Starling Germosen Reynoso 2014-1569

**Introducción**

El tema de la seguridad y gestión de la información está en boca de todo el mundo hoy día, a pesar de que es un tema viejo, hoy se ha puesto de moda por el incremento sustancial de las redes sociales, las cuales a su vez han hecho que nos convirtamos en dependientes de los dispositivos electrónicos y por consecuencia queramos realizar todo tipo de transacciones via los aparaticos como suele decir el maestro de la radio Álvaro Arvelo hijo, es por esto que la gestión informática, el uso de los datos y un gran número de conceptos raros y novedosos se suman a nuestro vocabulario y tenemos una base de la misma aunque no sepamos a en detalle lo que estas son.

Mi objetivo no es dar una descripción detallada y digerible de estos conceptos para entremezclarlos y sacar una batida que sea provechosa para el cerebro de cada lector, sino más bien ser más pragmático en cuando a los mismos y relacionarlos directamente con la seguridad de la información.

**Confidencialidad, integridad, disponibilidad, autenticación y no repudio.**

 La Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la [Tríada CIA](https://es.wikipedia.org/w/index.php?title=Tr%C3%ADada_CIA&action=edit&redlink=1), del inglés: "**C**onfidentiality, **I**ntegrity, **A**vailability") son los principios básicos de la seguridad de la información. Además de que estos términos son usados frecuentemente como sinónimos para poder definir el concepto de seguridad de la información. El objetivo de la seguridad radica en estos tres principios de manera integral.

El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.

La Autenticación que se define como la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra, esto es seguridad

No repudio al proporcionar en si mismo protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. Se convirtió en uno de los mecanismos mas usados en lo que tiene que ver con salvaguarda de los datos este, está estandarizado en la ISO-7498-2.

**Persona, tecnología y proceso.**

La relación entre estos 3 componentes y la seguridad de la información radica en que tanto las personas (recursos humanos) como los distintos procesos y las tecnologías a implementar tienen igual importancia o relevancia para el buen funcionamiento o efectividad de los sistemas de seguridad de la información.

Actualmente se considera que las nuevas tecnologías informáticas han cambiado nuestro modo de vivir, este desarrollo ha conllevado a cambios en la forma de actuar y de pensar de los hombres y ha traído con ello nuevas pautas de comportamiento inherentes a la dignidad humana. En los últimos años se están planteando a nivel internacional la necesidad de desarrollar e implantar el código ético y de seguridad informática que regule el saber informático.

Funcionalidad, seguridad y facilidad de uso.

Estos 3 aspectos forman el triángulo definido por el Consejo Internacional de consultores de E-Commerce, EC-Council por sus siglas en inglés, fundamental en el desarrollo de aplicaciones. Dicho triángulo está conformado por la funcionalidad, la usabilidad y la seguridad.

* Funcionalidad: es el conjunto de capacidades operativas y funcionales proporcionadas por los dispositivos. Por ejemplo, aplicaciones y widgets.
* Usabilidad: facilidades de uso de los dispositivos. Por ejemplo, interfaces más amigables e intuitivas.
* Seguridad: mecanismos implementados para asegurar la confidencialidad, integridad y disponibilidad de la información que es almacenada y/o utilizada en los dispositivos.

**“El desarrollo de cualquier tecnología debe buscar el equilibrio apropiado entre los tres aspectos para el buen funcionamiento de los sistemas de seguridad de información”.**

Entendiendo que la funcionalidad y usabilidad muchas veces van en direcciones opuestas a la seguridad en la información, es decir, la implementación de rigurosos sistemas de seguridad, implica una restricción en el nivel de implementación de capacidades operativas y el desarrollo de interfaces amigables.

En la mayor parte de los casos se le da más importancia a los aspectos funcionales y de uso (usabilidad) que a la seguridad de la información.