CAPÍTULO I: INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

En este capítulo se analizará los conceptos relacionados a la seguridad informática, las bases principales, sus componentes, términos usados, definiciones sobre virus, criptografía y los diferentes mecanismos de prevención, corrección en seguridad informática, también se abordará temas relacionados a los diferentes mecanismos de autenticación de usuarios.

1.1. La seguridad en términos generales

Al hablar de términos de seguridad informática se debe entender a las bases que conforman los cimientos de esta ciencia, para las partes más complejas de esta disciplina, una de estas bases es el concepto de seguridad, la cual consiste en un estado de bienestar, es la ausencia de riesgo por la confianza que existe en alguien o algo, si la seguridad se aborda desde el tema disciplinario el concepto se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que se encuentra una persona, un animal, el ambiente o un bien. Existen países en donde la seguridad es un tema nacional, aunque depende del tipo de seguridad, existen muchos tipos de ésta, por ejemplo, la seguridad ambiental, la seguridad económica, la seguridad sanitaria y en casi la mayoría de los países cuando se hace un análisis de la palabra seguridad, se hace referencia a la seguridad de las personas, por ejemplo, evitar el estado de riesgo de un robo, de un daño físico o de un bien material.

La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Así que, cuando se está buscando hacer algo más seguro, estas acciones son algo que se debe de considerar sin importar el área, se aplica a cualquier intento de tener mejor o mayor seguridad en cualquier tema que se requiera.

1.2. Concepto de seguridad informática

Lo primero que se debe mencionar es que en muchos casos se suelen confundir dos conceptos la **seguridad informática** y **la seguridad de la información**, aunque suenen muy parecidos tienen puntos clave que hacen una diferencia.

La **seguridad informática** se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y

métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

Actualmente la informática está siendo inundada por toda la información posible, pero la información por sí sola sigue siendo un universo más grande y en muchos casos más compleja de manejar, ya que los procesos en muchos casos no son tan visibles para los involucrados.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad se puede clasificar en tres partes como son los siguientes:

- Los usuarios
- La información, y
- La infraestructura

Los **usuarios** son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario.

La **información** se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo.

Por último, está la **infraestructura** esté puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización.

Aguirre (2006), también afirma que la seguridad informática puede definirse como el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la **información o los sistemas** ante una eventual amenaza que se pueda suscitar.

1.3. Los virus informáticos

Unos de los primeros conceptos cuando se habla de seguridad informática, es el de virus informático. Las computadoras solo entienden código binario como ceros y unos, en el mundo de las computadoras y de la informática existen muchos conceptos como el de programas, videojuegos, sistemas operativos y cualquier clase de software.

El software es uno de los conceptos más abstractos, se lo define como todo lo intangible de la computadora, son instrucciones que el ordenador espera que se realicen, las cuales pueden ser instrucciones complejas o instrucciones sencillas.

Según Beynon-Davies (2015), el término software o programa es utilizado para describir una secuencia de varias instrucciones que es leído por un computador, los cuales son escritos en un determinado lenguaje de programación que pueden ser clasificados de la siguiente manera:

- Lenguaje de máquina
- Lenguaje ensamblador
- Lenguajes de alto nivel

Analizado el tema clave sobre el software, un virus informático es un programa que tiene como objetivo dañar o cambiar el funcionamiento de la computadora. Esta es una definición bastante clara, pero el virus informático no siempre tiene que ser un programa completo, puede ser hasta cierto punto fragmentos de un programa.

Según Vieites (2013), se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación (C++, C, ensamblador, etc.) con el objetivo de infectar uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o autoreplicación, el cual trata de reproducirse de forma acelerada para extender su alcance.

Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora. También Vieites (2013), indica que existen varios tipos de virus que se los puede definir de la siguiente manera:

- Virus de sector de arranque (BOOT)
- Virus de archivos ejecutables
- Virus de macros
- Virus de lenguajes de Script
- Malware

- Gusanos
- Troyanos
- Spyware
- Keyloggers
- Adwares
- Dialers
- Backdoors
- Otros
- Rootkits
- Bacterias
- Bombas de tiempo

Se mencionó algunos, ya que la lista es bastante grande pero la mayoría son programados para causar daños relacionados con la red y tener la capacidad de autopropagación, esto quiere decir que se multiplica el mismo muchas veces y se posiciona en partes automatizadas del sistema operativo infectado.

Las bombas de tiempo, son virus que se activan al pasar un determinado tiempo o al producir un evento, el que puede ser, por ejemplo, abrir el navegador, pero los eventos suelen ir relacionados con ciertos cálculos matemáticos y registros de memoria, aunque también existen los que se activan con tareas sencillas, estos son solamente algunos de los tipos que se podrían mencionar.

También existe el denominado software malicioso que no es considerado como virus como tal, pero que también genera daños a la computadora, algo muy importante que se debe tener claro es que, el software malicioso debe de tener ciertas características para ser considerados como virus informático, una de las características elementales es que debe de poder reproducirse y generar copias, ya que es la forma en la que se propagan teniendo un comportamiento biológico similar al de los virus que se pueden encontrar en la naturaleza y atacan a los animales y personas.

1.4. Concepto de autenticación

La autentificación se puede definir como un proceso en el que se busca confirmar algo como verdadero, no se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona.

La autenticación es bastante usada en el mundo de la computación, sólo que actualmente la contraseña del correo o de una red social ha hecho olvidar que este método de validación era ya muy común, por ejemplo, todas las credenciales que expiden para realizar una votación en determinado país es un método de autenticación, otro ejemplo es cuando se ingresa a un país y solicitan un documento

como la visa o pasaporte, también es un método de autenticación, otro caso es cuando se asigna un número de cuenta o ID de identificación en el trabajo para acceder a ciertas áreas o también para llevar un registro de los movimientos y en caso de ser necesario poder validar esos movimientos. La Figura 1 muestra un ejemplo de autentificación de usuarios.

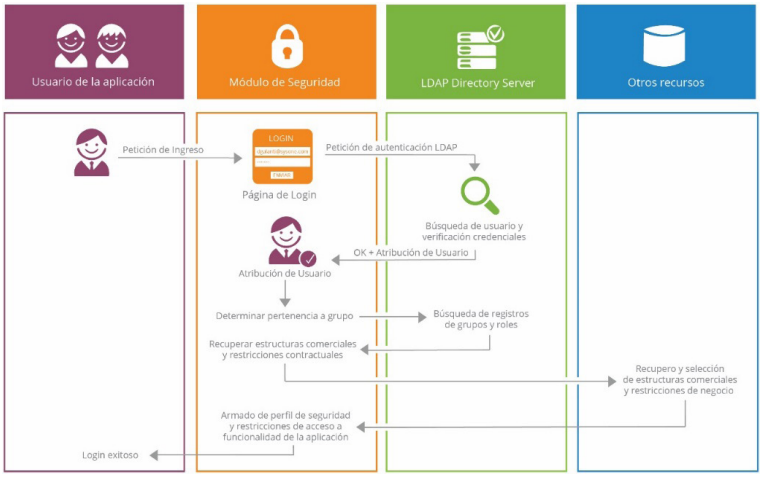

Figura 1. Autenticación de usuarios**.**

Fuente: https://sysone.gitbooks.io/isb/content/security/intro.html

Existen diversos tipos de autenticación, se va a conocer algunos de ellos los más implementados ya que todos los días se trabaja en encontrar más y mejores métodos.

Se tiene los tipos de autenticación en los que se tiene algo conocido, en teoría únicamente por el usuario, por ejemplo, una contraseña, eso es lo más común, pero en teoría, ya que, si se proporciona el usuario y la contraseña del correo electrónico, también puede entrar otro usuario y no significa que sea la persona dueña de la cuenta.

Otro tipo de autenticación es la que se basa en algo de propiedad del usuario, por ejemplo, la tarjeta de crédito, pasaportes o también son los Tokens que generan números aleatorios o palabras claves. También existen las tarjetas conocidas como inteligentes o que contienen cierta información, se pueden parecer a una tarjeta de crédito, pero el comportamiento o información puede variar.

Se tiene también los tipos de autenticación basados en una característica física, este tipo en comparación con lo que ya se mencionó se puede decir que son los más nuevos. Cuando se habla de características físicas se puede mencionar a:

- La voz
- Las huellas dactilares
- El ojo
- La escritura

La autenticación se puede considerar como parte de un método de control de acceso, la mayoría de las ocasiones esto se complementa con otras partes de un sistema, ya que hoy en día debido al manejo de la información y la personalización de los gadgets que se tiene disponibles, se vuelve una labor compleja la de tener control y manejo dentro del sistema.

Los tipos de autenticación no son excluyentes, así que, si se usa un método, no es una barrera para usar otro, de hecho, en sistemas complejos el usuario se puede encontrar con sistemas que utilizan tres tipos de autenticación, obviamente se tiene que pensar en el usuario, a veces es muy molesto siempre y cuando analizando el costo vs el beneficio.

1.5. Mecanismos preventivos en seguridad informática

Los mecanismos preventivos en la seguridad informática son los más olvidados, los cuales son vistos como una pérdida de tiempo, la parte administrativa en la mayoría de los casos lo ve como un costo extra, es algo parecido como por ejemplo, con los seguros médicos o seguros de vehículos, se puede pagar 10 años el seguro de un carro y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado una cantidad 10 años y sin usarla.

La definición de los mecanismos preventivos, consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos, por eso es que las revisiones dependen de los procesos de la empresa y cada una tiene sus propios procesos. Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero.

La mayoría de los ataques informáticos se pueden evitar o por lo menos disminuir el impacto, si se hiciera utilizando mecanismos preventivos, deficiencia de sistemas y otros problemas podrían encontrarse, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La Barrera más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

Entre los elementos que se pueden aplicar en los mecanismos preventivos se puede mencionar a:

- El respaldo de información: Es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general, las empresas entienden que los problemas con información son muy costosos, parece muy fácil pero seleccionar los mecanismos de respaldo no es tan sencillo como se analizar, se tiene que considerar los siguientes factores: Qué formatos de archivo se tienen, por ejemplo, MP3, archivos de texto, bases de

datos y otros, las imágenes y vídeos por ejemplo, son archivos que normalmente necesitan atención especial.

- Horario de respaldo: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.
- Control de los medios: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
- La comprensión de la información: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas.

Estos son sólo algunos de los puntos que se deben considerar, solamente para el mantenimiento y respaldo de la información. Otros ejemplos de proceso que se tienen en el mecanismo preventivo son:

- Actualización de sistemas
- Antivirus
- Firewall
- Navegación por internet
- Contraseñas
- Accesos remotos.

Estos son sólo algunos de los procesos, pero la organización puede personalizar lo que quiere considerar en los mecanismos preventivos.

1.6. Mecanismos correctivos en seguridad informática

Los mecanismos correctivos tienen una gran diferencia en tiempo con los mecanismos preventivos, estos se aplican cuando, después de que algo sucedió y la función principal es corregir las consecuencias. Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo, así que, contratar expertos para resolver el problema o el tiempo que le dedicara a el equipo de trabajo siempre va a costar mucho, en un porcentaje muy alto se acaban pagando servicios de solución a otras empresas, adquiriendo soluciones o comprando software y parches de actualización que logran resolver el problema.

Otra característica de los mecanismos correctivos es que el tiempo es limitado, así que el tiempo se vuelve algo muy apreciado en estos casos, pero también es muy escaso. Probablemente la empresa o la persona puede poder obtener dinero, pero tiempo es casi imposible.

Dentro de los mecanismos de corrección se tienen diferentes pasos de ejecución para enfrentar este problema serio en los que se puede mencionar:

- Catalogación y asignación de problemas: En este paso se hace un catálogo de los problemas a los que se pueden enfrentar, detectar y clasificar es algo muy recurrente en todo lo relacionado con la seguridad informática, ya que es una forma para poder saber cómo abordar las situaciones y buscar alguna respuesta o solución a lo que se presenta.
- Análisis del problema: En este paso es muy evidente que la actividad que se hace es analizar el problema que se ha presentado, en muchos casos esta parte se realiza por los expertos, ya no, por las personas involucradas en el problema.
- Análisis de la solución: Antes de intentar solucionar el problema se debe de analizar la propuesta de la solución, se ha cometido un error, puede ser que no de forma directa, pero es un error, el impacto no va a ser más o menos, si es culpa del usuario o de un tercero, así que la solución tiene que estar bien planteada y ejecutada. Antes de empezar a realizar los cambios, actualizaciones y movimientos se debe tratar de analizar y de predecir qué es lo que va a suceder.
- La documentación: Este componente es vital, ya que los cambios que se hacen probablemente son algo que se hizo con un tiempo limitado, rápido y que involucraron muchos recursos, así que la documentación es muy importante, ya que puede ser que por las velocidades no se recuerden todos los pasos y cambios que se han realizado. En caso de encontrar algún problema se puede consultar la documentación para detectar si la solución era correcta.

1.7. Mecanismos detectivos en seguridad informática

Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos dependiendo de la materia que se aborde, por ejemplo, seguridad de plataformas en línea, en específico de un tipo de bases de datos o tecnología como Wordpress, esto depende del sistema, aplicación o el ecosistema que tenga funcionando.

Los mecanismos de detección parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso. Siempre que se trabaja en los mecanismos de detección se tiene la premisa en mente, se debe de trabajar como si lo que se fuera a encontrar es lo peor y se debe estar preparados para la peor de las situaciones posibles.

Estos mecanismos de detección tienen dos objetivos:

- Poder detectar el punto exacto del ataque para poder llegar a una solución y recuperarse del mismo, pero no siempre es posible esto, depende de los problemas que se afrontan.
- Detectar la actividad que se considera sospechosa y conocer lo sucedido, ya que si no se encuentra donde fue el ataque, lo mínimo que se necesita es saber qué fue lo que sucedió y partir de esa parte.

Lo que es ideal es que se cumpla el objetivo primero, pero no siempre sucede lo ideal, así que se tiene que adaptar al problema, a la situación y todo lo que va saliendo en cada uno de los casos.

Uno de los conceptos que están inmersos en este tipo de mecanismos es la **intrusión**, la cual se la define como una secuencia de acciones realizadas de forma deshonesta, en donde la mayoría de las ocasiones se quiere lograr acceso no autorizado. Dentro de los mecanismos de detección el término más famoso de seguridad informática es el de detección de intrusiones, la cual se define como el proceso de identificación y respuesta ante las actividades ilícitas observadas contra algunos recursos de la red, sistema, plataforma o empresa.

Los mecanismos de detección de intrusión tienen unos pasos que se ejecutan como manera básica de detección que se menciona a continuación:

Revisión de patrones de acceso: En este caso lo que se hace es ver los patrones de acceso, esto quiere decir que se va a analizar los accesos y tratar de encontrar si se está manejando un patrón, por ejemplo, acceso a determinadas horas o el mismo usuario haciendo accesos a la misma sección o módulo. Los patrones siempre van a indicar algo, pueden ser muchos o Las mayorías falsas alarmas, pero es seguro, que si se hizo un ataque se puede encontrar patrones que llamen la atención para después encontrar el problema.

Revisión de transacción: En la mayoría de los casos se obtienen ciertos archivos o se intenta descargar o subir algo de información, así que la transacción es un método muy rápido para lograr esto, la mayoría de los intentos van a ir acompañados de al menos una transacción, esto no es una garantía, pero es algo muy probable, siempre durante la detección si se logra encontrar una transacción es como encontrar el objetivo del atacante lo cual es muy valioso.

Bloqueo automático: Algunas aplicaciones no tienen un sistema de bloqueo, así que, aunque en algunos casos se encuentre el problema y ya se tenga las razones, Si no se cuenta con un mecanismo de bloqueo de emergencia, el atacante podrá seguir haciendo lo que quería. Algunos de los mecanismos de bloqueo comunes son los de paro absoluto, es decir el bloqueo del sistema completo, es algo un poco drástico, pero en muchas ocasiones no se quiere otro riesgo y se considera la mejor opción a la mano.

1.8. El concepto de encriptación en seguridad informática

La encriptación o también conocido como cifrado, es un procedimiento en el que se busca que la información sea ilegible, ya aplicado este procedimiento la información es inservible para cualquier persona que no sea la autorizada, aunque el mensaje sea interceptado, como en muchos casos la información simplemente no significa nada para el interceptor, ya que no cuenta con los elementos involucrados en la encriptación, así que la información simplemente no sirve, la Figura 2 muestra un ejemplo de encriptación.

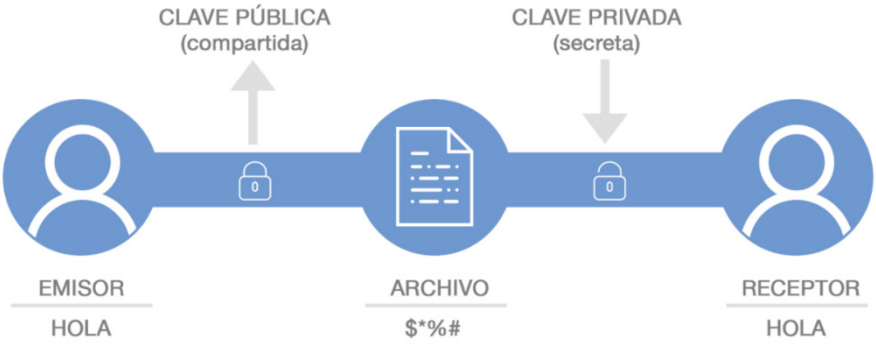

Figura 2. Ejemplo de encriptación.
Fuente: https://www.nextvision.com/2017/08/24/todo-sobre-encriptacion-de-datos-para-empresas/

Se puede decir también, que la encriptación busca la seguridad y la persistencia de los datos mediante un proceso en el cual se involucran algunas partes claves dependiendo del método, por ejemplo, en algunos métodos se utilizan contraseñas o llaves para autentificar la encriptación y la desencriptaciòn de la información, siempre se debe de recordar los objetivos principales de la encriptación y cifrado de datos que se nombran a continuación:

- Confidencialidad
- Autenticación
- Integridad de los datos

La confidencialidad consiste en que la información sólo puede ser accedida por su legítimo dueño o destinatario, la autentificación quiere decir que el emisor y el receptor son los que pueden confirmar la identidad, finalmente la integridad de la información significa que no debe ser posible que sea alterada en caso de que sea interceptada la información.

Según Marrero Travieso (2003), existen muchas amenazas de varias fuentes principalmente de internet que pueden ser:

- Correos electrónicos infectados por virus
- Firewalls mal Configurados
- Suplantación de contraseñas
- Contraseñas débiles
- Robo y destrucción de información, etc.

1.8.1. Métodos de encriptación

Algunos de los métodos de encriptación disponibles actualmente y que son bastantes conocidos se puede mencionar a:

- Encriptación simétrica
- Encriptación asimétrica de clave pública y privada

- Encriptación WPA
- Encriptación WEP
- Firma digital

Estos métodos mencionados anteriormente son la mayoría que se va a encontrar en el mundo de la seguridad informática. Estos métodos de encriptación son bastantes buenos para almacenar y transferir la información.

Encriptación simétrica

Según (Santos, 2014) este tipo de criptografía está basado en métodos criptográficos que usan una misma clave para cifrar y descifrar el mensaje, estos extremos cuando establecen la comunicación deben establecer un acuerdo sobre la clave que tienen que usar, para posteriormente los dos tener acceso a la misma clave, en donde el remitente cifra el contenido de la misma y el destinatario la descifra con el mismo mecanismo. Se puede indicar varios ejemplos de cifrado simétrico.

- Algoritmo de cifrado DES, usa claves basados en 56 bits
- Algoritmos de cifrado 3DES, Blowfish, e IDEA, usan claves de 128 bits
- Algoritmos de cifrado RC5 y AES

Encriptación asimétrica

También (Santos, 2014) indica que este tipo de encriptación se basa en que si el emisor cifra la información el receptor lo puede descifrar o viceversa, en este caso cada usuario del sistema debe poseer una pareja de claves y se tiene dos tipos.

- Clave privada: Custodiada por el propietario, por lo tanto, solo él tiene acceso a ella sin darla a conocer a nadie.
- Clave pública: conocida por uno o todos los usuarios

Como ejemplo de este tipo de algoritmos usados por este tipo de cifrado se tiene a **MD5** y **SHA**.

Firma digital

La Firma digital, es algo habitual en el uso de documentos oficiales, es decir documentos que involucran a una institución gubernamental. El objetivo de la firma es autentificar la identidad de quién envía el mensaje y quién firma el documento, las firmas digitales acostumbran manejar diferentes datos, además de información que se envía, por ejemplo, la hora y la fecha en que se hizo.

La firma digital es una forma matemática de adjuntar la identidad de una persona a un mensaje, está basada en la criptografía de clave pública, esto quiere decir que estos sistemas están utilizando dos claves, la primera sería la clave pública que es la que se conoce y la otra clave sería una clave privada qué es la que solamente el emisor del mensaje conoce.

Encriptación WEP y WPA

La encriptación WEP y WPA tienen algo en común, las dos son aplicadas a las señales inalámbricas y están basados en protocolos de conexión Wifi la primera y la segunda se basa en servidores de autentificación.

En el caso de WEP se tiene tres opciones, de 64 bits, de 128 bits y 256 bits, en donde la más utilizada es la de 128 bits ya que ofrece un buen nivel de seguridad sin tener que ser tan grande y sin aumentar lo complicado del tema. Actualmente la encriptación de 256 bits aún no es soportada por todos los dispositivos.

Existen siempre diferentes opiniones de cómo es que se puede considerar a un método de cifrado, como un buen método de cifrado o un método confiable, pero se puede llegar a una conclusión, un sistema de cifrado se puede considerar como bueno cuando la seguridad de cifrado consiste en la clave y no en el algoritmo.

Aunque se conozca el algoritmo, no se puede llegar a un descifrado de la información gracias a la clave. La mayoría de las aplicaciones que se dan a la encriptación hoy en día son:

- Mensajes de autenticidad
- Facturas electrónicas
- Banca electrónica
- Votos electrónicos
- Notificaciones
- Mensajería instantánea
- Correos electrónicos
- Almacenamiento de información