Introducción

La seguridad informática se entiende por el conjunto de normas,

Procedimientos y Herramientas con un objetivo en mantener y garantizar la disponibilidad integridad y confidencialidad del buen uso de la información almacenada en un sistema informático o ordenador.

ya que hoy en día hay personas con malas intensiones que intenta tener acceso a nuestros ordenadores y recopilar nuestra información, ya que con el acceso a una red informática o un equipo lleva una posible consecuencias como la perdida de datos ya que asi tengamos copias de seguridad no siempre es posible recuperar todos los datos.

el otro que es la perdida de información sensible y confidencial, la divulgación de la información de los usuarios, ejemplo las contraseñas de nuestras redes sociales correo electrónico….

Hoy en día con las constante evolución de los computadores se debe tener en cuenta los recurso necesarios para poder mantener la seguridad en los sistemas informáticos .

Objetivos

* Conocer conceptos de la seguridad informática,
* Conocer mecanismos de seguridad informática
* Tipos de riesgo

**Seguridad Informática**

La seguridad informática es la disciplina que se Ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

**Principios de Seguridad Informática**

La seguridad informática se fundamenta en tres principios que se deben cumplir en todo sistema.

**CONFIDENCIALIDAD**

Se refiere ala privacidad de elementos informáticos almacenados y procesados en un sistema informática deben proteger sistema de invasiones y acceso a personas o programas no autorizados

**INTEGRIDAD**

Se refiere a la validez y consistencia de los elementos de información almacenados y [procesador](https://www.monografias.com/trabajos5/sisope/sisope.shtml) en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los [procesos](https://www.monografias.com/trabajos14/administ-procesos/administ-procesos.shtml#PROCE) de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios , computadores y procesos comparten la misma información.

**DISPONIBILIDAD**

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

**TIPOS DE RIESGOS**