CONCEPTOS BÁSICOS SEGURIDAD INFORMÁTICA

Fader José Beltran, Andrés Cuervo Montoya, Ana Milena Ruiz, Evelyn Patiño, Juan David Ramirez

Documento académico, con conceptos básicos sobre seguridad Informática.

U N A D

G r u p o : 3 0 1 1 2 2 _ 8 4

O c t u b r e 2 0 1 8

Conceptos Básicos Seguridad Informática

1. DEFINICIONES

Es importante conocer algunos términos antes conceptualizar lo que es la seguridad informática.

Dato: De acuerdo a Gil Flores (1994), el dato es "(…) el resultado de un proceso de elaboración, es decir, el dato hay que construirlo" (pág. cap 1). A partir de este concepto se puede decir que el dato es una variable sin analizar que se puede procesar a través de cualquier sistema de información definido. En la siguiente imagen podemos apreciar una forma representar el dato:

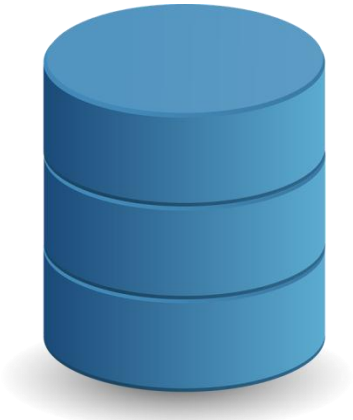

Ilustración de Datos. Tomada de (pixabay.com, 2013).

Información: De forma general, la información puede considerarse como un conjunto de datos recopilados, que brindan a través de algún análisis un conocimiento sobre algo.

Seguridad: Si se busca la definición de la palabra seguridad en diversos medios, se encontrarán numerosos conceptos, sin embargo, en términos generales, se entiende la seguridad como un sistema de apoyo y respaldo, que busca garantizar la tranquilidad y la protección de algo.

Seguridad Informática: Según la UNAM (s.f.)**,** la Seguridad Informática es "el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de una entidad." (pág. 3). La siguiente imagen nos ilustra de forma simbólica un sistema de seguridad informática:

Imagen Seguridad Informática tomada de (Flickr.com, 2014)

Aplicando el concepto general de seguridad en contexto con la definición anterior, podemos definir la seguridad informática como los métodos, estrategias y acciones que permiten proteger la información digital.

Sistemas Informáticos: Un sistema informático, es aquel que está conformado por el hardware, software, datos y personas; los cuales, son el medio a través del cual se genera el almacenamiento, procesamiento y envió de la información.

Con el fin de garantizar la seguridad, un sistema informático requiere la instalación de diversas herramientas, para identificar las herramientas a utilizar, es necesario plantearse los siguientes cuestionamientos:

De acuerdo al documento Capitulo 2. Seguridad Informática (s.f.), se debe realizar la instalación de diversas herramientas que permitan establecer el sistema de seguridad que se requiere. Para esto, según el documento es necesario responder a tres preguntas básicas:

¿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 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. (pág. 4)

En la siguiente imagen se puede visualizar un escudo y un candado que representan la seguridad, superponiéndose a un computador que este caso caracteriza lo que se quiere proteger.

Imagen de seguridad informática Tomada de (Kireeva, s.f.)

2. AMENAZAS Y VULNERABILIDADES

Cuando se habla de seguridad, se debe tener presente que existen amenazas y vulnerabilidades, que básicamente son los elementos que crean la necesidad de implementar sistemas de seguridad. A continuación, se presenta la definición de ambos términos en el contexto de seguridad informática:

Amenazas: Se llama a amenaza, a todo lo que represente un peligro específico para un recurso determinado. Ésta se puede presentar por personas o cualquier otra circunstancia que pueda provocar un daño. La siguiente imagen un hacker como ejemplo de una amenaza:

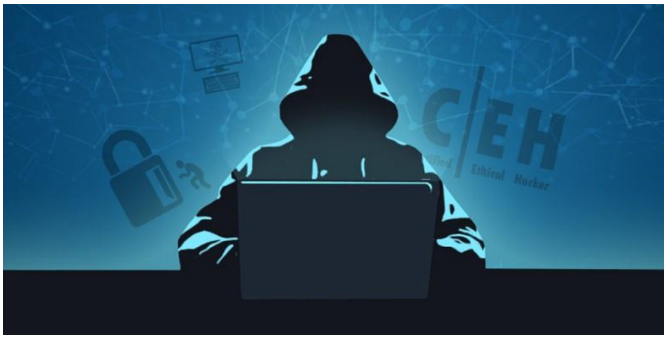

Ilustración de amenaza informática. Tomado de (Fareed, 2017)

Vulnerabilidades: Las vulnerabilidades por su parte, son todas las debilidades que adolece un sistema, y que pueden crear las aperturas necesarias para que las amenazas afecten o dañen el sistema.

Ilustración vulnerabilidad. Tomado de (A Cruz, s.f.)

2.1. CLASIFICACIÓN GENERAL DE LAS AMENAZAS:

Las amenazas se clasifican en los siguientes tipos:

Interrupción: Se origina ante una falencia del sistema que impida el funcionamiento correcto, deteniendo los procesos que se están realizando, ejemplo: un volcado de memoria o los famosos pantallazos azules de Windows que interrumpen el correcto funcionamiento del sistema operativo. Este tipo de amenazas, se pueden identificar rápidamente ya que son evidentes y tienen un impacto instantáneo en el trabajo del usuario.

Intercepción: Según Capitulo 2. Seguridad Informática (s.f.) la intercepción "es el acceso a la información por parte de personas no autorizadas" (pág. 3). Un ejemplo común, son las famosas chuzadas, que no son otra cosa que interceptaciones telefónicas ilegales.

Modificación: A diferencia de la Intercepción, que es un acceso no autorizado a un sistema que busca primordialmente captar y obtener información, tenemos que una amenaza de modificación, se caracteriza porque además de que el elemento externo accede al sistema, también efectúa cambios dentro del mismo. Como ejemplo tenemos la modificación de una base de datos accediendo al lenguaje DDL.

Generación: Este tipo de amenaza, se caracteriza por el acceso pleno al sistema informático, añadiendo y creando información.

Bibliografía

Fareed, H. (24 de Noviembre de 2017). *Ilustración Amenaza seguridad Informática*. Recuperado el 16 de Octubre de 2018, de medium.com: https://medium.com/secjuice/how-to-start-your-career-in-any-field-related-to-information-security-841adcf20901

Flickr.com. (24 de 10 de 2014). *photos/tecnomovida/15427075000*. Recuperado el 16 de 10 de 2018, de flickr.com: https://www.flickr.com/photos/tecnomovida/15427075000

Gil Flores, J. (1994). *Análisis de Datos Cualitativos. Aplicaciones a la Investigación Educativa.* Barcelona: PPU.

Kireeva, Y. (s.f.). *logo seguridad informatical*. Recuperado el 16 de Octubre de 2018, de 123rf: https://es.123rf.com/photo_64043712_la-seguridad-inform%C3%A1tica-proteger-sus-conceptos-port%C3%A1tiles-cuaderno-y-icono-del-escudo-con-candado-ilust.html

pixabay.com. (10 de Octubre de 2013). *base de datos almacenamiento de datos*. Recuperado el 16 de Octubre de 2018, de pixabay.com: https://pixabay.com/es/base-de-datos-almacenamiento-de-datos-149760/

UNAM. (s.f.). *Capitulo 1. Conceptos Básicos.* Recuperado el 16 de Octubre de 2018, de Universidad Nacional Autónoma de México: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/775/A4.pdf?sequence=4

UNAM. (s.f.). *Capitulo 2. Seguridad Informática.* Recuperado el 17 de Octubre de 2018, de Universidad Nacional Autonoma de Mexico: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/250/A5.pdf?sequence=5

.