Capítulo I

Antedecentes

En este capítulo de denotan los conceptos básicos para la compresión del proyecto.

1.1 Concepto de la Seguridad Informática

La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema automatizado mediante Tecnologías de la Información y sus usuarios, así, la seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

- La información contenida
  Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios no autorizados puedan acceder a ella. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella, que sea manipulada, ocasionando lecturas erradas o incompletas de la misma, o incluso que sea falsamente generada.

- La infraestructura computacional
  La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- Los usuarios
  La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general.

Técnicamente es imposible lograr un sistema informático ciento por ciento seguro, pero la implementación de medidas de seguridad informática lógicas, físicas y de redes de datos aunado a la fomentación de una cultura de seguridad informática en los usuarios, evitan daños mayores y problemas que puede ocasionar algún intruso o los mismos usuarios.

1.1.1 Evolución histórica de la Seguridad Informática

Haciendo un breve recorrido por la historia de la informática se observa que conforme se va desarrollando la tecnología se van incrementando las necesidades de resguardar y proteger la información que es de importancia para las organizaciones. Cabe mencionar que el mismo concepto de delito informático ha cambiado a través de los años inicialmente consistía en un reconocimiento de “haberlo hecho” donde el transgresor buscaba ser reconocido como la persona que atacó un sitio sin sustraer información del mismo.

En ocasiones acorde al avance tecnológico van apareciendo amenazas que no se tenían contempladas. He aquí algunas fechas clave:

1958: EE.UU. crea ARPA (Advanced Research Projects Agency), ciencia y tecnología aplicada al campo militar.

1960: Los hackers originales utilizaron los primeros mainframes del MIT para desarrollar habilidades y explorar el potencial de la informática.

1969: La agencia de proyectos de investigación avanzados del Departamento de Defensa (DoD), construyó Arpanet.

1970: Captain Crunch y Phreaking telefónico. El "Creeper" es difundido por la red ARPANET. El virus mostraba el mensaje "SOY CREEPER…ATRAPAME SI PUEDES!". Ese mismo año es creado su antídoto: el antivirus Reaper cuya misión era buscar y destruir al Creeper.

1980: La red ARPANET es infectada por un "gusano" y queda 72 horas fuera de servicio. La infección fue originada por Robert Tappan Morris

1986: Aparecen virus que atacan el sector de arranque

1986: Aparecen virus que atacan archivos

1988: Se funda el CERT (Computer Emergency Response Team). Aparece el primer software antivirus, escrito por un desarrollador de Indonesia.

1989: Primer caso de ciberespionaje en Alemania Occidental. The Mentor lanza el manifiesto Conscience of a Hacker, que finaliza con una frase inquietante: "pueden detener a una persona, pero no pueden detenernos a todos"

1993: Aparecen Virus que atacan virus

1999: Nacimiento del software anti-hacking.

2000: Se producen ataques de denegación de servicio (DoS) sobre los grandes nombres de la Red.

2001: XP, el Windows más seguro, es crackeado antes de su lanzamiento.

2007: Se producen varios ataques phishing específicos contra entidades españolas especialmente agresivos a través de un kit que comprende a muchos bancos españoles.

2008: Se descubre una nueva forma de engañar a los servidores DNS para que den respuestas falsas, gracias a un fallo inherente del protocolo. Hasta ahora, no se han dado detalles técnicos sobre el problema.

Como se observa, algunas de las medidas de seguridad que son utilizadas hoy en día surgieron como respuesta a incidentes que no se tenían considerados o que se desarrollaron a la par de nuevas tecnologías, por ello es importante no descartar todas y cada una de las amenazas de las cuales pudiera ser presa nuestro sistema informático y mantener actualizados tanto a expertos en la materia como a usuarios que hagan uso de la información en una organización; "no hay mejor defensa que una buena preparación".

1.1.2 Objetivos y misión de la Seguridad Informática

Entre los principales objetivos de la seguridad informática se destacan los siguientes:

- Proteger los recursos de los sistemas informáticos, siendo prioritaria la protección a la información, pero abarcando también la infraestructura, y el uso de las aplicaciones, entre otros.
- Garantizar la adecuada utilización de los recursos y aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos en los contratos.

La misión de la seguridad informática se puede plantear como una serie de actividades específicas para una organización que le permitan alcanzar los objetivos de seguridad.

Entre las más importantes están las siguientes:

- Desarrollo e implantación de políticas de seguridad que estén relacionadas directamente con las actividades reales de una organización.
- Mejora constante de los sistemas de seguridad por medio de su monitoreo y análisis, así como la adquisición y actualización de tecnologías.
- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Capacitar al personal encargado de la seguridad del sistema para que cuenten con conocimientos actualizados para desempeñar su labor de manera más eficiente.
- Concienciar a los usuarios del sistema informático sobre la importancia de las políticas de seguridad impuestas.

1.2 Amenazas

Las amenazas son la concepción de un peligro latente o factor de riesgo que pueden causar alteraciones a la información de la organización ocasionándole pérdidas materiales, económicas, de información, y de prestigio. Las amenazas se consideran como exteriores a cualquier sistema, es posible establecer medidas para protegerse de las amenazas, pero prácticamente imposible controlarlas y menos aún eliminarlas. A continuación se presentan los principales tipos de amenazas a la información:

a) Factor humano

   Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos. Esta amenaza surge por descuidos, negligencia, inconformidad y susceptibilidad del ser humano a cambiar su comportamiento. Dentro de las amenazas principales se encuentran:

- Ingeniería Social, es la manipulación de la tendencia humana a la confianza, y el objetivo de la persona que ejerce esta acción es obtener la información necesaria para acceder a la información sensible de una persona u organización.

- Ingeniería Social Inversa, se realiza cuando el atacante suplanta a una persona que se encuentra en una posición con autoridad suficiente para que el usuario o la persona de menor rango proporcione la información necesaria para poder producir un ataque.

  Abarca actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados.

b) Hardware

   Se da la amenaza por fallas físicas que presenten en cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

c) Red de datos

   Las dos principales amenazas que se presentan en una red de datos son, la no disponibilidad de la red, y la extracción lógica de información a través de ésta. Cuando la red de comunicación no está disponible, pudiera ser ocasionada por un ataque deliberado por parte de un intruso o un error físico o lógico del sistema mismo (fallas dentro de la planeación). La extracción de la información es cuando un agente pudiera obtener información dentro de la red de comunicación; la amenaza más conocida es un ataque de sniffing en redes Ethernet.

d) Software

   Las amenazas de software incluyen posibles fallas dentro del software de un sistema operativo, software mal desarrollado, mal diseñado o mal implantado, además de que existe software de uso malicioso que representa una amenaza directa contra un sistema.

e) Desastres naturales

   Son eventos que tienen su origen en las fuerzas de la naturaleza. Estos desastres no sólo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad del sistema completo (infraestructura, instalación, componentes, equipos, etc.) pudiendo dejar al sistema incluso en un estado de inoperabilidad permanente. Este tipo de amenazas también incluye la falta de preparación.

1.3 Vulnerabilidades

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 el sistema informático. Se trata de una debilidad que puede ser explotada para violar la seguridad. Las vulnerabilidades son también variadas, y con base en esta definición se presentan 6 tipos de vulnerabilidades:

a) Física

La podemos encontrar en el edificio o en el entorno físico de los sistemas de información. Se le relaciona con la posibilidad de entrar o acceder físicamente al lugar donde se encuentra el sistema para robar, modificar o destruir el mismo. Esta vulnerabilidad se refiere al control de acceso físico al sistema.

b) Natural

Se refiere al grado en el que el sistema puede verse afectado por desastres naturales o ambientales. Las vulnerabilidades pueden ser: no disponer de reguladores, no-Breaks, plantas de energía eléctrica alterna; tener una mala instalación eléctrica en los equipos, en caso de rayos, fallas eléctricas o picos de alta potencia. Otra vulnerabilidad es no estar informado de las condiciones climatológicas locales al construir un centro de cómputo o para tomar medidas en determinado tiempo.

c) Hardware

El no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento del equipo. Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, pueden existir algunos sistemas que no cuenten con la herramienta o tarjeta para poder acceder a los mismos.

d) Software

Este tipo de vulnerabilidad incluye todos los errores de programación en el sistema u otros tipos de aplicaciones que permiten atacar al sistema operativo desde la red explotando la vulnerabilidad en el sistema. Hay que tomar en cuenta que no siempre los sistemas son los únicos que traen errores de programación, también los programas hechos por los usuarios son puntos débiles que se deben de cuidar.

e) Red

Este tipo de vulnerabilidad toma a consideración desde la implementación de un mal diseño del cableado estructurado que no es sujeto a estándares, hasta la modificación total o parcial de la interconexión y transmisión de datos entre dispositivos algunos ejemplos son:

- La facilidad que es el acceso no autorizado al sistema de información de manera externa.
- La intercepción y extracción de información.
- La saturación y disponibilidad de servicios dentro de la organización.

f) Humana

Ser vulnerable a la ingeniería social y a la ingeniería social inversa, el no tener el servicio técnico propio de confianza, mala comunicación con el personal, falta de capacitación a los usuarios para responder ante diferentes situaciones de riesgo, no tener un control de registros de entrada y salida de las personas que visitan el centro de cómputo, falta de credenciales que identifiquen al personal, no tener detectores de metales o no contar con algún tipo de sistema biométríco como: huella digital, verificación de voz o verificación de huellas dactilares.

1.4 Sistemas y Mecanismos de Protección

Una vez conocidas las vulnerabilidades y ataques a los que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras pautas no lo son tanto es responsabilidad de los administradores detectar, sugerir e implementar medidas que permitan asegurar el sistema informático.

1.4.1 Seguridad Física

La seguridad física hace referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas. Los mecanismos de seguridad física deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

La seguridad física se complementa con la seguridad lógica.

1.4.2 Seguridad Lógica

La seguridad lógica se refiere a controles lógicos dentro del software y se implementa mediante la construcción de contraseñas en diversos niveles del sistemas donde permita solo el acceso con base en niveles de seguridad de usuarios con permiso, con base en el sistema operativo que use como plataforma el sistema a implantarse, es posible considerar además a nivel código, algoritmos que generen claves para poder cifrar los archivos de contraseñas dentro del sistema lo cual permita mayor seguridad en un entorno de red. Algunos de los objetivos que plantea la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no tengan capacidad de modificar los programas ni los archivos que no correspondan.
- Asegurar que sean utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.4.3 Seguridad en Redes de Datos

La seguridad es más que evitar accesos no autorizados a los equipos y a sus datos. También incluye el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto de la red. En un entorno de red debe asegurarse la privacidad de los datos. No sólo es importante asegurar la información sensible para la organización, sino también, proteger las operaciones de la red de daños no intencionados o deliberados.

El mantenimiento de la seguridad de la red requiere un equilibrio entre facilitar el acceso a los datos por parte de usuarios o procesos autorizados y restringir el acceso a los datos por parte de los no autorizados. Es responsabilidad de los administradores asegurar que la red se mantenga fiable y segura.

1.4.4 Biometría

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.

Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica. Sus aplicaciones abarcan un gran número de sectores: desde el acceso seguro a computadoras, redes, protección de archivos electrónicos, hasta el control horario y control de acceso físico a una sala de acceso restringido.

Por esta razón la definen como una rama de las matemáticas estadísticas que se ocupa del análisis de datos biológicos y que comprende temas como población, medidas físicas, tratamientos de enfermedades y otros similares.