CAPÍTULO 2

SEGURIDAD INFORMÁTICA

2.1 Definición de Seguridad Informática

Antes de definir el concepto de Seguridad Informática se mencionan algunos términos importantes que se ven involucrados.

Se entiende por datos a todas aquellas cifras y hechos sin analizar. La información se define como el conjunto de datos que han sido analizados u organizados de manera lógica.

"***El concepto de seguridad se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar alguna acción que comprometa a la información***"[1]

Entonces, la seguridad informática consiste en un conjunto de herramientas que permita proteger la información de cualquier peligro que se presente.

La seguridad informática se relaciona con la seguridad de la red, ya que la información necesita de un canal de transporte y las computadoras transmiten información por medio de la red, de esta manera, el objetivo principal es que los datos lleguen seguros a su destino.

La palabra seguridad es un concepto que brinda protección y confianza, la protección se orienta a todos los bienes mientras que la confianza la tiene quien esté operando ese recurso.

Se tiene que instalar una serie de herramientas necesarias para obtener la seguridad deseada, para saber qué herramientas son útiles es necesario contestar tres preguntas:

- *¿Qué se quiere proteger?* Es importante identificar qué recursos se van a proteger de los riesgos que puedan presentarse.
- *¿De qué se quiere proteger?* Cualquier recurso es vulnerable, por lo cual es necesario que los dueños de los bienes le pidan ayuda a

[1] López Barrientos María Jaquelina, Quezada Reyes Cintia. *Fundamentos de seguridad informática*. UNAM, Facultad de Ingeniería, 2006, p23.

especialistas para que analicen las posibles amenazas o peligros de su entorno.

- *¿Cómo se va a proteger?* Una vez contestadas las dos preguntas anteriores se plantearán las políticas de seguridad, pues esto permitirá contrarrestar las amenazas y vulnerabilidades.

Es importante señalar que la seguridad no está garantizada al 100% puesto que el eslabón más débil es la gente, siendo ésta la que manipula los sistemas informáticos, a pesar de este problema, se buscan reducir las probabilidades de que las fallas se presenten en el sistema.

2.2 Amenazas y vulnerabilidades.

Las amenazas y vulnerabilidades son dos términos que no hay que confundir, ya que generalmente se piensa que ambos tienen el mismo significado.

Se le llama amenaza a todo aquello que intente, pueda o pretenda destruir o dañar un recurso, el peligro está latente. Ésta se puede presentar por personas o cualquier otra circunstancia que pueda provocar el daño.

Las vulnerabilidades son aquellas debilidades que tiene el recurso activo donde se le permite al atacante quebrantarlos. Las vulnerabilidades pueden ser aprovechadas por las amenazas para dañar total o parcialmente los bienes.

A continuación se menciona la clasificación de las amenazas y las vulnerabilidades

2.2.1 Clasificación general de las amenazas

Las amenazas se clasifican en los siguientes tipos:

a) De humanos

Este tipo de amenaza ocurre cuando la persona no tiene cuidado con la información que posee, las causas pueden ser por un descuido, inconformidad, ignorancia, etcétera. Como algunos ejemplos pueden mencionarse la ingeniería

social, la ingeniería social inversa, el robo, el fraude, el sabotaje, el chantaje, el terrorismo.

b) Errores de hardware

La amenaza se presenta por fallas físicas en cualquier dispositivo de la computadora, la falla de las computadoras ocasionan en algunos casos pérdida de información, mal funcionamiento del equipo, pérdida del dispositivo.

c) Errores de la red

Esta amenaza se presenta cuando hay alguna falla en la red, ya sea por el mal diseño de la red y se satura el canal de comunicación llegando a bloquear el sistema, dejando como consecuencia que se pierda información o que otro usuario entre a datos no autorizados.

d) Problemas de tipo lógico

Esta amenaza se presenta cuando el diseño de un mecanismo de seguridad no fue bien implementado en el sistema. El usuario al desconocer lo que debe tener instalado en lo referente a software puede dar entrada a códigos maliciosos, el código malicioso es un programa que entra al sistema de cómputo provocando fallas en el sistema, algunos códigos maliciosos que se pueden mencionar son los caballos de Troya, los gusanos, los virus.

e) Naturales

Se refiere a las acciones provocadas por la naturaleza y donde los humanos no tienen participación alguna, en este tipo de amenazas se encuentran las inundaciones, los terremotos, incendios, vientos muy fuertes. Si se presenta algún tipo de éstas en cualquier empresa, repercute en el funcionamiento de los equipos, la red, las instalaciones.

El fuego es la amenaza principal en cuanto a desastres naturales, ya que por cualquier descuido se puede dar con facilidad, como instalaciones eléctricas mal diseñadas que no soporten determinados números de equipos conectados,

dejar conectado algún aparato que se caliente demasiado, un cable en mal estado.

2.2.2 Clasificación general de las vulnerabilidades

Existen seis tipos de vulnerabilidades:

a) Física

Este tipo de vulnerabilidad hace mención a la posibilidad de tener acceso físico al lugar, todo esto con el fin de poder dañar, modificar o robar información importante del sistema que se encuentre en dicho lugar. Por ejemplo, el no contar con buena seguridad en el área, como sería tener chapas frágiles donde éstas se puedan abrir fácilmente.

b) Natural

Los sistemas se ven afectados cuando ocurren desastres naturales, ocasionado por el descuido, por la falta de precauciones que debe tomar cada empresa respecto a la ubicación de la empresa.

Por ejemplo, la falta de extinguidores en cada piso, el no tener un espejo del sistema en otra ubicación, el no contar con ventiladores para evitar que los equipos no se sobrecalienten, un buen sistema de drenaje en caso de inundaciones, entre otras variadas causas de desastres naturales.

c) Software

Las vulnerabilidades que se encuentran en este tipo se deben a que existen programas mal diseñados y programados, carentes de seguridad siendo un programa con errores en la configuración y que cualquier ente no autorizado pueda acceder al sistema.

La mayoría de los programas que son controlados desde la red suelen ser inseguros debido a que no cumplen con todos los protocolos de

comunicación y la operación de ese sistema no suele ser monitoreado constantemente.

d) Hardware

Una de las causas principales que da origen a este tipo de vulnerabilidad es el ignorar los manuales donde vienen las características técnicas de cualquier dispositivo, siendo a la larga un serio problema, ya que al no leer el manual se comenten errores como un mal armado del equipo, el no tomar en cuenta cómo llevar a cabo su mantenimiento para que dure, el saber qué otras tecnologías soporta, el comprar equipo de mala calidad o simplemente hacer mal uso de él al no saber su funcionamiento correcto, exponerlo a fuertes cargas estáticas.

e) De red

El tener conectados equipos a la red provoca una gran probabilidad de que sea muy vulnerable el sistema, ocasionando que las personas que entran al sistema puedan interceptar la comunicación.

A esto añadirle otros problemas como sería un mal diseño de la red, un cableado con pésima calidad que no cumpla con los estándares, el no contar con equipo adecuado como lo son la falta de placas en el área y si hay alguna falla eléctrica no contar con un no- break en el servidor.

f) Humana

Se sigue con la misma línea que las amenazas, siendo que la gente es el eslabón más débil y la mayoría de las vulnerabilidades es a causa del descuido de la persona a cargo, como el no contratar gente con aptitudes para el puesto, ni contar con el personal necesario, que la gente no pida una identificación al querer entrar a un área restringida.

Que no se le dé capacitación al personal así como cursos de actualización pues si se quedan con el conocimiento estancado no sabrán de las nuevas tecnologías existentes para su empresa.

Los malos tratos que se dan dentro de la organización y peor aún hacia gente ajena a la empresa, el no contratar servicio de seguridad para la empresa, el no tener ética profesional, y algunas otras causas que provoque este tipo de vulnerabilidad.

2.2.3 Clasificación general de amenazas en la red

Existe una clasificación general de las amenazas en ésta se pueden observar cuatro categorías:

a) Interrupción: el sistema puede ser destruido o bien no estar disponible, este tipo de amenaza es en contra de la disponibilidad. (Véase figura 2.1)

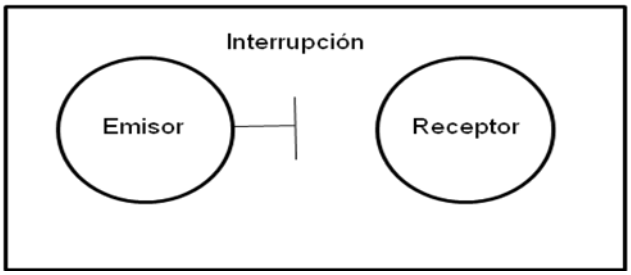

Figura 2.1 Flujo de Interrupción

b) Intercepción: algún usuario no autorizado puede tener acceso al recurso provocando una amenaza contra la confidencialidad. (Véase figura 2.2)

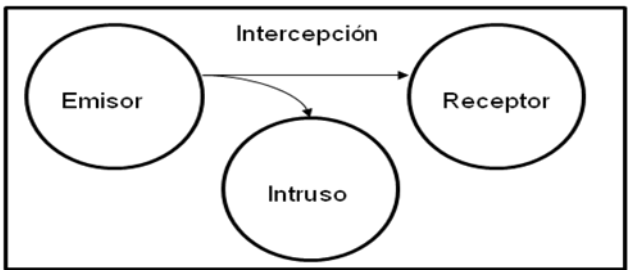

Figura 2.2 Flujo de Intercepción

c) Modificación: el usuario no autorizado puede acceder al sistema para manipularlo a su beneficio, esta amenaza es contra la integridad. (Véase figura 2.3)

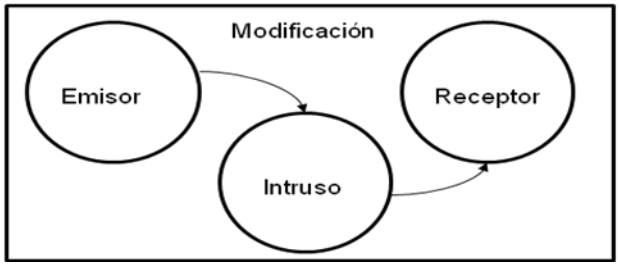

Figura 2.3 Flujo de Modificación

d) Suplantación o fabricación: el intruso puede insertar información falsa en el sistema siendo esto una amenaza contra la autenticidad. (Véase figura 2.4)

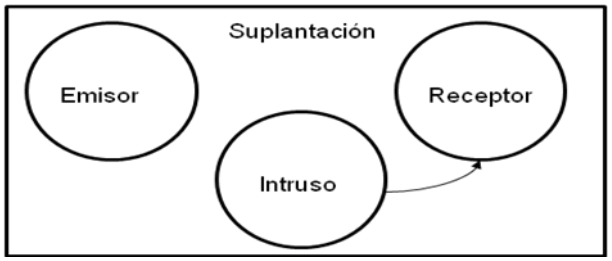

Figura 2.4 Flujo de Modificación

Un ataque es la realización o culminación de una amenaza. Es posible clasificar a los ataques dentro de las mismas cuatro categorías descritas anteriormente, considerando que la descripción no es sólo una posibilidad sino un hecho. También los ataques se engloban en dos grandes categorías.

- Ataque pasivo: aquí el atacante no altera ninguna información, sólo la observa o escucha, un ataque de tipo intercepción se encuentra en este rubro. Los ataques pasivos pueden prevenirse empleando herramientas adecuadas contra el análisis de tráfico.

- Ataque activo: el atacante modifica la información dentro de este rubro se encuentran la interrupción, la suplantación y la modificación. Es posible detectar y prevenir este tipo de ataques, sin embargo la detección puede presentarse de manera extemporánea.

Independientemente del tipo de ataque que se esté realizando, es menester mencionar que cuenta con tres etapas identificables:

1) Preparación: en esta etapa el perpetrador plantea los objetivos deseados, algunas formas que se utilizan para realizar esta etapa son:

- Recolección de información: La forma con la que se obtendrá la información de otros usuarios sin la necesidad de ser administradores. La ingeniería social es de mucha utilidad para el perpetrador, aunque algunas veces recibe ayuda del administrador del sistema, no siempre es así.

- Puerta trasera: Se instala un software que contiene mecanismos escondidos que permiten desviar información confidencial a otro lugar en donde el perpetrador sepa la ubicación.

- Exploración: Se busca información básica de la víctima para obtener datos importantes como lo es la contraseña que utiliza, el número telefónico, entre otra información que le sea de utilidad al perpetrador.

- Mal uso de la autoridad: Cuando el perpetrador logra tener acceso al sistema sin necesidad de utilizar algún método especial para lograrlo significa entonces que se carece de autoridad dentro de la organización.

2) Activación: esta etapa se puede llevar a cabo de las siguientes maneras:

- Si el sistema sufre una interrupción en el sistema operativo, posiblemente el código de ataque se llevará a cabo, si no sucede así, el perpetrador utilizará un programa que le permita interrumpir el sistema.

- Si el programa de ataque es más sofisticado, éste ocasionará que su identificación sea tardía, provocando en algunas ocasiones que el sistema sufra un daño más destructivo.

3) Ejecución: Esta etapa depende del objetivo que se quiera lograr, entre los cuales se pueden mencionar:

- Mal uso activo: se afecta cualquier tipo de información, generalmente los archivos son destruidos o en algunas ocasiones alterados.

- Mal uso pasivo: este objetivo no afecta de ninguna manera al sistema, ni los archivos son modificados, esto es porque el perpetrador sólo quiere fisgonear qué tipo de información se encuentra en dicho equipo.

- Robo del servicio: cuando se llega a robar el servicio, éste se puede utilizar para mandar correo electrónico a ciertas personas, mandar información confidencial de ese sistema, jugar con ciertos datos, etcétera.

2.3 Servicios de seguridad

Un servicio de seguridad se encarga de mejorar la seguridad del sistema de información, así como la manera en que será difundida en la organización. Este servicio protege contra ataques de seguridad y para poder brindar este servicio es necesario utilizar en ocasiones más de un mecanismo de seguridad.

A continuación se mencionan los diferentes servicios de seguridad:

1) Confidencialidad

   Se le considera confidencial a aquello que mantiene en secreto cualquier tipo de información, la confidencialidad protege información secreta de cualquier persona que no esté autorizada para manipularla.

Es de suma importancia para cualquier empresa mantener la confidencialidad de su información, ya que al ser descubierta por gente no autorizada, provocaría un gran daño para la empresa, pues el intruso tendría acceso a datos financieros, información confidencial de los recursos que se poseen, información personal.

Es conveniente contar con un buen control de seguridad para evitar problemas, ya que muchas personas intentan acceder la información confidencial.

El servicio de confidencialidad se encarga de asegurar que nadie pueda leer o copiar cualquier información sin autorización, tampoco que se pueda interceptarla.

2) Autenticación

Se trata de la forma en que uno verifica la identidad de un proceso o una persona.

El servicio de autenticación se encarga de asegurar que la comunicación se lleve de manera correcta, que lo que se espera recibir sea lo acordado. La autenticación se realiza a través de:

a) Algo que se sabe: cualquier sistema requerirá de algún dato que permita identificar que tal usuario es el indicado para acceder a la información, tales datos pueden ser una contraseña o algún número de validación.

b) Algo que se tiene: la forma para verificar la identidad se puede realizar por algún tipo de credencial que sea de utilidad y que sea aceptada por el sistema.

c) Algo que se es: se refiere a algo que puede indicar la identidad de manera más avanzada, como es la voz, la retina, huella digital, esto se realiza con aparatos especiales.

3) Integridad

La integridad se encarga de proporcionar controles que aseguren que el contenido de dicha información no ha sido modificado y que se mantenga intacta al ser transmitida a otro lugar. Si la integridad no existiera, la información sería manipulada a conveniencia de cualquier persona.

Para verificar que un producto llega completo, se comprueban los sellos que le colocan, si están intactos el producto no sufrió ningún altercado.

Para llevar a cabo la verificación de integridad en los sistemas de información es más difícil, ya que cualquier individuo puede cambiar los datos si logra acceder al sistema y si su intención es perjudicar a la empresa.

Se cuenta con dos tipos de servicio de integridad:

a) Servicio de integridad del contenido: ofrece pruebas de que el contenido no ha sido modificado.

b) Servicio de integridad de la secuencia del mensaje: se ofrecen pruebas de que el orden de la secuencia de mensajes se mantuvo intacta durante su trasmisión.

4) No repudio

Este servicio se encarga de que no se niegue que un mensaje ha sido transmitido. Esto es, encargarse de que se pueda demostrar recepción y envío de información a un tercero. Y los siguientes servicios son los que podrían ser proporcionados:

a) No repudio de origen: que se pueda probar que el emisor niegue haber mandado un mensaje con base en pruebas del origen de los datos.

b) No repudio de envío. Que se puedan dar pruebas de que se han enviado los datos.

c) No repudio de transporte: el probar que los datos fueron transportados y evitar la negación de que se hizo.

d) No repudio de recepción: que se pueda probar que se ha recibido el mensaje.

5) Control de acceso

Éste se encarga de limitar el acceso a la organización o al sistema de información de personas que no estén autorizadas. Para tener este control es necesario pedir que el usuario se identifique, una vez hecho esto le será permitido el acceso a su lugar de trabajo.

Los derechos de acceso son los que describen hasta qué grado tiene privilegios cierto usuario. Los privilegios son designados por el administrador y éste puede revocarlos o cambiarlos.

El control de acceso es diferente de acuerdo con el nivel de seguridad, variando desde una entidad individual hasta la administración de la red.

6) Disponibilidad

Como su nombre lo indica este tipo de servicio permite que las personas autorizadas tengan acceso a la información deseada independientemente del día y la hora.

2.4 Políticas de seguridad

Las políticas de seguridad son aquellas que tienen consideradas leyes, reglas y prácticas que regulen la forma de dirigir y proteger cualquier recurso en una organización.

Una empresa debe tener bien planteadas su misión y visión, pues las políticas de seguridad reflejan fielmente los objetivos de la organización, protegiéndola de amenazas y vulnerabilidades.

Si la organización plantea reglas que no le son útiles y están mal elaboradas las políticas de seguridad, tendrá una tarea muy difícil ya que no visualiza claramente lo que debe proteger.

Una organización con reglas bien plateadas podrá gestionar la seguridad de la información de manera eficiente, confiable y ordenada.

Es necesario que las políticas de seguridad se desarrollen en pequeños grupos, por ejemplo, en las oficinas y en los centros de cómputo, las políticas tendrán que cambiar ya que cada lugar tendrá diferentes tipos de vulnerabilidades y amenazas. Esto no representa la inexistencia de un reglamento general que se debe cumplir en toda la empresa, independientemente de cada departamento y diferente a las políticas de seguridad. Existen principios que se aplican en las políticas en general, a continuación se mencionan a detalle:

1) *Responsabilidad individual*: este principio hace referencia al hecho de que toda persona debe estar consciente de lo que hace, ya que cualquier acción que realice quedará registrada y será examinada.

2) *Autorización*: las reglas que establecen quién o quiénes pueden utilizar los recursos dados.

3) *Mínimo privilegio*: las personas sólo están autorizadas para utilizar las herramientas necesarias que permitan hacer su trabajo.

4) *Separación de obligaciones*: debe existir una separación de las funciones que realizan la misma actividad, ya que con esto se evita que una persona cometa un ataque sin ser detectado.

5) *Auditoría*: el trabajo que se realiza debe ser monitoreado desde el principio con el fin de tener registrado lo que cada persona realiza en sus funciones.

6) *Reducción de riesgos*: se debe contar con una estrategia para reducir riesgos a un nivel aceptable.

La redacción de las políticas de seguridad requiere de un compromiso serio por parte de la organización, pues se deben establecer las fallas y vulnerabilidades que existen en ella y actualizarse o modificarse de acuerdo con el dinamismo que exista en la empresa. Estos cambios pueden ser el aumento de personal, cambio en la infraestructura, creación de nuevos servicios, cambios de ubicación de la empresa, etcétera.

Las políticas de seguridad ofrecen una explicación sobre por qué se están tomando ciertas decisiones y demostrar qué tan importante son los recursos que se encuentran en la organización. Las políticas deben redactarse de forma clara y entendible, siguiendo una estructura positiva y haciendo referencia a alguna de las dos filosofías existentes que son la prohibitiva y la permisiva:

- La prohibitiva dice que todo está prohibido a excepción de lo que específicamente está permitido.
- La permisiva dice que todo está permitido a excepción de lo que específicamente está prohibido.

Al formular las políticas de seguridad es necesario considerar los siguientes aspectos:

- Se debe realizar un análisis de riesgos para valorar los activos de la organización y así redactar políticas que se apeguen al funcionamiento de la empresa.
- Una vez identificados los riesgos, se deben reunir las personas que redactarán las políticas con los dueños de dichos recursos y de esta manera proponerles las políticas pues estas personas poseen experiencia y se las harán hacer saber a los dueños.
- Las políticas deben cubrir todos los aspectos que se relacionen con el sistema, también deben protegerlo en los niveles físico, humano, lógico y logístico.

- Comunicar a todo el personal sobre el desarrollo de las políticas y el por qué se redactaron estas políticas, qué beneficios y riesgos tiene cada recurso activo.
- Las políticas de seguridad se deben adecuar a las necesidades y recursos de la empresa e identificar quién tiene la autoridad para tomar decisiones en cada departamento.
- Verificar que se cumplan las políticas así como revisar periódicamente las operaciones de la empresa y los cambios que puedan hacerse de forma que sea benéfica para la organización.

Aunque actualmente cada vez son más organizaciones que se preocupan por establecer políticas de seguridad, aún el porcentaje es muy poco ya que el primer obstáculo que se puede observar es que los altos ejecutivos difícilmente se convencen de lo benéfico que es tener políticas de seguridad en la empresa.

Las políticas de seguridad deben integrarse a las estrategias de la empresa, a su misión y visión con el propósito de que ésta funcione adecuadamente.

Para la realización de políticas de seguridad es necesario recordar tres preguntas básicas que anteriormente se mencionaron:

- ¿Qué se quiere proteger?
- ¿De qué se quiere proteger?
- ¿Cómo se va a proteger?

2.5 Algoritmos de cifrado

Con el paso del tiempo el manejo de información por medio de la red fue creciendo cada vez más hasta convertirse hoy en día en el medio principal para el transporte de mensajes, esto a su vez trae peligros ya que hay intrusos que desean obtener información de utilidad para ellos mismos o simplemente para ver qué tipo de documentos tiene determinado usuario, violándose así los servicios de seguridad como la integridad, autenticación, no repudio y control de acceso. Para evitar este tipo de sucesos es necesario proteger la información por medio de la criptografía.

La criptografía se encarga de estudiar las técnicas para convertir cualquier tipo de información a una forma que no se podrá entender sin tener el conocimiento del método y la clave que sirvan para su transformación. Esto se hace con el fin de ocultar información y de esta forma protegerla de cualquier intruso.

La ciencia que se encarga de estudiar las escrituras ocultas se llama criptología, en ella se incluye la rama de la criptografía y la esteganografía, este método se encarga de ocultar el contenido de un mensaje en un canal diferente, ya sea el sonido o una imagen.

La criptografía tiene por objetivo lograr la disponibilidad, la integridad y la confidencialidad en un mensaje. Cumpliendo lo anterior se asegura que el mensaje sólo sea leído por el personal autorizado.

En la criptografía se le llama texto en claro a aquel mensaje que se quiere transmitir de forma confidencial, el cifrado es el proceso que transforma el texto en claro en un texto que no cualquiera pueda interpretar, este texto recibe el nombre de texto cifrado. Al proceso de volver a transformar el texto cifrado en el texto en claro se le llama descifrado. La clave es la parte más importante de este proceso, ya que aquí se encuentra la seguridad de un sistema de cifrado, es por esto que debe mantenerse en resguardo para evitar que algún ente no autorizado se apropie de ella. El tamaño de la clave varía dependiendo de las características del proceso de cifrado.

En la figura 2.5 Se observan los elementos que intervienen en el proceso de cifrado.

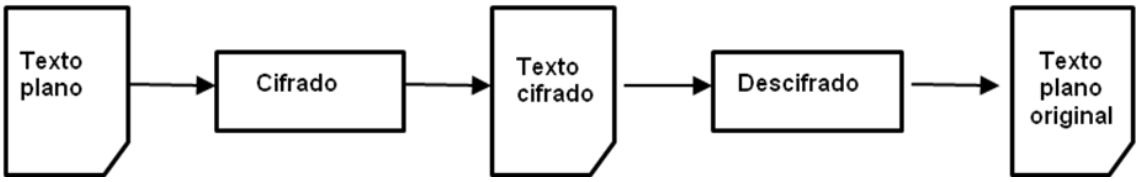

Figura 2.5 Elementos de un sistema criptográfico

En la antigüedad se utilizaban dos principios o técnicas de cifrado:

a) La sustitución consiste en cambiar cada carácter del texto plano por otro elemento, es decir, existe una correspondencia entre las letras del alfabeto que se encuentran en el texto original con los elementos de otro conjunto que puede ser de la misma forma o con diferente alfabeto y cada letra se va sustituyendo por el símbolo definido en dicho proceso. El destinatario debe saber la clave que se utilizó para poder descifrar y volverlo a su forma original.
b) La transposición consiste simplemente en cambiar el orden de las letras, a diferencia del método por sustitución éste sólo va reordenando las letras.

Existen 2 tipos de algoritmos de cifrado, si el emisor y receptor utilizan la misma clave de cifrado, se le conoce como cifrado simétrico, pero si el emisor y el receptor utilizan claves de cifrado diferentes, se le conoce como cifrado asimétrico.

a) Cifrado simétrico

Al cifrado simétrico se le llama de clave secreta o de clave privada ya que dicha clave la conoce tanto el emisor como el receptor únicamente. Es por eso que se debe tener cuidado en la forma en la que se acordó la clave, ya que no importa que se sepa el método que se utilizó, sino la forma de cómo se protegió el mensaje y esto es a base de las claves.

La clave debe ser utilizada una sola vez cuando se cifran mensajes diferentes, es decir, una vez utilizada cualquier clave, habrá que modificarla ya que se corre el riesgo de que se descubra el mensaje por algún intruso.

Esta forma de cifrado se usa generalmente cuando el volumen de los datos es demasiado grande.

Existen diferentes algoritmos que a continuación se enuncian:

- DES (Data Encryption Standard – Estándar de cifrado de datos). Fue creado en los años 70, el método utiliza un cifrado por bloques en donde se tiene una longitud de bloque de 64 bits y una longitud de la clave de 56 bits, consiste en 16 iteraciones de la misma función
- 3DES. Este método recibe el nombre porque se hace tres veces el cifrado del DES y su creación se debe a que se quiso agrandar la clave sin necesidad de cambiarse de algoritmo de cifrado. Con este método se logró hacer el DES más seguro, aunque está desapareciendo lentamente debido a la creación de otros métodos más eficientes. Aunque la mayoría de las tarjetas de crédito manejan este algoritmo.

- RC4. Fue diseñado por Ron Rivest en 1987 y el nombre completo del método es Ron Cipher (cifrado de Ron), el número 4 se debe a la versión del diseño, también se le conoce como ARC4.

Para usar este método se combina con el mensaje en claro usando la función XOR, se emplea una permutación de todos los 256 posibles símbolos de un byte de longitud, la permutación se inicializa con una clave de longitud variable entre 40 y 256 bits.

a) AES (Advanced Encryption Standard - Estándar de Cifrado Avanzado). Publicado por el NIST (National Institute for Standard and Technology-Instituto Nacional de Estándares y Tecnología) en el año 2001, con la finalidad de sustituir al DES. El AES maneja bloques de 128 bits, soporta el manejo de claves de diferentes longitudes (128, 192 y 256 bits). El AES hace uso de matemáticas polinomiales en estructuras de campos finitos.

b) Cifrado asimétrico

El cifrado asimétrico utiliza algoritmos donde la clave de cifrado es distinta a la de descifrado, además de que las operaciones matemáticas que realiza no son simples, ocasionado que los algoritmos sean de proceso lento al momento de descifrar en comparación con los algoritmos de cifrado simétrico.

Entre las partes que integra un cifrado asimétrico se encuentran el mensaje en claro, el algoritmo de cifrado, una clave pública y una privada, el mensaje cifrado y el algoritmo de descifrado.

Ejemplos de algoritmos asimétricos:

- RSA. Por las siglas de sus creadores Ronald Rivest, Adi Shamir y Leonard Adelman. Desarrollado en 1977, realiza la factorización de un número de gran tamaño.

Entre las desventajas de este algoritmo es que requiere mayor tiempo de ejecución en comparación con el cifrado simétrico, la seguridad del cifrado depende de la eficiencia computacional y por último la clave privada debe ser cifrada por algún algoritmo simétrico.

- Diffie-Hellman. Este método fue desarrollado por Whitfield Diffie y Martin Hellman en 1975. Este método consiste en intercambiar claves entre dos partes que previamente no han tenido contacto, utilizando un canal inseguro y de manera anónima.

  En cuestiones matemáticas este método se basa en las potencias de los números y en la función mod (módulo discreto). Esto es la potencia discreta de un número como $Y = X^a \bmod q$.

- MD4 (Message Digest Algorythm 4 – Algoritmo de Publicación de Mensaje). Desarrollado por Ron Rivest en el cual se hace una manipulación de bits para que se pueda obtener el hash (método para generar claves) para el uso en comprobaciones de integridad de mensajes, la longitud del mensaje es de 128 bits.

  En 1991 se desarrolló el MD5 como mejora del MD4 permitiendo la seguridad a la integridad de la información. La codificación del MD5 de 128 bits se representa como un número de 32 dígitos hexadecimales y así la obtención del valor hash se considera más segura.