitadas por cliente, en su versión profesional.

Actualizaciones

Estas dependerán nuevamente de la distribución que se esté usando. Se tomará como ejemplo el sistema de actualizaciones de Solaris de Sun Microsystems, el cual no se compone de una metodología estricta y planificada, sino de un conjunto de recomendaciones y sugerencias de buenas prácticas en la actualización de sus sistemas (Sun, 2004).

Entre las recomendaciones que sugieren, esta la política de actualización basada en necesidades inmediatas, esto es, que se recomienda actualizar un sistema únicamente en el momento y forma que sean necesarios, descartando actualizaciones innecesarias por la mera intención de estar al día.

Los parches y actualizaciones de software de esta distribución de Unix son desarrollados basados en la misma política, liberando actualizaciones todo el tiempo pero poniéndolas al alcance de sus usuarios solo en caso de que las requieran, lo cual debe estar primeramente en consideración del mismo usuario.

Requerimientos de hardware:

Estos requerimientos recomendados son para versiones de servicio (Sun, 2009).

- ✓ Procesador x86 o SPARC a 2 Ghz con cuatro núcleos
- ✓ 8 Gb de memoria RAM
- ✓ 16 Gb de disco duro.

Los siguientes requerimientos de hardware son los mínimos soportados por la versión más reciente del sistema operativo.

- ✓ Procesador x86 o SPARC a 1.6 Ghz con 2 núcleos
- ✓ 4 Gb de memoria RAM
- ✓ 8 Gb de disco duro.

3.3.3 Windows Server

Como se comentó en el marco teórico, Windows Server se encuentra actualmente en su versión 2008 R2. Esta cuenta con el núcleo más actualizado de la familia NT y ofrece ventajas nuevas en cuanto al manejo de políticas de seguridad y administración local del equipo, así como características para el monitoreo remoto (Microsoft, 2009a).

Windows Server 2008 R2 es la contraparte del Windows 7, el cual está orientado al uso casero. Aunque ambos están basados en el mismo kernel, sus diferencias más significativas están en el soporte que ofrecen, en las aplicaciones que incluyen y los costos por licencia.

Fortalezas

- ✓ Compatibilidad mejorada con las más recientes aplicaciones diseñadas para sistemas Microsoft
- ✓ Avances respecto a la estabilidad del sistema, con referencia a versiones anteriores el S.O
- ✓ Un ambiente totalmente gráfico para su administración, servicio y configuración.
- ✓ Soporte continuo.

Desventajas

- ✓ La administración remota requiere forzosamente la utilización de aplicaciones gráficas y estas requieren mucho más ancho de banda que las consolas de líneas de comandos
- ✓ El costo por licencia puede ser bastante elevado

- ✓ Requerimientos de hardware mayores para la instalación del mero sistema operativo y sus herramientas de mantenimiento (Microsoft B, 2007)
- ✓ Un mayor número de amenazas hacia el S.O. provenientes de virus y software malintencionado
- ✓ El uso de software antivirus es extremadamente recomendado.

Actualizaciones

Microsoft aplica una política de actualizaciones mucho más estricta y continua que otros sistemas operativos, en parte por ser el mayor foco de ataque de aplicaciones malintencionadas en Internet, y por otro lado por el número de errores que siempre traen arrastrando cada nueva versión de este sistema operativo. Esto no quiere decir que el sistema sea malo, sin embargo la relación costo/beneficio debe ser considerada seriamente para evitar gastos innecesarios.

Aunque Microsoft también libera actualizaciones para mejoras en su software, también es cierto que la mayor parte de sus actualizaciones son dedicadas a la corrección de vulnerabilidades en seguridad y en la autenticación de licencias.

Microsoft recomienda mantener bien protegidos sus sistemas, manteniéndolos al día con las últimas actualizaciones y utilizando sus sistemas de actualización integrados en el sistema operativo.

Requerimientos de hardware

Los requerimientos de hardware recomendados son los siguientes (Microsoft, 2007b).

- ✓ Procesador x86 a 2 Ghz
- ✓ 2 Gb de memoria RAM
- ✓ 40 Gb de disco duro
- ✓ DVD-ROM.

Las siguientes características son las mínimas soportadas por el sistema operativo.

- ✓ Procesador x86 a 1 Ghz o x64 a 1.4 Ghz
- ✓ 512 Mb de memoria RAM
- ✓ 10 Gb de disco duro
- ✓ DVD-ROM
- ✓ Tarjeta gráfica con resolución mínima de 800 por 600 pixeles.

3.3.4 Virus, antivirus y demás software malicioso

Existe software malicioso para cualquier sistema operativo, aunque la diferencia es el tipo de software del que se esté tratando.

Un problema bastante conocido de los sistemas Windows es la cantidad de virus que pueden infectar el sistema y que, de hecho, existen virus residentes en internet, que de no ser por firewalls y algún antivirus instalado sobre Windows, éste podría infectarse solo con conectarse a Internet.

Esto no quiere decir que los virus solo existan para Windows y sus varias presentaciones, sin embargo, las aplicaciones maliciosas que pueden existir para otros sistemas operativos, están diseñados con objetivos mucho más específicos, tales como exploids, software espía, entre otros, pero todos con el fin de penetrar la seguridad y poder sacar algún provecho de éste. Con esto se quiere dar a entender que la seguridad es crucial tanto en sistemas Windows como Linux o Unix, y se debe tener conciencia del tamaño de las amenazas que acechan los sistemas (ESET, 2010).

3.4 Aplicaciones en la seguridad informática

Entre las aplicaciones más comunes de la seguridad de la información tenemos IPSec, SSL, las PKI, y firmas y certificados digitales.

3.4.1 IPSec

Este es un conjunto de protocolos de seguridad que actúan dentro de las primeras tres capas del modelo OSI, lo cual lo hace transparente para toda aplicación.

Fue incluido obligatoriamente dentro de la sexta versión del protocolo IP, y aunque no se utilice esta versión de dicho protocolo, aún se puede incluir en la versión IPv4.

Esta extensión del IP fue incluida en el RFC 2401 (NWG BBN, 1998), el cual lo detalla y acota. Fue desarrollado inicialmente para IPv6, pero posteriormente fue migrado a IPv4 para su mejor integración con los sistemas actuales.

Aunque pueda parecer una excelente opción de seguridad, debe tenerse en cuenta que al no ser una implementación de software, esta infiere la integración de equipos especializados que puedan manejar este sistema, y al mismo tiempo se debe integrar a la perfección con los demás equipos de la red local, para evitar problemas de comunicación y compatibilidad.

Actualmente ya se cuenta con una gran variedad de equipos compatibles con esta tecnología, y también existen algunos S.O. como Windows que ofrecen compatibilidad con IPSec a nivel de aplicación, modificando o cifrando los encabezados de los paquetes desde antes de ser procesados por los equipos de red (esto puede mermar bastante el rendimiento de la red) (Microsoft, 2009c).

3.4.2 SSL

La capa de socket seguro o SSL por sus siglas en inglés (Secure Socket Layer), es una de las implementaciones de seguridad mas empleadas en la actualidad para el manejo de información segura, ya sea para gestión o para servicios.

Generalmente basta con la instalación de la aplicación o daemons correspondientes para la implementación de esta herramienta, aunque

se debe considerar el tipo de información a proteger, ya sea de servicio o de gestión.

Por usos y costumbres, el SSL se utiliza para servicios Web tales como servicios bancarios, correos electrónicos, entre otros, esto gracias a que maneja de manera nativa llaves de sesión y sistemas de cifrado simétricos y asimétricos (CSICE, 1998).

Es una opción buena y relativamente económica, la cual puede implementarse sin muchos problemas con la integración a las aplicaciones que puedan ser productivas en ese momento. Claro está que debe considerarse el impacto que se puede tener sobre usuarios que no tienen la capacidad de utilizar este protocolo, ya que esta incapacidad denegará el servicio a estos usuarios.

3.4.3 PKI

Una Infraestructura de llave pública (Public Key Infraestructure) es el mecanismo mediante el cual se puede establecer una comunicación segura cliente – servidor, sin haber tenido comunicación previa. Esto se logra mediante la utilización de autoridades certificadoras y certificados digitales, los cuales contienen las llaves públicas de las entidades de servicio generalmente, aunque también pueden incluir al cliente.

Puede considerarse como una de las opciones más seguras para las implementaciones de seguridad, aunque también la más cara, ya que los certificados de autoridades certificadoras con importancia mundial, pueden llegar a costar mucho dinero (Verisign, 2009).

El SSL antes mencionado puede ser una de las implementaciones relacionadas con una PKI, pero no necesariamente se necesita tener implementada esta para poder lograr una buena seguridad con SSL solamente.

De las ventajas que ofrece la implementación de una PKI es, además de la seguridad, la imagen de consolidación y compromiso con la seguridad de una empresa. Esto no quiere decir que sea la única manera de alcanzar estos estándares, pero puede ser un factor fundamental, para varios tipos de servicios, en la realización de transacciones seguras de servicio o hasta de gestión.

Esta es una opción muy delicada, debido a que sus costos pueden ser excesivos para la mayoría de las empresas medianas y pequeñas, y aun así puede ser de mucha ayuda en la concertación de varios tipos de servicios, tal y como se mencionó anteriormente.

3.4.4 Firmas Digitales

Nótese que cada aspecto de la seguridad puede aplicarse independientemente, pero siempre puede, y en ocasiones debe mezclarse, parcial o totalmente con otras aplicaciones de la seguridad informática. Este es el caso de las firmas digitales, las cuales forman parte de las infraestructuras de llave pública y al mismo tiempo son una variante o aplicación de los certificados SSL, sin embargo, su aplicación puede o no ser implementada junto con la certificación de la empresa y sus servicios, y puede ser implementada únicamente en correos electrónicos, o en algunos otros servicios de uso común, los cuales ayudan a mantener una autenticación unilateral de la institución para con los demás.

Debe recordarse que las firmas digitales no solo autentican al generador del documento en cuestión, sino que también garantiza la integridad del mismo, otorgando así dos servicios de la seguridad informática al mismo tiempo (CINVESTAV, 2005).

Al igual que las PKI, las firmas digitales pueden llegar a ser muy caras o bastante económicas, dependiendo del nivel de seguridad que se desee (Verisign, 2009).

Para casos donde las empresas son pequeñas, y solo requieren un aseguramiento básico de la identidad de las personas con las que se comunican, un certificado quizá sea demasiada inversión, mientras que para empresas en transición de medianas a grandes, esta es una inversión casi obligada, siempre y cuando la autenticación sea un servicio de seguridad crítico, tales como los bancos, entre otros rubros.

3.4.5 Telnet

Esta es una de las herramientas básicas para la administración remota de servidores Linux y Unix. Aunque es una de las más inseguras, debe mencionarse que en caso de no poseer otra herramienta, muchas veces el administrador se verá orillado a utilizar este tipo de protocolos de comunicación en claro.

El telnet como protocolo y aplicación viene incluido en la mayoría de los S.O. hoy en día. Su uso principal es como herramienta secundaria de gestión, esto derivado de su principal debilidad, la seguridad. Toda la información, incluyendo nombres de usuario y contraseñas, son enviadas en texto plano o en claro, lo cual lo hace muy poco eficiente, en lo que a seguridad se refiere (Telnet, 2009).

3.4.6 SSH

He aquí la contraparte del Telnet. Como su nombre lo indica, el Secure Shell ofrece un shell seguro para la gestión remota de equipos compatibles, tales como Unix y Linux.

El SSH puede trabajar bajo una serie bastante completa de sistemas de cifrado simétricos y asimétricos, tales como AES; IDEA, DES, 3DES, etcétera, todos estos con sus distintos modos de ejecución.

Tal como telnet, SSH es principalmente para la gestión remota de equipos, solo que ofrece un túnel de extremo a extremo en la comunicación, haciendo muy difícil o virtualmente imposible para cualquier intruso la decodificación de la información.

Existen versiones libres y propietarias de las aplicaciones SSH, sin embargo, en promedio, todas ellas ofrecen las mismas fortalezas, siendo la interfaz y el soporte lo único que varía de unas a otras. El proyecto openSSH es uno de los más importantes en el desarrollo de esta capa de conexión (OpenSSH, 2009).

A continuación se enlista una serie de aplicaciones libres populares para la gestión remota, muchas de las cuales soportan tanto Telnet, SSH, FTP, SFTP, entre otros protocolos de conexión:

- ✓ PuTTY
- ✓ TTSSH
- ✓ Cygwin
- ✓ WinSCP
- ✓ FileZilla.

4. Implementación de la seguridad en el software

Debe aclararse que la seguridad en el software está definida por la calidad de la programación con la que está hecho y la integración con otros sistemas o aplicaciones del mismo sistema operativo.

Para combatir las amenazas de software se debe asegurar primero que las aplicaciones que se estén utilizando sean de proveedores confiables, así como que sus actualizaciones sean constantes y bien estructuradas en tiempo y forma. Cada actualización debe resolver problemas específicos y no solo llevar a un número de versión más reciente. Así mismo, se debe tener control sobre el sistema de actualización, para que de esta manera no se vea comprometida la compatibilidad entre las aplicaciones.

4.1 Seguridad en la programación

Como se mencionó anteriormente, la seguridad en las aplicaciones comienza desde la programación. Un buen esquema de diseño para una aplicación, derivará en una aplicación estable, segura y versátil.

Cabe mencionar que una de las fallas más comunes de seguridad en las aplicaciones, son los desbordamientos de pila. Aunque este error puede ser evitado fácilmente, es sumamente sencillo caer en este error de diseño, esto por subestimar cantidades de datos de ejecución.

A nivel de aplicación puede haber una infinidad de propósitos y maneras de resolver problemas, los cuales pueden ser desde scripts con propósitos específicos, hasta desarrollos web dinámicos para servicio a clientes.

4.1.1 Programación Web

Las aplicaciones Web deben ser especialmente seguras, pues estarán a disposición y acceso de millones de personas. Dependiendo de los servicios que se ofrezcan, debe considerarse la integración de distintos lenguajes de programación y la utilización de SSL para algunas transacciones.

Actualmente la manera más común de desarrollar páginas seguras es encapsulando el código en mini aplicaciones que se ejecuten binariamente en el host, ya sea utilizando Java, PHP, .NET, entre otros.

4.1.2 Aplicaciones seguras

Se considerará en este subtema a las aplicaciones de servicio, que no sean desarrollos para la Web, incluyendo todas aquellas aplicaciones locales que sirvan para el funcionamiento de los equipos.

El problema más común de seguridad en los desarrollos actuales, es el hecho de que casi todas se basan enteramente en sus versiones anteriores, con lo que heredan parte de sus debilidades junto con sus fortalezas. Por lo anterior se debe saber con exactitud las correcciones que realiza cada parche que se instala, y cuando se realice una actualización mayor de la aplicación, debe verificarse que no existan vulnerabilidades ya corregidas en versiones anteriores.

Al momento de requisitar la instalación de una aplicación, esta debe ser sometida al escrutinio de un profesional, para poder evaluar que tan necesaria es la misma, los equivalentes propietarios y libres, y sobre todo, que estas puedan poner en riesgo de alguna manera la información con la que vaya a trabajarse.

Muchas veces es bueno comenzar con la utilización de software que sabemos que funciona bien por el conocimiento empírico de la aplicación, teniendo como referencia el uso de otras empresas y/o personas para evitar parcialidad en el juicio. Una vez que se tenga

comprobada la eficacia de la aplicación, entonces puede intentarse, en ambientes controlados, emplear otras herramientas que presuman de ser más eficientes, aplicando todas las precauciones ya mencionadas.

Enfocándose en la gestión de los equipos, dichas aplicaciones deben ser suficientemente seguras para permitir permisos controlados a los usuarios, y así prevenir cualquier mal uso potencial de las mismas.

4.2 Computación móvil

En la actualidad encontramos otros tipos de desarrollos y riesgos, tales como las aplicaciones móviles, ya sean para celulares, PDAs y cualquier otro dispositivo que pueda conectarse a otros equipos.

Debe tenerse un control de acceso planificado hacia los equipos de servicio, para evitar que cualquier usuario pueda convertirse en un administrador potencial, ya que ambas redes deben ser independientes y no estar relacionadas por ningún equipo, salvo aquellos que sean considerados como accesos controlados para casos emergentes.

La gestión de los equipos de servicio debe estar limitada a equipos, personas y ubicaciones especificas, dependiendo de las necesidades de seguridad, y nunca abierta a cualquiera que quiera acceder a ellos.

Con el auge actual de las telecomunicaciones, y los dispositivos cada vez más potentes y pequeños, el control de acceso de gestión debe enfocarse a la autenticación de las personas y de la red desde la cual se conecta el administrador del equipo, ya sea con contraseñas o certificados SSL y VPNs (Virtual Private Network – Red Virtual Privada).

4.3 Normatividad internacional

La normalización de estándares mundiales en comunicaciones, así como el control de las mismas ayuda a una mejor evolución de la seguridad, definiendo los márgenes de acción de cada desarrollo computacional.

Actualmente existen estándares que definen a las herramientas cotidianas, tales como el ISO 17799 y el ISO 27001, los cuales son importantes por sus implicaciones en la seguridad informática.

También existen organismos internacionales que ayudan a las empresas a estar actualizadas con respecto a nuevas amenazas informáticas, así como de las novedades en la seguridad. Entre estas instituciones pueden encontrarse en (CERT, 2010) y el (NIST, 2010), como miembros de la organización FIRST (Forum for Incident

Response and Security Teams – Foro para Respuesta a Incidentes y Equipos de Seguridad) (FIRST, 2009).

4.3.1 ISO 17799

Este estándar está destinado a definir una guía de buenas prácticas para la implementación de la seguridad, el cual plantea políticas de seguridad, organización de la seguridad de la información, manejo de activos, seguridad de recursos humanos, seguridad física y del entorno, manejo de operaciones y comunicaciones, control de acceso, mantenimiento, desarrollo y adquisición de sistemas de información, administración de incidentes de seguridad, manejo de la continuidad del negocio y por último el cumplimiento de todas las anteriores (DGSCA, 2008).

Cada apartado define su objetivo y los controles necesarios recomendados para llevarlo a cabo, de los cuales se describen de manera muy breve, tomando en cuenta una interpretación didáctica del estándar.

Políticas de seguridad

Deben ser autorizadas por la dirección, y difundidas a todos sus empleados, siendo actualizada periódicamente.

Organización de la seguridad de la información

La dirección de la empresa debe aportar una guía de seguridad con las responsabilidades de seguridad claramente definidas, así como una definición completa del control de acceso para personal externo

4.3.2 ISO 27001

Éste otro estándar está destinado a la promoción de una cultura de seguridad entre los usuarios y personas que tengan alguna relación con los sistemas informáticos. Así mismo plantea un sistema cíclico de seguridad el cual comienza con la implementación del Sistema de Gestión de la Seguridad Informática (SGSI), posteriormente plantea la operación y monitoreo del sistema, el mantenimiento y la mejora continua, y regresa al establecimiento o modificación al sistema para su mejora.

Con respecto a los puntos que se detallan dentro del estándar, se comenzará por describir de manera consecutiva cada uno de los puntos (http://www.iso27000.es/).

En el punto 1 se menciona la aplicación del estándar, donde se establecen los requisitos y las excepciones al mismo. En el punto 2 están las referencias normativas, en las cuales se hace mención del estándar 17799:2005. El punto 3 es para la definición del glosario que se utiliza a lo largo del estándar.

A lo largo de los subtemas del punto 4, se define el proceder durante el ciclo antes mencionado, así como una serie de recomendaciones para el mantenimiento de registros escritos de todo cambio y mejora al SGSI.

En los puntos 5, 6, 7 y 8 se definen las responsabilidades de la administración del SGSI, su auditoria, revisiones periódicas, y su mejora continua respectivamente (ISO, 2005).

4.3.3 COBIT v4.0

Ahora se comentará éste otro sistema de control de la seguridad informática para las empresas.

La diferencia principal del COBIT con respecto a los demás estándares, es que precisamente no es un estándar, sino un documento que sirve como referencia a las empresas interesadas para la implementación del modelo se seguridad que se propone.

Sus siglas significan Control Objectives for Information and related Technology (Objetivos de Control para la Información y Tecnología relacionada), y en su visión definen que COBIT existe para subsanar la necesidad del área de TI de cuadrar con los requerimientos de la empresa mediante la implantación de un esquema de trabajo especializado.

El esquema de trabajo o framework que plantea el COBIT consta de cinco bloques principales:

- ✓ Información
- ✓ Plan y organización
- ✓ Adquisición e implementación
- ✓ Entrega y soporte
- ✓ Monitoreo y evaluación.

De manera similar a lo que se realiza en el ISO 27001, el COBIT establece una retroalimentación en su esquema de trabajo.

Todo comienza en el bloque de información, donde se intercambia información con la dirección de la empresa. Posteriormente, durante la planeación y organización, se establece la manera en que la tecnología informática ayuda a seguir con los objetivos estratégicos de la empresa. En la adquisición e implementación se plantean las consideraciones al comprar e instalar nuevas tecnologías o actualizaciones de las ya existentes. Para la entrega y soporte, define una manera de control para la correcta entrega y definición de una buena política de soporte para las tecnologías recién implementadas. Aunque el monitoreo y evaluación es parte del soporte, se define de manera independiente para la correcta retroalimentación y seguimiento de la corrección de fallas. (ISACA, 2010)

4.3.4 Criterios Comunes

La variedad de estándares y propuestas orilló a esta organización a crear lo que ahora se conoce como Common Criteria o Criterios Comunes, el cual es un intento de unificación de criterios y estándares para empresas dedicadas a la comercialización de productos de seguridad.

Los criterios comunes fueron desarrollados en conjunto con los gobiernos de Canadá, Francia, Alemania, Holanda, Inglaterra y Estados

Unidos, y actualmente cuenta con alrededor de 25 miembros, tales como Austria, Turquía, Dinamarca, entre otros (CC, 2009).

Los CC están estandarizados en el ISO 15408, y a diferencia de los ISO que se han tratado, este permite que la empresa defina sus propias necesidades y al mismo tiempo mantiene el control sobre la implementación y control de las políticas de seguridad para la empresa y sus proveedores.

4.4 Administración de la seguridad

Hasta ahora se ha tratado la seguridad como un asunto relacionado únicamente con el área de TI y su dirección, sin embargo, debe aterrizarse que esto concierne a toda la empresa y que se requiere definir una administración de la misma, independiente del área de TI, pero relacionada en su control.

Se debe comenzar relacionando la misión de la seguridad con la misión de la empresa. Esto garantizará que los objetivos de la implantación sean seguidos y que la seguridad implementada sea congruente con las necesidades de la institución.

Seguido a la incorporación de la seguridad a la administración de la empresa, ésta debe ser sometida a una serie de análisis que permitirán tener una mejor idea de lo que se necesita y como se necesita. Los análisis más relevantes son los relacionados con los riesgos y análisis cuantitativos y cualitativos.

4.4.1 Fases generales de un análisis de riesgo

Éstas son enunciadas de tal manera que faciliten la identificación de los activos y al mismo tiempo la localización oportuna de vulnerabilidades.

- ✓ Enunciar el alcance
- ✓ Identificar las amenazas
- ✓ Priorizar las amenazas
- ✓ Estimar el impacto total de la amenaza
- ✓ Identificar medidas de protección (controles)
- ✓ Realizar un análisis costo/beneficio
- ✓ Ordenar las medidas de protección por prioridades
- ✓ Reportar el resultado del análisis

Posterior a estas fases y previo al desarrollo de las políticas de seguridad, se deben utilizar los inventarios de activos, las vulnerabilidades encontradas, en combinación del análisis formal de costo/beneficio, para aplicar mecanismos que permitan la minimización de riesgos, protegiendo los activos y contrarrestando las vulnerabilidades en la medida de lo posible.

La lista de los activos se recomienda que se actualice de manera regular, y esta debe contener los activos regulares así como a relación de hardware, software, datos, documentación, etcétera (DSI, 2008).

4.4.2 Análisis cuantitativo y cualitativo

Este análisis es parte fundamental del análisis de riesgos, ya que a la dirección de la empresa le da una idea clara de cuanto se tiene y cuanto se puede perder en caso de alguna contingencia.

Es necesario el avalúo de los activos físicos, mediante el control fidedigno de facturas, notas y demás comprobantes de compra, así como el avalúo del software que se maneja en la empresa, tanto el software adquirido como el propietario o desarrollado por la misma empresa. La relación de costos en el software no siempre se lleva a cabo con referencia a sus costos de adquisición o de desarrollo, sino

que también se toma en cuenta su peso específico en el correcto funcionamiento de la empresa.

La manera de presentar este reporte, desde el área de TI, debe ser con gráficas y cifras concretas para que la dirección no tenga dudas en la implantación de las políticas de seguridad, ya que de este análisis depende, en muchas ocasiones, la aprobación o rechazo de las propuestas de TI (DSI, 2008).

4.4.3 Beneficios de la administración de la seguridad

La administración es una parte fundamental de la seguridad informática y de los análisis de riesgo. Dicha administración ayuda a ubicar los puntos más débiles de los procesos críticos de la organización, los cuales estén directamente relacionados con las TI.

Una de las características más útiles de la administración de la seguridad es la auto supervisión, lo que proporciona información de cuándo es necesaria la implementación de nuevos esquemas de recuperación de desastres, nuevas políticas de seguridad, entre otras.

En resumen, la administración de los riesgos proporciona una perspectiva distinta a la misma problemática de la seguridad informática, con la diferencia de que esta cuenta con un enfoque menos técnico y más regulador, lo cual ayuda a las empresas a aterrizar todo lo que se planee desde el punto de vista tecnológico.

4.4.4 Prevención y recuperación de incidentes

Las funciones por las que existen estos planes de contingencia son para prevenir errores, fatalidades y facilitar la toma de decisiones en los momentos cuando la empresa se encuentra en una emergencia, ya sea por un fenómeno de carácter natural o de cualquier otra índole.

La preservación de la información vital para el funcionamiento de la empresa es la principal preocupación de un plan de prevención y recuperación de incidentes. Esto no quiere decir que no se vele por la seguridad del personal, pero al final estas políticas deben estar diseñadas para la preservación de funciones y la optimización de procedimientos.

Un esquema general de recuperación de incidentes debe tomar en cuenta los siguientes puntos:

- ✓ Diseñar un plan de recuperación de incidentes
- ✓ Determinar las prioridades en situaciones de emergencia
- ✓ Establecer un centro de mando
- ✓ Establecer sitios alternos y cómo llegar a ellos
- ✓ Mantener la información esencial

- ✓ Establecer el equipo de gestión de incidentes
- ✓ Establecer los equipos de respuesta a incidentes.

Está de sobra mencionar que el centro de mando, así como los sitios alternos deben estar separados a una distancia considerable de las oficinas principales, para poder prevenir eventos naturales y algunos otros socio-políticos, como manifestaciones en las calles, huelgas, etcétera.

El respaldo de la información debe realizarse de manera remota, de preferencia en otra región del país o del mundo.

Previo a toda contingencia debe haberse definido un grupo de personas responsables del control y manejo del programa de recuperación de incidentes, el cual controlaría las funciones de los equipos de respuesta y coordinaría los esfuerzos para la pronta recuperación de las funciones básicas de la empresa.

Como recomendación, se mencionan las siguientes prioridades para el procedimiento planteado:

- ✓ Preservar vidas humanas
- ✓ Recuperación de información sensible
- ✓ Preservar equipos

- ✓ Poner en producción la información sensible
- ✓ Cuidar la imagen de la empresa
- ✓ Recuperación de información general
- ✓ Tomar medidas legales.

Como parte del proceso de prevención de incidentes, se debe contar con procesos administrativos que garanticen la actualización continua de los planes de contingencia, así como el aseguramiento del funcionamiento correcto de los planes en caso de requerir su ejecución (DSI, 2008).

5. Conclusiones

La seguridad informática es de vital importancia en la operación correcta de las empresas de hoy en día, y dicha seguridad se implementa utilizando técnicas de última generación, así como técnicas tan antiguas como los imperios de la historia antigua. Esto lleva a reflexionar acerca de los conceptos que se llegan a tener con respecto del uso de las últimas tecnologías.

Todo empresario dueño de una empresa, de cualquier tamaño, que requiera en algún grado la implementación de seguridad informática debe ser consciente de todo lo que aquí se ha planteado y debe poder discernir por si mismo las necesidades de la empresa y deseos personales. Los deseos deben estar plasmados en la misión de la empresa, y no ser una serie de argumentos informales.

Por lo que se concluye que si es posible garantizar la implementación de un esquema robusto y eficiente en las empresas, siempre y cuando se tomen en cuenta los siguientes dos aspectos:

1ro.- Se debe contar con personal capacitado para el mantenimiento y operación de los equipos.

2do.- Deben tomarse en cuenta las buenas prácticas de la seguridad (punto 5.1), y la correcta identificación de las características de la empresa y su correlación con las recomendaciones establecidas en el punto 5.2.

5.1 Buenas prácticas

Este término es adoptado en el medio de la seguridad como la guía o lineamientos que pasaron de ser recomendaciones verbales hacia algo por escrito y más formal, con base al conocimiento de las causas que pueden originar violaciones a la seguridad de las empresas o información personal. Muchas de ellas se han convertido en rutina para las personas que tienen un contacto continuo con computadoras, tales como el uso de contraseñas, bloquear la sesión cuando se alejan de la computadora, no compartir información sensible, entre otras.

Aún cuando ya se tienen mejores conocimientos de lo que se requiere para mantener la información segura, es necesario plasmar por escrito cuales son las recomendaciones básicas que se deben seguir.

- ✓ Uso de contraseñas siempre que se pueda
- ✓ Combinar al menos dos autenticaciones para el control de acceso siempre que sea posible

- ✓ La información se debe proteger dentro y fuera de la empresa
- ✓ En caso de resguardo de un perímetro, siempre procurar que las instalaciones estén adecuadas o hechas con el propósito de proteger el interior
- ✓ Nunca perder de vista el beneficio que se debe esperar de toda inversión económica
- ✓ Tener en todo momento un respaldo jurídico de cada movimiento realizado, como la adquisición y préstamo de equipo de cómputo para el personal de la empresa
- ✓ Tener particular cuidado con la información que sale de la empresa, para evitar que sea compartida indeseadamente o robada
- ✓ Una vez cubiertos las necesidades básicas de la seguridad, asegurarse que la gestión remota de los equipos sea la necesaria para el aseguramiento de la información
- ✓ En la gestión remota, siempre se debe cifrar la información
- ✓ Debe mantenerse un buen control de la parte administrativa, como son comprobantes de compra, documentaciones, memorias técnicas, etcétera.

Entiéndase nuevamente, que las buenas prácticas propuestas en este documento no deben ser interpretadas como las únicas ni las que le convengan a uno y otro caso particular, sino que deben servir como

guía para el planteamiento de las prácticas que mejor convengan a cada situación, y deben basarse exclusivamente en los conocimientos que se tengan en materia de seguridad y seguridad informática.

5.2 Resultados obtenidos

Para un mejor entendimiento de la relación que tienen las necesidades de la empresa con respecto a las implementaciones para una gestión remota segura, a continuación se presenta una tabla en la cual se ilustran en relación cruzada, las recomendaciones en función de lo que se tiene y el tipo de empresa en la que se está trabajando.

Para un mejor entendimiento, las empresas se dividieron en 5 tipos, dependiendo del tamaño de su infraestructura de TI y el personal con que se cuenta para su mantenimiento y gestión. Esto se ejemplifica en la (Tabla 5.1).

Tabla 5.1 Categorías de Infraestructura de red (CI)

Personal / Servidores	1 a 2	3 a 8	9 a 15	16 a 40	>40
1 a 2	A				
3 a 10	A	B			
10 a 20	C	B	C		
21 a 40		D	C	D	
>40			E	D	E

Una vez ubicada la categoría de la empresa, es necesario saber las necesidades de la misma conforme a la (Tabla 5.2), las cuales se clasifican de manera similar a la infraestructura. En esta tabla se está en función de la clasificación de la empresa con respecto a su información.

Tabla 5.2 Clasificación de las Necesidades de las Empresas (CNE)

Empresa / Información	micro	pequeña	mediana	grande	gobierno
pública	nula	baja	baja	media	media
privada	baja	media	media	alta	alta
clasificada	baja	media	alta	alta	completa
secreta	media	alta	alta	completa	completa

Se debe tener bien acotada la clasificación de la información. Aquí se propone una clasificación de cuatro categorías (pública, privada, clasificada y secreta), las cuales definen la secrecía de la información en cuestión. En la (Tabla 5.3) se puede observar una propuesta para la clasificar de manera sencilla el nivel de seguridad requerida para la información a proteger. Se debe dar valor de una unidad a cada atributo de la información, y dependiendo del número de atributos que se le afecte, entonces se tendrá el nivel de clasificación de la información.

En este momento, y una vez que se tienen clasificadas tanto las necesidades como la infraestructura, es necesario triangular los resultados en otra tabla, para poder entonces establecer las recomendaciones concluyentes de este documento.

Tabla 5.3 Clasificación de la información

	Información
Confidencialidad	
Autenticación	
Integridad	
Disponibilidad	
Total:	

Tabla 5.4 Recomendaciones según clasificación de CI y CNE

CI\CNE	nula	baja	media	alta	completa
A	1	2	3	4	5
B	2	3	4	5	6
C	3	4	5	6	7
D	4	5	6	7	8
E	5	6	7	8	9

En base a la (Tabla 5.4) se presentan las siguientes nueve recomendaciones las cuales se adecuan a cada caso, en función a la empresa.

Recomendación 1. Esta empresa requiere un nivel escaso de protección ya que cuenta con una infraestructura pequeña y personal limitado, además de que la información que maneja no es crítica. Es necesario garantizar al menos una comunicación de gestión protegida e integra, esto se puede lograr usando el SSH como protocolo; no se requiere nada más.

Recomendación 2. En este caso la empresa requiere un nivel mayor de seguridad. Es recomendable que se considere un control de acceso físico básico (una sola autenticación), y seguridad aplicada en los protocolos de gestión, tal como el SSH y SFTP son necesarios. Aun puede considerarse que el acceso remoto al servidor no necesita más

que una contraseña y dicha contraseña podría o no ser administrada por el mismo administrador del equipo.

Recomendación 3. Las condiciones de este escenario requieren un control de acceso físico básico, y la misma protección para los protocolos de gestión remota que en la recomendación 2. Las contraseñas de los equipos así como la administración de control de acceso físico ya deben ser gestionadas por una tercera entidad, la cual debe vigilar y controlar el uso de los accesos, así como las actividades que se realicen con ellos. Las contraseñas de acceso remoto deben ser seguras a un nivel medio.

Recomendación 4. El control de acceso debe validar la identidad con al menos dos identificadores, los accesos remotos deben ser renovados periódicamente. Se recomienda el uso de certificados personales en los correos electrónicos y todo protocolo de gestión debe ser cifrado. La red interna debe protegerse, bloqueando contenido no requerido para la función de la empresa, tal como bloqueo de puertos de mensajería instantánea. Se recomienda la implementación de redundancias en los servidores críticos.

Recomendación 5. Este escenario es particular por la peculiaridad de englobar los casos cuando la empresa tiene una infraestructura pequeña, pero requieren un nivel de seguridad completa, así como el caso contrario donde la empresa no requiere una seguridad rigurosa, pero cuentan con una infraestructura grande. Para este caso se

recomienda que se fortalezca el control de acceso, requiriendo al menos dos validaciones de identidad, y a su vez el control de acceso remoto requiere que las contraseñas sean complejas y que la entidad de gestión de contraseñas las renueve periódicamente. Las firmas digitales y certificados en los correos y en las comunicaciones remotas deben considerarse como opción. La red interna debe aislarse completamente de la red pública. Solo los puertos de gestión deben estar abiertos. La redundancia en los servidores se vuelve indispensable junto con el balanceo de carga. Los servidores deben tener obligatoriamente respaldo de energía eléctrica.

Recomendación 6. Las firmas digitales y certificados personales deben implementarse y el uso de servicio pagado de vigilancia se considera recomendado. Los equipos deben contar con sistemas de alarmas y por consiguiente, un sistema de servidores para gestión de alarmas debe ser implementado. Se requiere que el soporte de TI esté disponible las 24 horas al día. Es altamente recomendado que existan equipos especializados dentro del personal de TI para la gestión de los servidores. El respaldo de energía eléctrica para los servidores debe ser por medio de UPS y líneas de alimentación alternas.

Recomendación 7. El control de acceso debe ser riguroso y debe incluir el resguardo de la documentación de operación, tales como memorias técnicas, planes de aceptación, etcétera. La redundancia se recomienda que ya sea en sitios geográficos distintos y que los enlaces de comunicación sean igualmente redundantes. Es requerida la

operación de varios equipos para coordinarse mutuamente, como personal administrativo, de operación y mantenimiento, y de ejecución. Los servidores deben tener implementados un control de las computadoras que deben ser capaces de conectarse hacia ellos.

Recomendación 8. El control de acceso físico tiene que ser total y la utilización de profesionales de la seguridad física se vuelve una necesidad absoluta. Las contraseñas de acceso remoto deben ser cambiadas en cada ocasión (contraseñas Token), y la implementación de certificados para la comunicación SSH es recomendada. El acceso a los servidores debe ser implementado a través de nodos especializados para la gestión, es decir, servidores dedicados a servir de intermediarios en la comunicación de administración. La asignación y acceso de VLANs dentro de la red de datos deben ser controlados por sistemas de administración de acceso. La certificación en estándares internacionales debe ser considerada. Debe haber equipos especializados para el cifrado de la información dentro de la red de gestión.

Recomendación 9. La seguridad completa requiere que el control de acceso físico sea total y que las contraseñas hacia los nodos de acceso se renueven con cada uso. Los servidores de gestión deben manejar certificados para el acceso a los demás equipos. Todo servidor debe constar de sistemas alternos de acceso remoto para casos de emergencias. La empresa debe certificarse y constar con recursos humanos especializados en la supervisión en el cumplimiento de los

estándares y que su utilidad real esté siendo implementada correctamente.

Bibliografía

Diffie Hellman. (2009). *Diffie Hellman Algorithm*. Retrieved Enero 08, 2010, from http://www.diffiehellman.com/

A, U. (2009, Noviembre 13). *Documentación de Ubuntu GNU/Linux*. Retrieved Noviembre 29, 2009, from doc.ubuntu.com: http://doc.ubuntu-es.org/Sobre_Ubuntu

ALEGSA. (1998). *Diccionario Informático.* Retrieved 01 05, 2010, from http://www.alegsa.com.ar/Dic/servidor.php

CC. (2009). *Common Criteria*. Retrieved Enero 02, 2010, from http://www.commoncriteriaportal.org/

CERT. (2010). *Equipo de Respuesta a Incidentes de Seguridad en Cómputo.* Retrieved Enero 13, 2010, from Computer Emergency Response Team: http://www.cert.org.mx/index.html

CINVESTAV. (2005, Octubre 22). *Firma Digital.* Retrieved Diciembre 17, 2009, from http://computacion.cs.cinvestav.mx/~jjangel/todos/firma_digital.pdf

CISCO SYSTEMS. (1999, Julio). *Internetworking Technology Handbook.* Retrieved 01 10, 2010, from CISCO SYSTEMS Inc.: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html

CSICE. (1998). *Portal del departamento de Tratamiento de la información y codificación*. Retrieved Diciembre 16, 2009, from Centro Superior de Investigaciones Científicas de España; Marañón, Gonzalo Álvarez: http://www.iec.csic.es/CRIPTonOMICon/ssl.html

DGSCA. (2008, Noviembre 17). *Enterate en linea UNAM*. Retrieved Diciembre 17, 2009, from http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm

DSI. (2008). Diplomado en Seguridad de la Información DGSCA, UNAM. Distrito Federal, México.

ESET. (2010). *ESET - Técnicas y amenazas informáticas*. Retrieved Enero 10, 2010, from http://www.eset-la.com/centro-amenazas/2225-ataques-multi-stage

Fedora. (2010). *Fedora Project*. Retrieved Enero 15, 2010, from http://fedoraproject.org/es/

Fernández, M. (2008, Octubre 11). *Wikipedia migra a Ubuntu Server*. Retrieved Nov 20, 2009, from http://tecnoticias.info/noticias-de-la-red/tecnologias-y-la-web/wikipedia-migra-a-ubuntu-server.html

Firewall. (2009). *Wikipedia*. Retrieved Enero 08, 2010, from http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29

FIRST. (2009). *Forum for Incident Response and Security Teams – Foro para Respuesta a Incidentes y Equipos de Seguridad.* Retrieved Enero 20, 2010, from http://www.first.org/

IDG COMMUNICATIONS. (2010). *¿Que es el balanceo de carga?* Retrieved 02 15, 2010, from http://www.idg.es/computerworld/%C2%BFQue-es-el-balanceo-de-carga?/seccion-ges/articulo-111063

IEEE. (2009). *IEEE 802.11 WIRELESS LOCAL AREA NETWORKS*. Retrieved Enero 19, 2010, from http://www.ieee802.org/11/

IPSec. (2006). *IPSec - Como*. Retrieved Diciembre 20, 2009, from http://www.ipsec-howto.org/spanish/x161.html

ISACA. (2010). *ISACA - COBIT*. Retrieved Enero 10, 2010, from http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

ISO. (2005). *El Portal de ISO 27001 en Español*. Retrieved Enero 10, 2010, from http://www.iso27000.es/

Linux Online Inc. (2010, Enero 18). *Linux Online.* Retrieved Enero 20, 2010, from http://www.linux.org/

Microsoft A. (2009). *Windows Server 2008 R2*. Retrieved Diciembre 07, 2009, from Microsoft Inc.: http://www.microsoft.com/windowsserver2008/en/us/default.aspx

Microsoft B. (2007, Septiembre 24). *Microsoft Windows Server 2008 System Requirements*. Retrieved Diciembre 7, 2009, from Microsoft Co.: http://msdn.microsoft.com/en-us/windowsserver/cc196364.aspx

Microsoft C. (2009). *IPSec desde Windows*. Retrieved Diciembre 16, 2009, from Microsoft Co: http://support.microsoft.com/kb/254949/es

NIST. (2010, Enero 15). *National Institute of Standards and Technology.* Retrieved Enero 15, 2010, from Instituto Nacional de Estándares y Tecnología: http://www.nist.gov/index.html

NWG BBN. (1998, Noviembre). *The Internet Engineering Task Force (IETF).* Retrieved Diciembre 16, 2009, from Network Working Group BBN Corp: http://www.ietf.org/rfc/rfc2401.txt

OpenSSH. (2009, Noviembre 19). *OpenSSH.* Retrieved Diciembre 17, 2009, from http://www.openssh.com/

Programación en castellano. (2010). *Java en Castellano.* Retrieved Enero 07, 2010, from BEA Weblogic: http://www.programacion.com/java/tutorial/beaintro/8/

Real Academia de la Lengua Española. (2001). *Real Academia Española.* Retrieved 01 10, 2010, from http://www.rae.es/rae.html

Red Hat. (2010). *Red Hat*. Retrieved Enero 15, 2010, from http://www.redhat.com/

Sun. (2009). *Solaris Operating - System Requirements*. Retrieved Diciembre 7, 2009, from Sun Microsystems Inc.: http://www.sun.com/software/solaris/specs.jsp

Sun. (2004, Agosto). *Sun Microsystems Inc.* Retrieved Diicembre 5, 2009, from http://dlc.sun.com/pdf/817-0574-12/817-0574-12.pdf

SuSE. (2010). *openSUSE*. Retrieved Enero 15, 2010, from http://es.opensuse.org/

Telnet. (2009). *Telnet.org*. Retrieved Diciembre 13, 2009, from http://www.telnet.org/

The Open Group. (2009, Agosto 15). *The Open Group.* Retrieved Enero 03, 2010, from http://www.unix.org/

The Open Group. (2009, Agosto 15). *The Open Group*. Retrieved 12 5, 2009, from The Unix system home page: http://www.unix.org/version3/unix03.html

Ubuntu. (2009a, Noviembre 13). *Documentación de Ubuntu GNU/Linux*. Retrieved Noviembre 29, 2009, from doc.ubuntu.com: http://doc.ubuntu-es.org/Sobre_Ubuntu

Ubuntu. (2009b, Octubre 19). *Ubuntu System Requirements*. Retrieved Diciembre 7, 2009, from https://help.ubuntu.com/community/Installation/SystemRequirements

Verisign. (2009). *VeriSign Identity and Authentication Services*. Retrieved Diciembre 16, 2009, from Verisign Inc.: http://www.verisign.com/latinamerica/esp/authentication/index.html

Wikipedia. (2009, Octubre 29). *Historia de Windows*. Retrieved Noviembre 20, 2009, from Windows Server 2008: http://es.wikipedia.org/wiki/Windows_Server_2008