CRITERIOS Y PRINCIPIOS DE SEGURIDAD INFORMÁTICA

Fader José Beltrán, Andrés Cuervo Montoya, Ana Milena Ruiz, Evelyn Patiño, Juan David Ramírez

Documento académico, donde se explican los criterios y principios de la seguridad informática

UNAD

Grupo: 301122_84

Octubre 2018

PRINCIPIOS Y CRITERIOS DE LA SEGURIDAD INFORMÁTICA

1. Principios

Según (UNAM, s.f.) Hay tres principios de la seguridad informática que son:

- Principio del Acceso más fácil
- Principio de caducidad de la información
- Principio de la eficiencia (pág. 1)

Principio del Acceso más fácil: El principio del Acceso más Fácil, hace énfasis en el hecho de que el intruso del sistema siempre buscará las formas más simples de lograr el acceso, lo cual hace encontrando las debilidades.

Ilustración Fácil Acceso. Autoría Propia .Octubre 2018

Teniendo en cuenta las debilidades que presenta un sistema es necesario identificar:

1. La manera en que se muestran estas debilidades.
2. Qué tipo de amenazas pueden sacar provecho de las debilidades presentes.
3. Qué medidas tomar para manejar la situación.

Dando alcance al primer punto, se puede decir que las debilidades se manifiestan por causa de tres factores que son la exposición, las amenazas y las vulnerabilidades. La exposición, es básicamente el riesgo que tiene un sistema de sufrir daños por causa de accesos no autorizados o malos manejos. Las amenazas por su parte, son una situación, cosa o persona que de forma fortuita o voluntaria puede representar un peligro latente para la estabilidad y correcto funcionamiento de un sistema de información. En cuanto a las vulnerabilidades, son el punto más frágil de un sistema, y es precisamente el factor crítico de la seguridad informática poder identificarlas para minimizar la exposición de un sistema y prevenir las posibles amenazas.

Sobre el segundo punto, hay que tener claro cuales amenazas se pueden presentar tales como errores de manejo, desastres, ataques directos o indirectos al sistema a través de virus o diferentes tipos de malwares, fallas de nivel físico y lógico en el sistema, etc. Una vez identificado lo anterior, y teniendo en cuenta que el objeto de ataque puede ser el hardware, el software o los datos, es necesario clasificar las amenazas, que según (UNAM, s.f.) se clasifican en “amenazas de interrupción, intercepción, modificación y generación de la información en general.” (pág. 2).

El tercer punto, hace referencia a los métodos, estrategias, herramientas y todo lo necesario para implementar un sistema de seguridad que pueda garantizar la protección del sistema información.

Principio de Caducidad de la información: Este principio hace énfasis en definir la vida útil de un dato, como límite temporal para la protección del mismo. Básicamente, se conoce que la información tiene una caducidad, y por tanto la protección de los datos será acorde con al tiempo que se proyecte para mantener sus restricciones de seguridad. Así pues, en pro de la relevancia que tenga la información a proteger se definirá la complejidad de los sistemas implementados.

Principio de la Eficiencia: Este principio, hace énfasis en que las medidas de control implementadas sean de verdadera utilidad para las situaciones específicas, y que además, sean simples y no más complejas de la cuenta.

Se entiende que algo eficiente es funcional, por tanto para que un sistema de seguridad cumpla con este principio, es necesario que las funciones programadas respondan a cabalidad en el momento oportuno y con una buena utilización de recursos.

2. CRITERIOS

Existen numerosos criterios en lo que se refiere a la seguridad informática, sin embargo, este documento se enfocará en los tres criterios principales que son:

Integridad: Es un requerimiento fundamental que la información enviada sea la misma que se recibe y viceversa, los datos no deben sufrir cambios sin autorización. Los cambios no autorizados son la puerta de entrada para que se cometan actos delictivos como fraudes o secuestros de información. Si bien, la integridad es uno de los criterios de mayor relevancia en cualquier campo que utilice sistemas de información, toma más relevancia aún en sectores que involucren transacciones constantes como lo es por ejemplo el sector financiero.

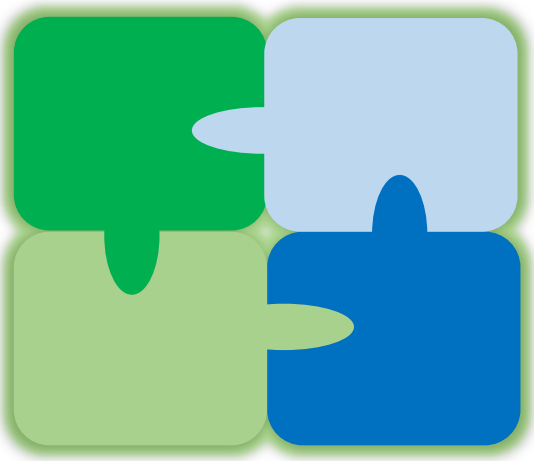

Ilustración Integridad. Autoría Propia Octubre 2018

Confidencialidad: Según Jerez Lugo (2004) el criterio de confidencialidad se refiere a "la protección de datos frente a la difusión no autorizada", haciendo referencia a que la información no se debe divulgar sin autorización. Este criterio, toma mayor relevancia teniendo en cuenta las leyes existentes sobre la protección de datos personales que hace que, principalmente en el sector corporativo adopten sistemas de protección de los datos. Como ejemplo, se encuentra la ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales.

Ilustración Confidencialidad. Autoría Propia Octubre 2018

Jerez Lugo, C. A. (6 de Mayo de 2004). *Seguridad para lograr Confiabilidad y Calidad de los Servicios Digitales en Internet.* Recuperado el 20 de Octubre de 2018, de Universidad de Las Américas Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf

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