CAPITULO II

SEGURIDAD INFORMATICA

2.1 INTRODUCCION

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde su aparición, y más aún desde la globalización de la Internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y más empresas sienten la necesidad de conectarse a este mundo.

La información es un valor clave para cualquier institución ya sea pública o privada. La carencia de información o una información defectuosa pueden llevar a la empresa a su ruina. Para que la empresa tenga éxito debe tener una información de calidad.

Una información es de calidad, cuando satisface los requerimientos que la gestión de la empresa le pide, como son:

La integridad.
La disponibilidad.
La confidencialidad.

2.2 OBJETIVO DE LA SEGURIDAD DE LA INFORMACIÓN

El objetivo de la seguridad es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, así como tratando de proteger las redes privadas y sus recursos mientras se mantienen los beneficios de la conexión a una red pública o a una red privada.

Seguridad de la información en redes es mantener bajo protección los recursos y la información involucradas en la red, a través de procedimientos basados en políticas y sistemas de seguridad tales que permitan el completo control del sistema.

Dentro del concepto de seguridad debemos distinguir lo que se refiere a la seguridad física, para tener un concepto mas claro se detalla la misma a continuación.

2.3 PROPIEDADES DE LA SEGURIDAD INFORMATICA

La seguridad informática debe vigilar principalmente las siguientes propiedades:

- **Integridad,** la información debe ser consistente, fiable y no propensa a alteraciones no deseadas.
- **Disponibilidad,** la información debe estar en el momento que el usuario requiera de ella.
- **Autentificación**, verificar la identidad del emisor y del receptor.

- **Privacidad**, la información debe ser vista solo por personas autorizadas a ello.

2.4 CLASIFICACION DE LOS FACTORES QUE INTERVIENEN EN LA SEGURIDAD

La seguridad en un sistema está determinada por:

2.4.1 El factor Organizacional

Usuarios

- Tipo de usuarios que se tienen.
- Reglamentos y políticas que rigen su comportamiento.
- Vigilar que esos reglamentos y políticas se cumplan, y no queden sólo en papel.

La alta dirección

- Inversión en capacitación de los administradores.
- Apoyo económico orientado a la adquisición de tecnología de seguridad.
- Negociar acuerdos de soporte técnico con los proveedores de equipo.

2.4.2 El factor Software

La aplicación

- Vigilar que tenga mecanismos para control de acceso integrados.
- Observar las facilidades de respaldo de información que se tienen.
- Establecer que tan crítica es la aplicación y desprender su disponibilidad.

El Sistema Operativo

- Mostrar preferencias por los sistemas abiertos (UNIX).
- Vigilar que soporte estándares de seguridad como C2.
- Observar las recomendaciones del fabricante y aplicar los parches que libere.
- Vigilar siempre las bitácoras.
- Mantenerse informado sobre las alertas de seguridad.

Software de red

- Vigilar de cerca las estadísticas de acceso y tráficos de la red.
- Procurar implementar cortafuegos (firewalls), pero no confiar en ellos.
- En la medida de lo posible, apoyar las conexiones cifradas.

2.4.3 El factor hardware

Hardware de red.

- Elegir adecuadamente el tipo de tecnología de transporte (ethernet, FDDI, etc.).
- Proteger muy bien el cableado, las antenas y cualquier dispositivo de red.
- Proporcionar periódicamente mantenimiento a las instalaciones

Servidores

- Mantenerlos en condiciones de humedad y temperatura adecuadas.
- Establecer políticas de acceso físico al servidor.
- El mantenimiento también es importante aquí.

2.5 BENEFICIOS DE UN SISTEMA DE SEGURIDAD

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- 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.
- Mejora de los climas laborales para los RR.HH.

2.6 TIPOS DE ATAQUES O AMENAZAS

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Las cuatro categorías generales de amenazas o ataques son las siguientes :

- **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.
- **Intercepción*:*** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador.
- **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.
- **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

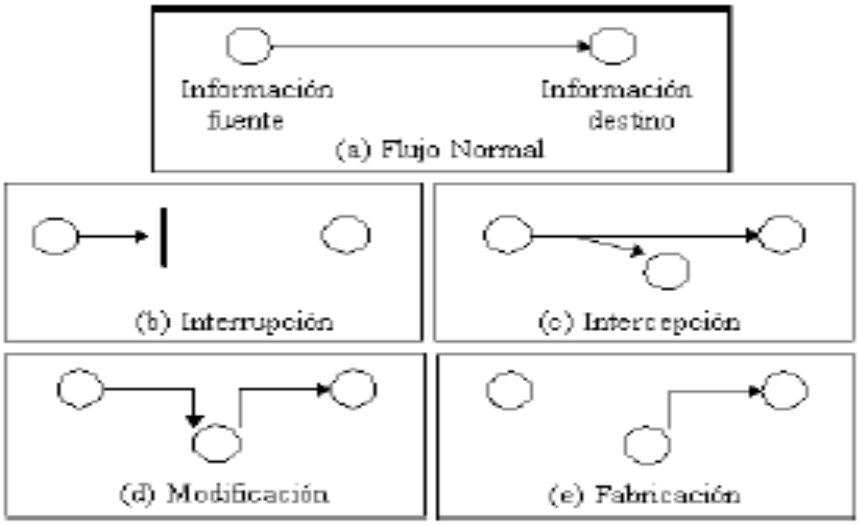

GRAFICO # 2. TIPOS DE ATAQUES Y AMENAZAS

La identificación de las vulnerabilidades permite conocer los tipos de ataque que podrían ser efectuados, así como también sus consecuencias. Se realizará una descripción general de los principales tipos de ataque.

2.6.1 Ingeniería social

Consiste en persuadir a los usuarios para que ejecuten acciones o revelen la información para superar las barreras de seguridad.

2.6.2 Cracking de contraseñas.

Existen dos métodos:

- **Diccionario**: consiste en efectuar encriptaciones de palabras (posibles claves) y comparar estas encriptaciones con el original.
- **Fuerza Bruta**: consiste en realizar todas las combinaciones posibles de un conjunto de caracteres. En el siguiente cuadro se ve el tiempo de búsqueda de una contraseña de acuerdo a la longitud y tipo de caracteres utilizados.

Long. En caracteres	**26 (letras minúsculas)**	**36 (letras y dígitos)**	**52 (letras mayúsculas y minúsculas)**	96 (Todos los caracteres)
6	50 min.	6 horas	2.2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10.5 meses	17 años	219 años
9	21 meses	32.6 años	881 años	2287 años
10	45 años	1159 años	45838 años	21 millones años

TABLA # 3. TIEMPO PARA HALLAR UNA CLAVE VÁLIDA (100.000 CLAVES POR SEGUNDO).

2.6.3 Escaneo de puertos

Existen herramientas para verificar los servicios que presta una máquina por medio de la revisión de los puertos abiertos.

2.6.4 Sniffers y escuchas electrónicas.

La mayoría de ataques que se realizan a servidores de aplicaciones web por lo general solo se limitan dañar o modificar su página web, literalmente se podía decir que este es lo peor que se puede hacer en contra de un servidor, pero la verdad es diferente.

De hecho aunque estos ataques pueden parecer dramáticos y suelen generar grandes titulares, no son nada si se los compara con un ataque real. Los intrusos reales no suelen anunciar su presencia, ni hacen alarde de lo que consiguen, sino que instalan dispositivos de monitorización ocultos que recogen la información de la red. Los distintos sniffers realizan tareas diferentes, que oscilan entre las sencillas (capturar nombres y contraseñas) y las extremas grabar todo el trafico de red.

2.6.4.1 Riesgos que conllevan los sniffers.

Los sniffers representan un alto nivel de riesgo, ya que:

- Pueden capturar contraseñas.
- Pueden capturar información confidencial o patentada.
- Pueden utilizarse para hacer mella en la seguridad de los entornos de red o para obtener acceso por la fuerza.

De hecho los ataques de sniffers han provocado daños más serios que cualquier otro tipo de ataque.

Pero no todo lo referente a los sniffers es malo; por una parte, es aconsejable explotar su valor, ya que los sniffers son herramientas indispensables para diagnosticar problemas de red o para estar al tanto de las acciones de los usuarios. Pero por otra parte, es necesario emplear todos los medios posibles para asegurarse que determinados usuarios no instalen sniffers en las unidades.

2.6.5 Spoofing

El Spoofing tradicional se produce cuando los atacantes autentifican una máquina con otra mediante la falsificación de paquetes de un host en el que se confía. En estos últimos años, esta definición se ha ampliado para abarcar todos los métodos de modificación en las relaciones de confianza o en la autentificación basándose en las relaciones de confianza o en la autentificación basándose en direcciones o en nombres de hosts.

2.7 POLITICAS DE SEGURIDAD INFORMATICA.

El objetivo de desarrollar una política de seguridad informática, es definir las expectativas de una institución respecto al uso adecuado de los ordenadores y de la red, así como definir los procedimientos precisos para prevenir y responder a los incidentes de seguridad.

2.7.1 Definición de una política aceptable.

Las herramientas y aplicaciones forman la base técnica de la política de seguridad, pero la política de uso aceptable debe considerar otros aspectos:

- ¿Quién tiene permiso para usar los recursos?
- ¿Quién esta autorizado a conceder acceso y aprobar los usos?
- ¿Quién tiene privilegios de administración del sistema?
- ¿Qué hacer con la información confidencial?
- ¿Cuáles son los derechos y responsabilidades de los usuarios?

Por ejemplo, al definir los derechos y responsabilidades de los usuarios:

- Si los usuarios están restringidos, y cuáles son sus restricciones.
- Si los usuarios pueden compartir cuentas o dejar que otros usuarios utilicen sus cuentas.
- Cómo deberían mantener sus contraseñas los usuarios.
- Con qué frecuencia deben cambiar sus contraseñas.
- Si se facilitan copias de seguridad o los usuarios deben realizar las suyas.

Para poder entrar en un recinto, leer unos datos y modificar un registro, etc, será necesario saber de quien se trata y si el sujeto está autorizado. Por lo tanto será preciso identificar al sujeto (identificación) de forma totalmente fiable (autentificación o verificación), y consultar un archivo, base de datos y/o algoritmo

que nos diga si el sujeto tiene o no, autorización para realizar la acción demandada (autorización).

2.7.2 La política en el correo electrónico.

Las organizaciones deben preparar una política clara con respecto al uso de correo electrónico, incluyendo:

- Ataques en el correo electrónico; intercepción, virus.
- Protección de ataduras al correo electrónico.
- Pautas de cuando no usar el correo electrónico.
- La responsabilidad del empleado para no comprometer a la compañía; enviando correo electrónico difamatorio, usado para compra desautorizada.
- El uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos.
- Retención de mensajes que, si guardó, podría descubrirse en caso de litigación.
- Controles adicionales para verificar mensajes que no están autorizados.

2.7.3 Mecanismos de seguridad.

Para implementar estas políticas de seguridad se utiliza, lo que comúnmente se conoce como mecanismos de seguridad.

Los mecanismos de seguridad se dividen en tres grupos:

- **Prevención**: aquellos que aumentan la seguridad de un sistema durante su funcionamiento normal.
- **Detección**: aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.
- **Recuperación**: aquellos que se aplican cuando el sistema ha sido atacado.

En esta investigación se trata un mecanismo de prevención en particular como es el cifrado.

2.8 NIVELES DE SEGURIDAD.

En la actualidad se han establecido diferentes niveles de seguridad, establecidos por la ISO en función al grado de importancia de la información que se quiere proteger. Estas especificaciones definen siete niveles de seguridad, denominadas A1, B3, B2, B1, C2, C1, D. Siendo el D de menor seguridad y A1 de mayor. Cada nivel incluye las exigencias de los niveles inferiores.

Nivel D. Estos sistemas tienen exigencias de seguridad mínimos, no se les exige nada en particular para ser considerados de clase D.

Nivel C1. Para que un sistema sea considerado C1 tiene que permitir la separación entre datos y usuarios, debe permitirse a un usuario limitar el acceso a determinados datos, y los usuarios tienen que identificarse y validarse para ser admitidos en el sistema.

Nivel C2. Para que un sistema sea de tipo C2 los usuarios tienen que poder admitir o denegar el acceso a datos a usuarios en concreto, debe de llegar una auditoria de accesos, e intentos fallidos de acceso a objetos (archivos, etc.), y también especifica que los procesos no dejen residuos (datos dejados en registros, memoria o disco por un proceso al terminar su ejcución).

Nivel B1. A un sistema de nivel B1 se le exige control de acceso obligatorio, cada objeto del sistema (usuario o dato) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nominas, ventas, etc.).

Nivel B2. Un sistema de nivel B2 debe tener un modelo teórico de seguridad verificable, ha de existir un usuario con los privilegios necesarios para implementar las políticas de control, y este usuario tiene que ser distinto del administrador del sistema (encargado del funcionamiento general del sistema). Los canales de entrada y salida de datos tienen que estar restringidos, para evitar fugas de datos o la introducción de estos.

Nivel B3. En el nivel B3 tiene que existir un argumento convincente de que el sistema es seguro, ha de poderse definir la protección para cada objeto (usuario o dato), objetos permitidos y cuales no, y el nivel de acceso permitido a cada cual. Tiene que existir un

“monitor de referencia” que reciba las peticiones de acceso de cada usuario y las permita o las deniegue según las políticas de acceso que se hayan definido.

El sistema debe ser muy resistente a la penetración de intrusos, así como tener una auditoria que permita detectar posibles violaciones de la seguridad.

Nivel A1. Los sistemas de nivel A1 deben cumplir los mismos requerimientos que los de nivel B3, pero debe ser comprobado formalmente el modelo de seguridad definido en el nivel B1.

2.9 ETAPAS PARA IMPLEMENTAR UN NIVEL DE SEGURIDAD.

Para implementar un sistema de seguridad, y los elementos que componen este sistema empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

- Introducir el tema de seguridad en la visión de la empresa.
- Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
- Capacitar a los gerentes y directivos, contemplando el enfoque global.
- Designar y capacitar supervisores de área.
- Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
- Mejorar las comunicaciones internas.

- Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
- Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

2.10 SEGURIDAD FÍSICA.

Los dos aspectos más importantes son: el lugar en que se encuentra ubicado el servidor y las personas que tienen acceso físico al mismo. Los controles de seguridad son inútiles si usuarios malintencionados tienen acceso al servidor.

El centro de operaciones de red es un área restringida donde se encuentran los servidores. Idealmente un centro de operaciones de red debería ser una oficina independiente a la que tuviesen acceso muy pocas personas. Aquellas personas que estén autorizadas deberían tener claves o en su defecto tarjetas de acceso que incluso restringen el acceso a usuarios autorizados a ciertas horas del día. Por ultimo, merece la pena llevar un registro escrito de acceso y ordenar que incluso el personal autorizado firme al entrar y salir [19].

Además el centro de operaciones de red deberá cumplir con los siguientes requisitos:

Debe encontrarse dentro de otro espacio de la oficina y alejado del publico; es preferible que no se encuentre en la planta baja.

[19] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

- La sala y los pasillos que conducen a ella deben ser totalmente opacos: sin puertas de cristal [20].
- Las puertas de acceso deben tener un blindaje que incluya el cerco de la puerta. Esto evita que los intrusos fuercen la cerradura [21].
- Si se emplea vigilancia (circuito cerrado de TV o imágenes instantáneas secuenciales), dirija la señal desde la cámara a un VCR remoto. Esto le garantizará que aunque los ladrones dañen el equipo y se lleven la cinta, seguirá teniendo pruebas [22].
- Mantenga todos los dispositivos de almacenamiento en un lugar seguro, o aun mejor, en un lugar distinto [23].

Suministro de energía para el hardware.

Es imprescindible el asegurar un suministro estable y continuo de energía eléctrica al hardware, utilizando normalmente UPS (Sistema de suministro ininterrumpido de energía) que regularán la tensión evitando los picos de voltaje que pueda traer la red y proporcionará un tiempo de autonomía por medo de baterías en caso de cortes del suministro eléctrico.

[20] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002
[21] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002
[22] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002
[23] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

Control de temperatura y la humedad del entorno

Se aconseja siempre la instalación de dispositivos de control y monitorización de la temperatura y la humedad del entorno. El factor más crítico suele ser la temperatura, siendo la humedad un factor secundario sólo a tener en cuenta en climas determinados.

Lo correcto sería en la mayoría de los casos, el tener una adecuada ventilación en los centros en donde se alojen una considerable cantidad de equipo informático.

Será importante de considerar la instalación de equipo de monitoreo de temperatura, con la finalidad de mantener un control de la misma en la mayoría de los casos bastará con la instalación de termómetros electrónicos.

2.10.1 Medidas de seguridad para el hardware de red.

Para evitar poner en peligro el hardware de red, se emplearan algunos pasos de sentido común. Estos pasos serán suficientes, ya que los problemas de los puntos vulnerables de hardware de red no son habituales comparados con los de software.

En la mayoría de los casos, el riesgo del hardware de red se produce por errores del operador. Muchos usuarios no activan el cifrado o no definen contraseñas de administración, de mantenimiento o de los usuarios, lo que deja la configuración del hardware intacta, como salió de fábrica, y abre el sistema de ataques.

Se deberá también aislar el hardware de red de los usuarios locales en los que no confíe.

2.10.2 Contraseñas de BIOS y consola

La mayoría de arquitecturas como X86,PPC o Sparc utilizan contraseñas de BIOS-PROM, contraseñas de consola o de ambos tipos. Los fabricantes de hardware incluyen estos sistemas de contraseñas como una capa extra de seguridad.

Las contraseñas de la BIOS o de la PROM evitan que usuarios malintencionados accedan a la configuración de los sistemas, mientras que las contraseñas de consola protegen los perfiles de usuario de la estación de trabajo.

Sin embargo, no hay que olvidarse de establecer la contraseña de configuración y de usuario. Actualmente, las teclas y contraseñas predeterminadas de configuración de la BIOS de casi todos los fabricantes son muy conocidas.

Además se deberá asegurar de que la contraseña no coincida con otras que utilice en la red, lo que garantiza que si rompe la contraseña de la BIOS o de consola, las aplicaciones o otros servidores no estarán desprotegidas.

Cabe señalar que no se deberá confiar en las contraseñas de la BIOS y de consola ya que se puede anular la contraseña de la BIOS con solo provocar un cortocircuito en la batería de la CMOS; en otros casos ni siquiera necesitan hacerlo ya que el fabricante de la placa base incluye un jumper que colocado de modo adecuado borra la CMOS.

2.11 SEGURIDAD PARA LOS USUARIOS LINUX

2.11.1 Ataques a contraseñas

El término ataque a contraseña es un termino genérico. Describe diversas actividades entre las que se incluye cualquier acción dirigida a romper, descifrar o borrar contraseñas o a sortear de cualquier otra forma los mecanismos de seguridad de las contraseñas.

En orden jerárquico en cuanto a seguridad, los ataques a contraseñas son lo primero. De hecho, lo primero que aprenden los piratas e intrusos es como romper las contraseñas, principalmente porque exige una experiencia técnica mínima.

Actualmente, cualquiera puede romper contraseñas de Linux utilizando herramientas automatizadas. Sin embargo no debe confundirse la sencillez con la ineficacia. En la mayoría de los casos, una deficiente seguridad de las contraseñas

pone en peligro a todo el sistema. A menudo con ataques a contraseñas logran acceso como root y arrebatan el control de todo el servidor [24].

Para evitar este tipo de acceso se deberá implementar varias políticas así como herramientas que protejan las contraseñas de los servidores.

- Instalación del shadowing de contraseña.
- Refuerzo de contraseñas en aplicaciones de terceros.
- Refuerzo del sistema frente a ataques a contraseñas.
- Desarrollo de políticas efectivas de contraseñas.

2.11.2 Elección humana de contraseñas y seguridad del sistemas

El cifrado es un componente vital de la seguridad. Sin embargo por muy potente que sea nuestro cifrado, fallará si el usuario elige contraseñas débiles.

Generalmente los usuarios son propensos a ser olvidadizos, a menudo crean contraseñas a partir de los siguientes datos:

- Fecha de nacimiento.
- Numero de cédula.
- Nombres de los hijos.
- Nombres de sus artistas favoritos.

[24] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

- Palabras del diccionario.
- Secuencias numéricas como 123456.
- Palabras escritas al revés

Estas elecciones son terribles. Cualquier crack romperá este tipo de contraseñas en segundos. De hecho las buenas contraseñas son difíciles de conseguir incluso si se tienen conocimientos de cifrado.

Pero para evitar la creación de contraseñas incorrectas existe una técnica denominada Comprobación Proactiva de Contraseñas, con la cual se eliminan las contraseñas débiles antes del envío a la base de datos de las contraseñas.

El proceso se lo realiza de la siguiente forma:

Cuando un usuario crea una contraseña, ésta se compara en primer lugar con una lista de palabras y con una serie de reglas. Si la contraseña no cumple los requisitos de este proceso, se obliga al usuario a elegir otra [25].

En los ataques tradicionales a contraseña, los atacantes capturaban los archivos de contraseñas del sistema y utilizan utilidades de intrusos contra ellos, su meta principal es llegar al servidor como root, pero esto se puede eliminar con la utilización del shadowing [26].

[25] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002
[26] Fuente: Linux Maxima Seguridad Edición Especial, ANONIMO, Pearson Educación S.A. Madrid 2002

2.11.2.1 Uso de contraseñas

Los usuarios deben seguir una buena práctica en la selección y uso de las contraseñas.

Las contraseñas proporcionan un medio para validar la identidad de un usuario y así establecer acceso correcto al proceso de información o servicio. Todos los usuarios deben estar aconsejados a:

- Guardar las contraseñas confidencialmente.
- Evite guardar en papel el registro de contraseñas, a menos que esto pueda guardarse segura y firmemente.
- Cambie las contraseñas siempre que haya una indicación de un posible comprometimiento de la misma.
- Seleccione una contraseña selecta con un mínimo de longitud de seis caracteres que sean:

    - Fácil de recordar.
    - No comparta las contraseñas individuales de usuario.
    - No basada en nada que alguien más podría suponer fácilmente, o podría obtener usando la información de una persona relacionada, (nombres, número telefónico, etc.).
    - Evite caracteres consecutivos idénticos o grupos ya sea todo numérico o todo alfabético. Cambie las contraseñas en intervalos

regulares o basado en número de accesos (para las cuentas privilegiadas las contraseñas deben ser cambiadas con más frecuencia que las contraseñas normales); y evite el re uso de contraseñas viejas.

2.12 SEGURIDAD EN LA RED CON RED HAT LINUX.

2.12.1 Secure Socket Layer (SSL)

El protocolo SSL es un protocolo de capa que esta situado entre un protocolo de capa de red fiable orientado a una conexión como TCP / IP y el protocolo de la capa de aplicación como el HTTP. SSL proporciona una comunicación segura entre el cliente y el servidor permitiendo una autentificación mutua, el uso de firmas digitales para comprobar la integridad del mensaje y la encriptación para al integridad del mismo .

La capa de sockets seguros (SSL) es un método de tres niveles que utiliza RSA y autenticación y encriptación DES, así como comprobación MD5 adicional. Con estos métodos SSL, hace frente a los tres problemas inherentes en la comunicación basada en la Web [27]:

[27] Fuente: Guía Avanzada Firewalls Linux, ZIEGLER Robert, Prentice Hall Iberia, Madrid 2000

- En el momento de la comunicación, el cliente y el servidor definen e intercambian una clave secreta, que se utiliza para decodificar los datos en el transito. Por consiguiente aunque pueda rastrearse el tráfico SSL está encriptado y es difícil de descifrar [28].

- SSL soporta criptografía de clave pública, así que el servidor puede autentificar a los usuarios utilizando esquemas populares como RSA y el estándar de firma digital (Digital Signatura Standard, DDS) [29].

- El servidor puede verificar la integridad de sesiones en curso utilizando algoritmos de resumen de mensajes, como MD5 y SHA. De este modo SSL puede protegerse contra el secuestro de una sesión por parte de terceras personas [30].

SSL protege los datos por medio de dos capas y dos pasos. En la primera el cliente y el servidor realizan un protocolo de intercambio (similar al de TCP). Durante este proceso, intercambian claves y después establecen y sincronizan un estado criptográfico entre ellos. A continuación, SSL coge los datos de la aplicación (en la capa de registro) y los encripta; más tarde en el destino este proceso se ejecuta a la inversa

[28] Fuente: Guía Avanzada Firewalls Linux, ZIEGLER Robert, Prentice Hall Iberia, Madrid 2000
[29] Fuente: Guía Avanzada Firewalls Linux, ZIEGLER Robert, Prentice Hall Iberia, Madrid 2000
[30] Fuente: Guía Avanzada Firewalls Linux, ZIEGLER Robert, Prentice Hall Iberia, Madrid 2000

Estás características hacen de SSL una herramienta excelente para asegurar las transacciones de comercio electrónico entre un servidor que este bajo su control y clientes desconocidos.

2.12.2 Servidor Apache Seguro (HTTPS)

Se entiende por servidor seguro un servidor de paginas web que establece una conexión cifrada con el cliente que ha solicitado la conexión, de manera que nadie salvo el servidor y el cliente, puedan tener acceso a la información transmitida de forma útil. El uso de servidores seguros es un elemento imprescindible en todos aquellos servicios que utilicen información confidencial.

El servidor Apache HTTP con el módulo se seguridad mod_ssl activado para usar la librería y el conjunto de herramientas OpenSSL. La combinación de estos tres componentes, proporcionados con Red Hat Linux, se conoce como el Servidor Seguro Web o simplemente como el Servidor Seguro [31].

El módulo mod_ssl es un módulo de seguridad para el Servidor Apache HTTP.

[31] Fuente: http://www.europe.redhat.com/documentation

El módulo mod_ssl usa las herramientas proporcionadas por el Proyecto OpenSSL para añadir una característica muy importante al servidor Apache (http), la habilidad de tener comunicaciones encriptadas [32].

Al contraste, usando HTTP normal, las comunicaciones entre el navegador y el servidor Web son enviadas en texto plano, lo cual puede ser interceptado y leído por alguna persona no autorizada.

2.12.3 Controlando el acceso a archivos en el servidor.

Muchos sitios son interesantes en la limitación del escape de la información con su servidor web. Esto podría ser causado en un servidor web, cuando en una institución distribuye datos internamente, libros de teléfonos, datos externos, mucho tránsito de información. Para proveer estos requerimientos, muchos servidores Web tienen un sistema para restringir el acceso a documentos web.

Muchos servidores soportan dos técnicas para controlar el acceso a archivos y directorios:

- Acceso restringido a direcciones IP particulares, o dominios DNS.

[32] Fuente: http://www.europe.redhat.com/documentation

- Acceso restringido a usuarios particulares. Los usuarios son autenticados a través del uso de password que es almacenado en el servidor.

Los servidores que están equipados con software necesario para llaves públicas encriptadas, tienen una técnica para restringir el acceso:

Acceso restringido para usar llaves públicas que son firmadas por una autoridad con certificación apropiada.

Cada una de estas técnicas tiene ventajas y desventajas. La restricción para direcciones IP es relativamente simple dentro de la institución, aunque es una leve apertura para los ataques basados en "IP spoofing". Usando hostname, en cambio de la dirección IP, corremos el riesgo de ser engañados.

De estas tres técnicas el acceso restringido a personas quienes presentan propiamente firmas de certificados es probablemente la más segura.

2.12.4 Seguridad para un web site público.

El web site público tiene también el punto de entrada para violaciones en la red interna de la organización para propósitos de acceso confidencial de la información. Las prácticas recomendadas son diseñadas para ayudar a prevenir estos y otros daños con respecto a la seguridad.

Hay dos razones principales en la seguridad relacionada a la operación de un sitio web público:

La configuración u operación impropia del servidor web puede dar como resultado la revelación inadvertida de información confidencial.

El host usado por el servidor web puede estar expuesto

Para mejorar la seguridad del sitio web público, se recomienda 3 pasos.

- Selección del servidor y la tecnología del host
- Configuración del servidor y la tecnología fundamental del host
- Manejo del servidor.

Además, se recomienda que se establezcan políticas de seguridad que mantengan prácticas apropiadas para el administrador de red y los usuarios.

Área	**Practica recomendada**
Selección de la Tecnología del Servidor	1. Incluye los requerimientos de seguridad explícita cuando se selecciona el servidor y las tecnologías de host
Configuración de la tecnología del Servidor	2. Aislar el servidor Web de la red interna de la organización

	3. Mantener una copia autorizada del contenido del sitio Web en un Host más seguro. 4. Ofrecer solamente los servicios de red esenciales y los servicios de sistema operativo en el servidor. 5. Configurar el servidor Web para aumentar la seguridad. 6. Considerar la implicación de la seguridad cuando se escogen los programas externos que el servidor ejecutará.
Operación del servidor	7. Administrar el servidor Web de una manera segura. 8. Observar los cambios inesperados de directorios y archivos. 9. Inspeccionar sus sistemas y network logs.

TABLA # 4. REQUERIMIENTOS DE SEGURIDAD EXPLÍCITA CUANDO SE SELECCIONA EL SERVIDOR Y LAS TECNOLOGÍAS DE HOST

Los requerimientos de seguridad típicamente incluyen:

- La habilidad para restringir las actividades administrativas para usuarios autorizados solamente.
- La habilidad para denegar el acceso a la información de otros servidores.
- La habilidad para deshabilitar servicios de red innecesarios que puedan estar en el sistema operativo o el software del servidor.

Se puede realizar de la siguiente manera:

- Identificar tecnologías que satisfaga su funcionalidad, ejecución y requerimientos de seguridad.
- Estimar las diferencias de costo de apertura de tecnologías de competitividad, incluyendo los costos comerciales de incidentes potenciales de seguridad.
- Seleccionar la tecnología que ofrecerá el mejor balance de funcionalidad, ejecución, seguridad, y sobre todo costo.

2.12.5 Seguridad en el servidor de correo electrónico.

El correo electrónico en la Internet es un medio poco seguro y se presta a suplantación de personalidad, errores y manipulación no deseada, por lo cual; se debe tomar la firme determinación de enviar todos los mensajes de correo electrónico con firma digital, por ejemplo gnupg.

2.13 CRIPTOLOGIA

Las amenazas que sufre la información durante su proceso, almacenamiento y transmisión son crecientes y complejas. Para contrarrestarlas se han desarrollado numerosas medidas de protección, que se implementan en el equipo físico o lógico mediante los denominados mecanismos de seguridad.

De éstos, el mecanismo por excelencia es el de cifrado de la información. La Criptología se divide en dos ciencias importantes: la Criptografía y el Criptoanálisis. La Criptografía se puede traducir como " La forma de escribir de forma secreta " (krypto, escondido; graphia, escritura).

Es una ciencia que se ocupa principalmente de conseguir que nuestros mensajes sean comprensibles exclusivamente para aquellos que nosotros deseemos e ilegibles para el resto de la humanidad, aplicando para ello procedimientos matemáticos o claves. El texto inicial, el de partida, recibe el nombre de texto claro. El que resulta de aplicarle el algoritmo criptográfico, es el texto cifrado.

Históricamente los militares y los cuerpos diplomáticos han utilizado y han contribuido, de una manera importante, en el arte de la Criptología. Sin embargo, hoy en día su interés merece una atención especial para todos los sectores públicos o privados para los que la información es algo muy valioso.

Los sistemas de cifrado modernos se clasifican en:

- Simétricos o de clave secreta: la clave utilizada es la misma tanto para cifrar como para descifrar. El algoritmo debe ser público, pero la clave debe ser siempre secreta.
- Asimétricos o de clave pública: la clave para cifrar es pública y la de descifrar secreta, y están relacionadas entre sí. El algoritmo puede ser público o secreto. Cualquier persona que disponga de la clave pública puede cifrar el mensaje, pero solo el que ha generado las claves y tiene la clave secreta puede descifrar el mensaje.

No hay ningún algoritmo irrompible. El algoritmo puede ser más o menos duro. La dureza de un algoritmo se mide teniendo en cuenta su factor de trabajo, que es la cantidad necesaria de trabajo para descubrir las claves.

Dentro de la criptografía moderna, es decir, aquella en que los algoritmos operan en bits, dos son los algoritmos más conocidos y utilizados, el DES (Data Encryption Standard) y el RSA (Rivest, Shamir y Adleman). Las contraseñas de Linux se crean utilizando el algoritmo de cifrado DES

2.13.1 Firmas digitales

Una firma digital es un bloque de caracteres que acompaña a un documento, acreditando quien es su autor (autenticación) y que no ha existido manipulación de los datos (integridad).

El proceso de la firma digital lo realiza un software (por ejemplo PGP, gnupg) que aplica un algoritmo sobre el texto a firmar, obteniendo un extracto (número) de longitud fija, y único para ese mensaje. Este extracto cuya longitud oscila entre 176 y 160 bits se somete a continuación al cifrado (RSA o DSS) mediante la clave secreta del autor, previa petición de contraseña.

Para verificar la firma, el receptor descifra la firma con la clave pública del emisor, comprime con la función hash al texto original recibido y compara el resultado de la parte descifrada con la parte comprimida, si ambas coinciden el emisor tiene garantía de que el texto no ha sido modificado. Como el emisor utiliza su clave secreta para cifrar la parte comprimida del mensaje, puede probarse ante una tercera parte, que la firma sólo ha podido ser generada por el usuario que guarda la componente secreta.

2.13.1.1 Fundamentos teóricos de GNUPG

Desde su aparición en 1991,como PGP (Pretty Good Privacy) se ha convertido en una de las herramientas más utilizadas a nivel mundial para conseguir

privacidad y autenticación tanto en los mensajes de correo como en los archivos almacenados en el disco duro del ordenador. A ello ha contribuido indudablemente su distribución como herramienta gratuita, así como su puesta al día en las sucesivas versiones aparecidas mejorando los algoritmos criptográficos utilizados. El gnupg nos permite dos cosas:

Cifrar mensajes y archivos para que no resulten legibles sin nuestra autorización.

Firmarlos digitalmente para asegurarnos que no son modificados sin nuestro consentimiento.

2.13.1.2 Cifrado de mensajes

Para cifrar los mensajes y archivos, gnupg recurre al empleo de los dos tipos de cifrado existentes: simétrico y asimétrico. El cifrado convencional de clave única o cifrado simétrico utiliza la misma clave para cifrar y para descifrar.

Esto presenta el inconveniente de la distribución de esta clave a los receptores a través de un canal que consideramos inseguro. Este problema se soluciona con el cifrado de clave pública, que emplea dos claves distintas para el cifrado y el descifrado.

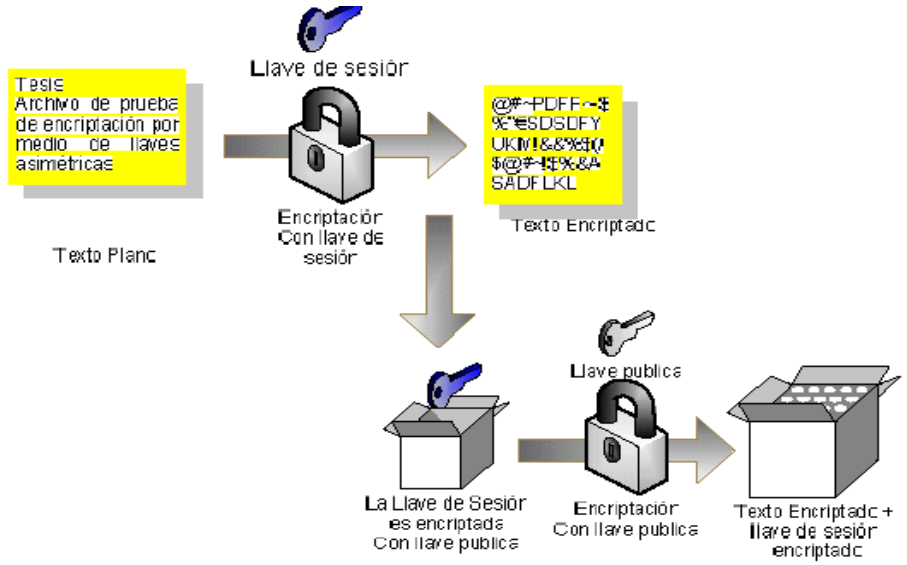

GRAFICO # 3. ENCRIPTANDO CON GNUPG

En el proceso de desencripción, se utiliza la llave privada para recobrar la llave de sesión temporal y gnupg utiliza esta llave única para desencriptar utilizando el método simétrico sobre el texto cifrado, dando como resultado una mejora en la velocidad y consumo de recursos de la encripción.

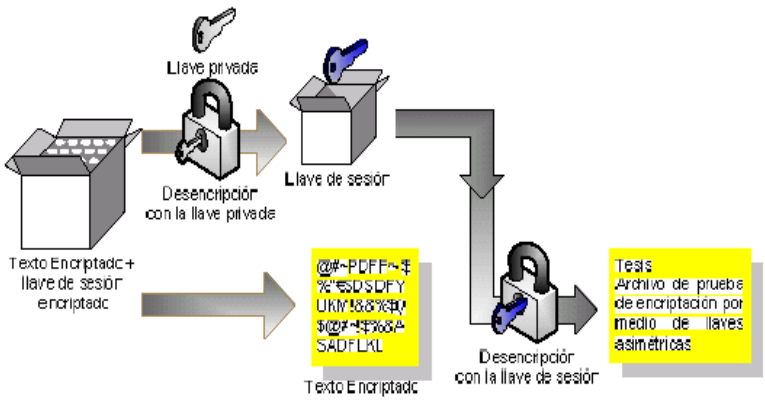

GRAFICO # 4. DESENCRIPTANDO CON GNUPG

La firma digital cumple con el mismo propósito que la firma manuscrita. El uso de la firma digital en la criptografía de llave pública se puede apreciar en la siguiente figura.

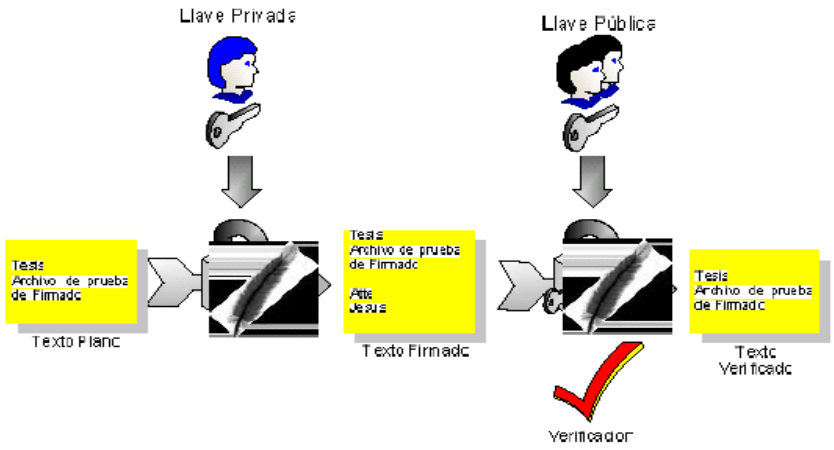

GRAFICO # 5. CRIPTOGRAFÍA Y FIRMA DIGITAL

Este sistema es intensivo en procesamiento y expande la información. Gnupg utiliza una función de hash con una cadena de 160 bits. Si la información cambia un solo bit la función hash produce una salida completamente diferente. Esta salida es llamada message digest o extracto de mensaje. Gnugpg usa el extracto del mensaje y la llave pública para generar la firma.

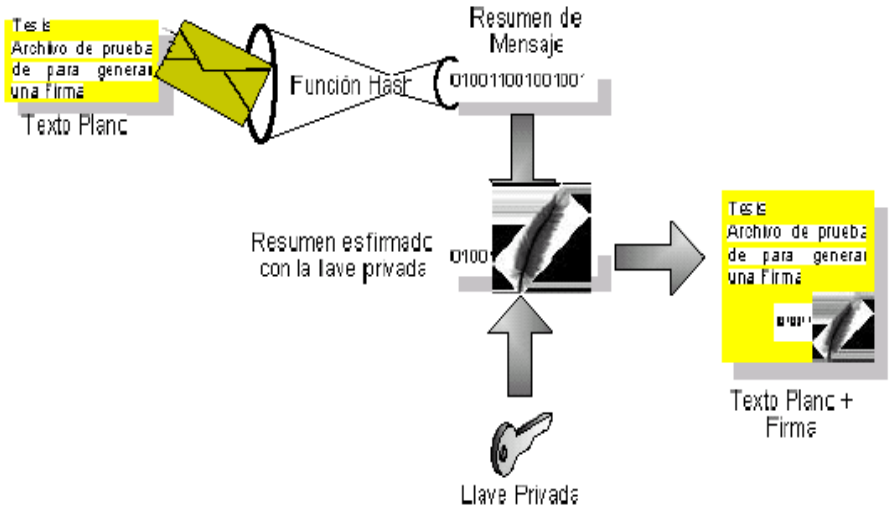

GRAFICO # 6. FIRMA DIGITAL