Fundamentos Teóricos

1. Fundamentos teóricos

En la actualidad el avance de las comunicaciones y las tecnologías de la información han hecho que la manera de compartir, acceder y comunicar la información sea más rápida y fácil. El hecho de poder consultar todo tipo de información desde cualquier parte del mundo en todo momento desde algún dispositivo como lo son las computadoras, es una de las maravillas que hoy se puede tener gracias a medios como el Internet.

Al poder tener toda esta información se tiene la necesidad de protegerla ya que no toda la información puede ser consultada, editada, borrada o eliminada por personas sin autorización. Si cualquier persona pudiera editar, borrar, destruir, consultar y leer la información de manera arbitraria, sin un orden, crearía un caos, pérdidas económicas, robos de identidad, información errónea, entre otras muchas más.

Es por esto que el tema de la seguridad de la información es un tema muy explotado en películas, las cuales presentan personas que se dedican al robo y otras acciones ilícitas por medio del uso de computadoras, celulares y otros dispositivos digitales.

Estas personas son generalmente aquellas que no tienen límites en sus habilidades al poder acceder a cualquier tipo de información desde diversos lugares, obteniendo ésta en cuestión de minutos.

Esto ha creado la ilusión de que es imposible el poder detener a este tipo de personas con habilidades extraordinarias que se conocen como “hackers”, sin embargo, en realidad este tipo de publicidad es totalmente falsa. Muchos de los términos que se utilizan normalmente, son erróneos, o no utilizados de manera correcta.

Dado que la información que comúnmente no es del todo fidedigna y se emplean de manera incorrecta muchos de los términos, se cometen errores y se es presa de desinformación, lo cual en ocasiones conduce a las personas a tomar decisiones incorrectas que ponen en peligro su información.

Los medios de comunicación presentan nuevos dispositivos de cómputo con capacidad de almacenar, enviar y consultar información de todo tipo, como son fotos, video, audio, texto, entre otros, los cuales contienen información que puede ser o no importante para el usuario. Esta información en ocasiones es utilizada para beneficio de manera ilícita al exponer o publicar esta información en internet, difundirla vía radio o televisión y otros medios.

Este tipo de acciones crea incertidumbre y miedo en el usuario de que la información pueda ser vista por otras personas, es por eso que las compañías promueven dispositivos novedosos, herramientas para la seguridad principalmente antivirus y sistemas operativos que prometen mantenerla de manera más segura.

Este tipo de publicidad "fraudulenta" promete proteger la información de diversas amenazas, como son los hackers, virus informáticos, troyanos, rootkits, scripts, bloqueo de e-mails scam, phishing, y realizar análisis de sitos en internet para una navegación segura, configurar firewalls, entre otras acciones. Este tipo de publicidad crea la ilusión de que los" hackers" crean y controlan estos virus que son la razón de la pérdida y robo de la información.

Este tipo de publicidad tiene por objetivo el vender, prometiendo que sus productos son confiables y de fácil manejo, es decir, que no contienen fallas de ningún tipo y que cualquiera puede manejarlos de una manera muy sencilla con resultados asombrosos. Esto crea una falsa seguridad en la que las personas piensan que su información está protegida y segura.

La realidad es que los medios de comunicación y las organizaciones que fabrican estos productos han exagerado en el hecho de promover éstos al punto de garantizar la seguridad de la información.

Es importante el comprender la relevancia que tiene la seguridad de la información ya que todo el mundo tiene "enemigos". Este tipo de personas puede utilizar la información de manera ilegal para obtener algún tipo de beneficio propio.

Para ilustrar esto, se puede mencionar que cualquier país tiene enemigos, todas las organizaciones tienen competidores, y de manera más pequeña pero no menos importante, las envidias y celos dentro de un grupo de trabajo.

Por otra parte, el considerar que una organización o persona intente, pretenda, robe, destruya u obtenga cualquier tipo de información de manera ilícita o sin el consentimiento del dueño de ésta, es considerado como un ataque, no importando si es de manera intencional o por error. Cabe mencionar que en ocasiones el que el dueño de la información puede ser el propio enemigo ya que por error, desconocimiento o de manera intencional puede realizar algún tipo de ataque con la finalidad o no de obtener algún beneficio.

1.1 Conceptos básicos de seguridad informática

La necesidad de contar con definiciones adecuadas acerca de la seguridad de la información, cobra mucha importancia, ya que contando con un mejor conocimiento acerca de estos temas será más sencillo, fácil y eficiente proteger la información.

En términos generales, se puede afirmar que la mayoría de las personas cometen errores por el hecho de confundir y saber definiciones incorrectas sobre estos temas, el desconocimiento de los temas relacionados, y la desinformación de los medios al difundir la información de manera errónea, entre otros.

Antes de poder definir lo que es la seguridad informática se deben definir algunos conceptos que ayudan a esclarecer mejor el concepto.

- Organización

Una organización es un conjunto de recursos materiales y humanos con el propósito de alcanzar objetivos y metas. Una organización puede ser un país, una empresa, una universidad, una familia, etcétera.

- Recursos Humanos

Recibe el nombre de recursos humanos el conjunto de los empleados o trabajadores de una organización.

- Bienes o Activos

Reciben el nombre de bienes o activos cualquier propiedad de una organización o de una persona. Entre éstos se pueden encontrar, equipo, edificios, autos, mobiliario, derechos de autor, marcas registradas, nombre de la empresa, información, etcétera.

- Información

La información es el conjunto de datos que obtienen algún significado para quien los manipula.

Ahora bien, antes de pasar a la definición es necesario aclarar que la información en ocasiones no solo se encuentra en forma digital, no dejando por esto de ser información. Por otra parte, el lugar donde se almacena y se maneja dicha información es de suma importancia, ya que sin éste, la información no estaría protegida; por último pero no menos importante, el aclarar que el personal o las personas que trabajan con ella, son las encargadas y responsables de su manejo.

Por esto, es posible definir a la seguridad informática como:

- Seguridad de la información o la seguridad informática

Es el manejo adecuado y protección de todo tipo de información (impresa, digital, oral o conocimiento acerca de la organización), de los recursos como son, los bienes o activos (equipos, renombre, recursos informáticos, entre muchos otros) así como de los recursos humanos.

Ya que se cuenta con una definición de lo que es la seguridad informática, y sabiendo que es la encargada de proteger los bienes y recursos de la organización, es importante el saber de qué o de quién se protegen los bienes y recursos de una organización. Para esto es necesario definir dos conceptos.

- Amenaza

"Una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación de la seguridad."[1]

Podemos definir como amenaza a todo aquello que intente, puede o pretende destruir o dañar.

[1] María Jaquelina López, Cintia Quezada, Fundamentos de seguridad informática, p.91

Las amenazas pueden provenir de varias fuentes:

1) Humanas
2) Errores de hardware
3) Errores de la red
4) Problemas de tipo lógico o errores de software
5) Desastres

1) Humanas

Este tipo de amenazas son generadas por los seres humanos al manejar la información. Este tipo de amenazas se pueden dar por la ignorancia, la falta de capacitación, descuido, negligencia, errores, intencionales.

En este tipo de amenazas es posible mencionar las siguientes: ingeniería social, robo, el mal uso de los recursos, fraude, sabotaje, terrorismo, espionaje, entre otros.

2) Errores de hardware

Este tipo de amenazas se da por fallas en los dispositivos como son, deterioro, funcionamiento incorrecto, fallas en la energía eléctrica, sobrecalentamiento, problemas en el diseño, mala implementación.

3) Errores de la red

Ocurren cuando la red no está bien diseñada ya que el flujo de información es mucho más grande de lo que se tenía previsto, o cuando existe alguna mala configuración en los sistemas que conforman la red. Entre éstos se pueden encontrar, cableado defectuoso, interferencia, la lentitud en el tráfico.

4) Problemas de tipo lógico o errores de software

Se presentan cuando se implementa algún tipo de seguridad de manera errónea o malas configuraciones, así como cualquier tipo de malware. Algunos ejemplos son los virus, gusanos, código malicioso, caballos de Troya.

5) Desastres

Las amenazas de este tipo son fenómenos naturales que ocasionan algún tipo de siniestro, entre éstos se encuentran los incendios, las inundaciones, los tornados, huracanes, terremotos, entre otros. También se conocen como actos de Dios.

- Vulnerabilidad

"Una vulnerabilidad es un punto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo, es decir, representan las debilidades o aspectos atacables en un sistema informático. Se trata de una debilidad que puede ser explotada para violar la seguridad." [2]

Se define como vulnerabilidad a todas las debilidades existentes en un sistema.

Las vulnerabilidades se pueden clasificar de la siguiente manera:

1) Físicas
2) Naturales
3) De hardware
4) De software

[2] Ídem, p. 100

5) De red

6) Humanas

1) Físicas

Este tipo de vulnerabilidad se refiere al acceso físico a las instalaciones de una organización. En otras palabras de refiere al acceso a edificios, estacionamientos, laboratorios, oficinas, y demás áreas que puedan existir en una organización.

2) Natural

Las vulnerabilidades de tipo natural se refieren a cómo es que las condiciones geográficas y las condiciones ambientales pueden afectar al sistema cuando no se cuenta con las medidas necesarias para prevenirlos o disminuir el impacto, es decir, la posibilidad de que el entorno pueda afectar el sistema al tener nuestras instalaciones en regiones donde los incendios, huracanes, inundaciones, terremotos y otros fenómenos naturales sean muy comunes, de esta misma forma que las condiciones ambientales hagan difícil el manejo u operación del equipo como son las condiciones de extremo calor o frio.

También se incluyen los malos diseños de las instalaciones, o la poca previsión de algún tipo de instalación que no se tenía contemplada en el momento de construir, así como el crecimiento de la misma. La falta de copias de seguridad y de la dependencia de una sola área que contenga toda la información en algún punto geográfico, la falta de dispositivos auxiliares, la cercanía a instalaciones de alto riesgo en las que se contengan materiales peligrosos.

3) De hardware

En este tipo de vulnerabilidades se presentan cuando hay malas instalaciones, falta de mantenimiento, y falta de protección de los dispositivos.

4) De Software

Las vulnerabilidades en el software surgen por la falta de previsión al realizar la programación, errores en la misma, también se dan por la mala configuración de los programas y problemas, conflictos y errores en los sistemas operativos que puedan alterar información, permitir modificaciones en los programas, así como la modificación y consulta de la información del sistema.

5) De red

Se presentan cuando no se tiene un control sobre los equipos que se conectan a una red o al sistema, las fallas en la implementación al realizar el cableado estructurado, la falla en la configuración de cualquier tipo de acceso a la red, (incluyendo también las tecnologías inalámbricas, bluetooth, infrarrojos, radio frecuencia, ZigBee, entre otras).

6) Humana

Las vulnerabilidades de tipo humana, se presentan al no contar con personal adecuado, por la falta de capacitación, la falta de ética, la mala disposición del personal, etcétera.

Es importante saber distinguir entre una amenaza y una vulnerabilidad, ya que no son términos que hagan referencia a lo mismo.

Una amenaza se aprovecha de las vulnerabilidades para dañar o destruir, es decir, las amenazas explotan las vulnerabilidades.

Para clarificar esto, se puede decir que al ir a una gasolinera y cargar combustible hay una vulnerabilidad, la cual es que esa área puede incendiarse con facilidad. La amenaza sería que alguien encendiera un cigarro.

La persona que enciende su cigarro podría causar un incendio en la gasolinera. La persona que enciende su cigarro sería la amenaza que se aprovecharía de que la gasolinera es un lugar que es propenso a los incendios y que no cuenta con las medidas de precaución convenientes para evitarlo.

El entender las amenazas y las vulnerabilidades proporciona información que puede ayudar a prevenir incidentes que debilitan, dañan o destruyen a la organización. El hecho de que se presente algún incidente es una clara muestra de un ataque.

Es necesario entonces también definir qué es un ataque:

- Ataque

"Es intentar de alguna manera quebrar el sistema destino, los mecanismos de redes y de seguridad." [3]

Como se ha visto, la seguridad informática protege cualquier tipo de bien o activo de una organización, así como del personal que labora en ella. Tomando esto en cuenta se observa que:

Un ataque es entonces el intento por el cual se pretende obtener, dañar, destruir, o realizar cualquier tipo de modificación a un bien o activo de una organización, siendo éste exitoso o no. Un ataque es la culminación de una amenaza cuando ésta explota una vulnerabilidad.

Con base en lo anterior, un atacante es el individuo, grupo de individuos u organización que realiza algún ataque.

Es importante mencionar que se puede clasificar a los ataques en dos tipos:

I. Pasivos

II. Activos

I. Pasivos

Este tipo de ataques son aquellos en los cuales sólo se reúne información, es decir, se obtiene la información con el fin de poder elaborar y llevar a cabo un plan mediante el cual se pueda obtener un beneficio.

[3] http://www.seguridadinformatica.dcyc.ipn.mx/glosario.html

De esta forma el atacante no modifica, daña o destruye nada, su propósito es el reunir toda la información posible mediante la observación, la escucha o la lectura para que de esta manera pueda elaborar y realizar su plan para obtener un beneficio.

Al ser atacado de manera pasiva es sumamente difícil y complicado el percatarse de esto, es decir, no se sabe que se está siendo atacado ya que el atacante sólo reúne información, por esto no hay indicios de ningún tipo de daño, pérdida o destrucción evidente en el momento en el que está ocurriendo.

II. Activos

Un ataque activo es aquél en el cual el atacante daña, destruye, y realiza modificaciones a los bienes de una organización de manera evidente. Este tipo de ataques es perceptible, es decir, a diferencia de los ataques pasivos en los cuales en el momento del ataque no se sabe que se está siendo atacado, en una ataque activo es muy fácil percatarse de él.

El éxito de este tipo de ataque depende en gran manera del pasivo, ya que dependiendo de qué tanta información haya obtenido el atacante, mayor será el daño que cause a los bienes de la organización. En la mayoría de los casos es difícil el contrarrestar este tipo de ataques si el atacante cuenta con la información necesaria para lograr su objetivo.

Cuando una organización es atacada de manera activa puede generar gran confusión, pánico, miedo, daños considerables a los bienes de la organización. Un ejemplo claro de este tipo de ataques son los ataques terroristas los cuales tiene una planeación cuidadosa al reunir información acerca del objetivo (ataque pasivo), en el momento en que se lleva a cabo el plan se convierte en un ataque activo.

1.2 Servicios Informáticos

La seguridad informática tiene como objetivo el proteger los bienes de una organización, principalmente la información, de cualquier tipo de ataque ya sea pasivo o activo. De esta manera la seguridad informática cuenta con los servicios informáticos los cuales están enfocados al manejo, control y a la confiablidad principalmente.

Los servicios informáticos, también llamados servicios de seguridad, deben estar presentes todo el tiempo dentro de cualquier organización; la seguridad informática debe garantizar que estos servicios estén presentes al implementar cualquier medida de seguridad. Éstos se pueden clasificar en:

1) Confidencialidad
2) Autenticación
3) Integridad
4) No repudio
5) Control de Acceso
6) Disponibilidad

1) Confidencialidad

Este servicio consiste en asegurar que la información sólo puede ser accedida por ciertas personas, es decir, sólo personas que estén autorizadas por el dueño de la información serán las que podrán tener acceso a ésta.

La privacía o confidencialidad es un servicio que cumple con la función de mantener en secreto la información.

2) Autenticación

La autenticación es la verificación de la identidad. Este servicio se encarga de verificar o tener la seguridad de que la identidad sea confirmada.

3) Integridad

El servicio de integridad es la verificación de que la información no ha sido alterada o modificada y que permanecerá de esta manera mientras el dueño de la misma así lo requiera o necesite.

4) No repudio

Este servicio consiste en evitar y garantizar que los emisores, receptores, o las partes involucradas puedan negar la recepción, transmisión, lectura u otras actividades con respecto a la información.

5) Control de Acceso

El control de acceso es el servicio encargado de impedir o permitir el acceso a un sistema, área, o recurso, así como el limitar el acceso al mismo.

6) Disponibilidad

Es el servicio que se encarga de garantizar que el recurso, sistema, información o área pueda ser accedida cuando se requiera o necesite.

Los servicios de seguridad utilizan estos principios en conjunto para garantizar que los recursos, la información, los sistemas, y demás bienes sean utilizados, accedidos, consultados, modificados, borrados sólo por las personas designadas por el dueño de éstos. Con esto se pretende evitar las pérdidas y los accesos a estos bienes de manera que sean utilizados para los propósitos para los que fueron designados originalmente.

1.3 Mecanismos de Seguridad

Así como los servicios de seguridad tienen el propósito de que los recursos, información, sistemas y demás bienes sean utilizados para lo que fueron destinados. Los mecanismos de seguridad se basan en:

- Conjuntos de algoritmos, los cuales permiten implementar técnicas criptográficas.
- Conjuntos de procedimientos, que establecen cómo se emplearán los algoritmos.
- Información secreta, que puede ser algo que se tiene, que se posee o que se sabe (claves, contraseñas, credenciales, etcétera).

Esto es con el fin de implementar los diferentes servicios de seguridad dentro de una organización. Estos mecanismos se emplean dependiendo del nivel de seguridad deseado y del tipo de servicio que se desee implementar.

Algunos de estos mecanismos de seguridad son:

1) Intercambio de autenticación
2) Cifrado
3) Integridad de datos
4) Firma digital
5) Control de encaminamiento
6) Unicidad

1) Intercambio de autenticación

Los mecanismos de intercambio de autenticación son los encargados de verificar y corroborar la identidad por medio de técnicas criptográficas, para verificar con certeza el origen y destino de la información. Un ejemplo de este tipo de mecanismo son los certificados digitales en páginas para las transferencias bancarias.

2) Cifrado

Es un mecanismo por el cual mediante técnicas criptográficas se garantiza que la información sea ilegible para los usuarios no autorizados. Con esto se garantiza la confidencialidad de la información.

3) Integridad de datos

La integridad de datos es un mecanismo en el cual se utiliza el cifrado y compresión de una cadena de datos con el fin de que el receptor pueda realizar una verificación de la integridad de la información enviada.

4) Firma digital

Es el mecanismo en el que se utilizan técnicas criptográficas con lo que se garantiza la integridad de la información así como la autenticación del emisor. Consiste en un conjunto de caracteres que vinculan al autor con el documento y se anexan a él, con el fin de acreditar quién es el autor y comprobar que la información no haya sido manipulada.

El receptor procesa la información para validar al autor y la integridad de la información. Cabe señalar que la firma digital no cifra el mensaje, únicamente garantiza el origen.

5) Control de encaminamiento

Este mecanismo de seguridad permite enviar información de manera controlada por zonas determinadas. Con este tipo de mecanismo se evitan zonas donde se detecten violaciones a la integridad de la información enviada.

6) Unicidad

La unicidad consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, incluyéndose en la firma digital o integridad de datos. De esta forma se logra que la información tenga una secuencia única.

1.4 Gestión de contraseñas

Las contraseñas son un mecanismo mediante el cual se accede a información, recursos, sitios, etcétera. También mediante las contraseñas es posible autenticar la personalidad al querer acceder a algún recurso de manera lejana o remota, lo cual es de suma utilidad ya que en ocasiones se requiere manipularlos sin que se estar presente.

Este mecanismo es el más utilizado, por lo que si algún atacante consiguiera la contraseña, sería capaz de acceder a los recursos, a la información, suplantar la identidad obteniendo así algún beneficio de manera ilícita.

Es por esto que se define el término contraseña o clave como una forma de autenticación que utiliza información secreta para tener acceso a algún recurso, sistema o sitio.

Las contraseñas son como las llaves que se emplean normalmente para la apertura y cierre de puertas, cerraduras, candados que normalmente se utilizan para proteger casas, oficinas, autos, cajas de seguridad, etcétera. Sería ridículo perder las llaves o prestarlas a cualquier persona ya que eso tendría el riesgo de que alguien pudiera realizar algún acto mal intencionado como lo es el robo. En este caso las contraseñas funcionan de la misma manera.

Sin embargo, al igual que las cerraduras, candados y puertas, pueden ser forzadas o abiertas de manera ilícita o usando técnicas de cerrajería, los mecanismos para validar, que son lo equivalente a las puestas, candados y cerraduras, también sufren ataques.

Estos ataques consisten en adivinar las contraseñas, la prueba de múltiples combinaciones de datos asociados al usuario, como son fechas, nombres, eventos, frases, libros, mascotas y datos de personas cercanas al dueño de la contraseña o el usar combinaciones de datos e información de forma aleatoria y la creación de diccionarios de información son algunas de las técnicas más socorridas para obtener el acceso y así burlar los diversos mecanismos de seguridad que requieran una contraseña.

Con el fin de que la contraseña sea más fuerte, es decir, que el atacante requiera invertir más recursos y mucho más tiempo para obtener acceso, existe la gestión de contraseñas. La gestión de contraseñas es el coordinar los recursos disponibles para conseguir que una contraseña sea confidencial, es la utilización de técnicas y recomendaciones para lograr que una contraseña sea más confiable, que se mantenga en secreto y que aminore el riesgo de que el atacante pueda obtener el acceso. La gestión de contraseñas es de gran importancia

ya que por medio de ella se puede resguardar y proteger la información de una mejor manera.

Es importante el mencionar que no importa qué tan seguro sea el mecanismo de seguridad para el acceso, si no se hace uso de la gestión de contraseñas, el atacante podrá tener acceso de una manera relativamente sencilla y acceder a recursos, información, sitios, etcétera.

Para contar con una apropiada gestión de contraseñas, a continuación se mencionan algunas recomendaciones y técnicas para la creación y mejoramiento de la seguridad de las contraseñas que son más utilizadas en el acceso a los diferentes sistemas que requieren ingresar alguna cadena de caracteres, como son el correo electrónico, cuentas de bancos, cuentas internet de cualquier tipo, etcétera.

- Evitar contraseñas cortas

El añadir más caracteres a una contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Por esto es recomendable que la longitud mínima de una contraseña sea de seis dígitos.

- Memorizar las contraseñas

El evitar apuntar las contraseñas en alguna parte es una vulnerabilidad ya que existe el riesgo de que alguien pueda acceder a esa información y pueda hacer mal uso de ella. Por eso es recomendable que las contraseñas sean memorizadas.

- Tener una contraseña para cada recurso

Es recomendable el tener una contraseña por cada cuenta ya que si la contraseña llegara a ser obtenida de alguna forma, los recursos de los cuales se es responsable estarían en un riesgo inminente de ser accedidos.

- Evitar el uso de información contenida en diccionarios de cualquier clase o idioma

El hacer uso de palabras o información contenidas en cualquier diccionario o publicación en cualquier idioma puede ser utilizado por algún atacante para obtener el acceso.

- Cambiar la contraseña periódicamente

El cambiar la contraseña periódicamente tiene la ventaja de que si ésta fue obtenida se evita que exista algún tipo de ataque pasivo, con el cual el atacante pudiera obtener información valiosa para la planificación de un ataque activo. Es recomendable que la contraseña se cambie al menos cada 6 meses.

- Uso de mayúsculas, minúsculas, números y caracteres especiales.

El uso de múltiples caracteres complica que sea adivinada o vulnerada, ya que aumenta el número de combinaciones que un atacante tendría que probar para obtener el acceso.

Como se ha visto a lo largo de este capítulo, la seguridad informática abarca muchas áreas entre las que se encuentran las redes, el cifrado, las comunicaciones, entre otras.

Una de estas áreas es el desarrollo de políticas de seguridad, la cual tiene como uno de sus objetivos el crear lineamientos, estrategias, guías, normas que ayuden a las personas, las capaciten, y creen conciencia acerca de cómo manejar y cuidar de una mejor manera los recursos, bienes y la información.

La seguridad informática tiene como una de sus metas el proteger la información y bienes de las personas, pero es importante el remarcar que la seguridad depende en gran parte de las personas responsables y los dueños de la información y los bienes.