Nombre del alumno: Johanne Joaquín Arriaga Díaz

Nombre del profesor: Icel Bernardo Lepe Arriaga.

Nombre del trabajo: Ensayo unidad I

Materia: Seguridad en la información.

Grado: Noveno cuatrimestre.

Grupo: ISC13SDC0119-F

Frontera Comalapa, Chiapas a 28 de Mayo de 2022

La seguridad de la información

Todos conocemos la importancia de la información pero sabemos más aún que es importante mantenerla segura y esto queda claro al ver la basta cantidad de capital invertida solamente para mantenerla segura. Solo así podemos tener una referencia al valor de esta y a la importancia de usarla de manera inteligente y gestionarla de esta misma manera. Es por ello que las compañías invierten en preservar muy seguro este preciado recurso y es aquí en donde entra la tecnología más implícitamente en las maquinas que la almacenan y procesan.

La tecnología mencionada anteriormente se refiere a aquel hardware que almacena la información como lo son las bases de datos, software, redes, etc. Que se encarga también de procesarla y todo esto con el único propósito de transformar de manera económica los datos y procesos en conocimiento. Esto si tomamos en cuenta que los datos son descripciones básicas de las cosas, acontecimientos, actividades y transacciones las cuales se clasifican y almacenan. Pueden ser datos numéricos, alfanuméricos, figuras, sonidos e imágenes. La información representa datos organizados que han adquirido valor y significado para el receptor. Y el conocimiento es cuando se sustituye los datos organizados o información que se ha organizado y procesado para que sea entendible.

Pero ¿de qué debemos proteger la información? Realmente existen amenazas desde un punto de vista lógico como lo son software malicioso, que a resumidas cuentas es un programa dañino (virus) el cual se instala en la computadora del usuario o que de alguna otra manera acceda a información personal sin notificarle al usuario y por lo tanto sin su consentimiento. El tema de los virus es muy extenso ya que cada virus que aparece en el mercado cumple funciones distintas y están enfocados a sistemas específicos, su función principal es vulnerar la seguridad del sistema en sí, y apropiarse de los sistemas del equipo, robar información, controlar procesos etc. Y los virus de este tipo usualmente se mantienen ocultos en archivos, memorias y otras formas ocultas en forma de datos útiles a estos se les llama: Virus residentes. Ahora después de conocer los virus residentes también encontramos los virus de acción directa que son aquellos que lo que hacen es ejecutarse rápidamente y extenderse por todo el equipo trayendo consigo el contagio de todo lo que encuentren a su paso y sin que se diga más sabemos que son un tipo de virus peligroso por su propagación y dificultad para erradicar. Los virus cifrados, los de arranque, los del fichero o la sobreescritura son igualmente otros de los peligros contagiosos más importantes que pueden afectar a nuestro ordenador. Y ante tantos peligros encontramos la forma de contraatacar que usualmente son antivirus, cortafuegos, firewalls, la información normalmente se encripta y lo más usual es aquello que usamos a diario como lo son las contraseñas.

Pero no solamente los virus informáticos son los únicos métodos para vulnerar sistemas o robar información también existen formas de acceder a los equipos de forma directa y remota, esto es una intrusión, para lo cual se ha tenido que diseñar su propio programa informático pero también está su contraparte que detecta estas intrusiones y es el conocido anti-spyware, se trata de programas que detectan programas espía que le dan acceso a nuestros equipos a personas ajenas a nosotros, estos anti-spyware detectan de manera inmediata lo que son esos programas espías que se encuentran en nuestro sistema informático y que lo que realizan es una recopilación de información del mismo para luego ofrecérsela a un dispositivo externo sin contar con nuestra autorización en ningún momento.

Para que un sistema pueda ser considerado lo cual quiere decir que solo debe contener información modificable sólo por las personas autorizadas, y solo accesibles a estas mismas personas (confidencial), debe ser irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

De nada servirían tantos programas informáticos si los usuarios no saben a cerca de esos temas y de todas formas, como en la mayoría de los ámbitos de la seguridad, lo esencial sigue siendo la capacitación de los usuarios, esto permitirá mejor seguridad a largo plazo. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.

En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Por ello conocemos dos tipos de seguridad informática: Seguridad física y seguridad lógica. La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención para que no le ocurra nada al ordenador, la seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Y aparte de esto nuestro sistema no sólo puede verse afectado de manera física, sino también contra la Información almacenada, El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren.

Los principales objetivos de la seguridad informática son:

Confidencialidad: es precisamente la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación esto es una medida muy importante que la seguridad informática toma muy en cuenta.

La confidencialidad es uno de los principales problemas a los que se enfrentan muchas empresas; ya que las estadísticas muestran que en los últimos años incremento el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio, etc.

Disponibilidad: podemos decir que es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

Integridad: diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

No repudio: este objetivo garantiza la participación de las partes en una comunicación.

En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.

Como conclusión podemos decir que la seguridad en informática es tan importante ya que en una sociedad tan inmiscuida en la tecnología es muy fácil pasar por alto aspectos tan importantes como lo son la seguridad. Entonces como dice el pensamiento popular, el conocimiento es poder y nosotros tenemos el poder de crear entornos más seguros y poder proteger nuestra información.