Técnico en

DESARROLLO DE SOFTWARE

Seguridad Informática

Instituto Von Neumann

Seguridad Informática

Unidad I

1. Conceptos básicos de seguridad

Dato: Un dato es una representación simbólica de un atributo o variable cuantitativa o cualitativa.

Información: Constitución de grupo de datos, procesados, es decir: ordenados y verificados, la información no es lo mismo que los datos.

Los requerimientos de seguridad de la información dentro de una organización han pasado por dos grandes cambios en las últimas décadas. Antes del uso generalizado del procesamiento de datos equipo, la seguridad de la información considerada valiosa para una organización era principalmente por medios físicos y administrativos. Un ejemplo de lo anterior es el uso de archivadores resistentes con cerradura de combinación para almacenar documentos confidenciales.

En los ordenadores y servidores, la necesidad de herramientas automatizadas para proteger los archivos y otra información almacenada se hicieron evidentes.

Esto es especialmente el caso de un sistema compartido, como un sistema de tiempo compartido, y la necesidad es aún más grave para los sistemas a los que se puede acceder a través de una red telefónica pública, red de datos o Internet.

El segundo gran cambio que afectó la seguridad es la introducción de sistemas distribuidos y el uso de redes e instalaciones de comunicaciones para transportar datos entre el usuario y la computadora y entre computadoras.

Las medidas de seguridad de la red son necesarias para **proteger los datos durante su transmisión**. De hecho, el término seguridad de la red es engañoso, porque prácticamente todas las organizaciones comerciales, gubernamentales y académicas se interconectan mediante equipos de procesamiento de datos con una colección de redes interconectadas. Tal red de redes es lo que se conoce como internet.

La seguridad informática es un tema al que mucha gente no le da la importancia que realmente tiene. Pero los hackers intentan tener acceso a los datos en los ordenadores.

El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sin **copias de seguridad validas**.

El problema más común es el robo de **información sensible** y **confidencial**. La divulgación de la información que posee una empresa sobre sus clientes puede derivar en demandas millonarias contra esta.

La seguridad es inversa a la accesibilidad y esto es visible en la triada de seguridad CID.

2. Triada de seguridad CID (CIA Triad)

La seguridad informática según The National Institute of Standards and Technology (NIST) es definida como la protección otorgada a un sistema de información automatizado para lograr los objetivos aplicables de preservar la integridad, disponibilidad, y confidencialidad de los recursos del sistema de información (incluye hardware, software, firmware, información/datos y telecomunicaciones).

- **Integridad (Integrity):** Se enfoca en que los datos estén protegidos en contra de cambios no autorizados o accidentales.
- **Confidencialidad (Confidenciality):** Esta relacionada con cómo mantener la información, las redes y los sistemas seguros frente a un acceso no autorizado.
- **Disponibilidad (Availability):** Competencia para que el recurso sea accesible para un usuario, aplicación o sistema de computación, siempre que sea requerido.

Como conceptos adicionales tenemos:

- **Autenticidad (Authenticity)**: La propiedad de ser genuino y poder ser verificado y confiado; confianza en la validez de la transmisión, el mensaje o el autor. Esto significa verificar que los usuarios son quienes dicen ser y que cada entrada que llegue al sistema provenga de una fuente confiable.
- **Rendición de cuentas (Accountability)**: El objetivo de seguridad que genera el requisito de acciones de una entidad para ser rastreado únicamente a esa entidad. Esto apoya el no repudio, aislamiento de fallas, detección y prevención de intrusiones, y acción posterior recuperación y acciones legales. Debemos ser capaces de **rastrear una brecha de seguridad a un responsable**. Los sistemas deben mantener registros de sus actividades para permitir posteriores investigaciones forenses para rastrear brechas de seguridad o para ayudar en disputas de transacciones.

3. Factores involucrados en la seguridad informática

En la seguridad informática hay distintos factores que forman parte del conjunto. Entre los cuales tenemos las amenazas, las vulnerabilidades, los ataques.

Vulnerabilidad

Es una **debilidad** en el sistema que puede ser utilizada como superficie de ataque por una amenaza en una circunstancia dada.

Amenaza

Es una potencial violación a la seguridad, que existe cuando hay una acción, evento o circunstancia que permite violar la seguridad y causar daño. Es decir, una amenaza es una **posibilidad** de realizar un ataque sobre una vulnerabilidad.

Ataques

Es un asalto al sistema en cuestión **utilizando una vulnerabilidad deliberadamente** por un actor, para evadir los servicios de seguridad y violar las políticas de seguridad del sistema.

Tipos de ataques:

- **Pasivos**: son los ataques que pretenden aprender y recopilar información de los sistemas perpetrados, pero sin causar ningún daño que afecte el funcionamiento del sistema.
- **Activos**: Es un ataque que busca afectar el funcionamiento del sistema.

La seguridad informática es tan importante como la llave de nuestro auto, de nuestra casa, de nuestro casillero. El enfoque principal de la seguridad en la información como tal recae en contener la información y aislarla de actores no autorizados.

La **integridad** de la información es el factor que evalúa la capacidad de garantizar que un flujo de datos no sea corrompido, duplicado, sin inserciones o reordenamientos.

La **sensibilidad** de la información es el factor de evaluación en la capacidad mantener los datos fuera de los ataques pasivos.

La seguridad es relativa a todos los factores que se involucren dentro del sistema que deseamos proteger, es decir depende del administrador, las políticas de la red, los corta fuegos, la inversión monetaria en seguridad y otros factores.

La seguridad **no es alcanzable es un ideal**, el único sistema seguro es el que esta desconectado de todo acceso.

A todo esto: ¿por qué es tan importante la seguridad?

La seguridad informática es tan importante como la llave de nuestro auto, de nuestra casa, de nuestro casillero, etc. Nadie deja nada de esto con las llaves puestas, mucho menos abierto, el enfoque principal de la seguridad en la información como tal recae en contener la información y aislarla de quien no queremos que tenga acceso, dos puntos

de vista importantes: la integridad de la información: esto es muy importante, cuando se maneja información cualquier cosa puede pasar, como un archivo copia de una versión muy vieja, así como una copia falsa de un programa antivirus por ejemplo, esta es una de las cosas que debemos tomar muy en cuenta debido a que podríamos estar siendo engañados con la información que se nos presenta en pantalla por ejemplo, el segundo es sensibilidad de la información esto conlleva a dar un ejemplo sencillo como el número de cuatro dígitos de seguridad (PIN) de una tarjeta de crédito, partiendo en este punto nos damos cuenta que tan sensible puede ser una pequeña serie de dígitos y que consecuencias podría desencadenar que con un simple vistazo alguien pueda tener acceso a una cuenta bancaria.

Contenido extra

- https://www.microsoft.com/es-es/security/default.aspx
- http://www.cisco.com/web/ES/seguridad-redes/index.html
- “Network Security Essentials”, 6/e, by William Stallings, Chapter 1 – “Introduction”

Descargo de responsabilidad

La información contenida en este documento descargable en formato PDF o PPT es un reflejo del material virtual presentado en la versión online del curso. Por lo tanto, su contenido, gráficos, links de consulta, acotaciones y comentarios son responsabilidad exclusiva de su(s) respectivo(s) autor(es) por lo que su contenido no compromete al área de e-Learning del Departamento GES o al programa académico al que pertenece.

El área de e-Learning no asume ninguna responsabilidad por la actualidad, exactitud, obligaciones de derechos de autor, integridad o calidad de los contenidos proporcionados y se aclara que la utilización de este descargable se encuentra limitada de manera expresa para los propósitos educacionales del curso.