UNIVERSIDAD DEL SURESTE DE LA FRONTERA COMALAPA

ASIGNATURA: Seguridad en la Información

DOCENTE: Liliana Lizeth Mejia Salaz

ALUMNO: Josué Roberto Pérez López

CUATRIMESTRE: Noveno

GRUPO: A

CARRERA: Ingeniería en sistemas computacionales.

PARCIAL: Primero

TRABAJO: Mapa Conceptual Unidad I

FECHA: 13 de Mayo de 2023.

INTRODUCCIÓN A LA SEGURIDAD INFORMACIÓN

EL VALOR DE LA INFORMACIÓN

La información tiene un gran impacto en la toma de decisiones. Aunque no tiene valor absoluto, su valor esta relacionado con quien lo usa y en la situación de uso.

La tecnología en un sistema de información se refiere a aquellos dispositivos comohardware, bases de datos, software, redes y otros que se emplean para procesar la información.

La meta principal del sistema de información: transformar en forma económica los datos y procesos en conocimiento

DEFINICIÓN Y TIPOS DE SEGURIDAD INFORMACIÓN

Un sistema informático puede ser protegido desde un punto de vista lógico (con el software o físico (vinculado al mantenimiento eléctrico, por ejemplo)

Las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como virus) o llegar via remota.

Entre las herramientas mas usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos, la encriptacion de la información, y el uso de contraseñas.

OBJETIVOS DE LA SEGURIDAD INFORMACIÓN

Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de informacion, incluyendo, hardware, software, firmware y aquella informacion de procesan, almacenan y comunican.

El objetivo del dominio es establecer la administración de la seguridad de la información, siendo la parte fundamental de los objetivos y las actividades de la empresa.

POSIBLES RIESGOS EN LA INFORMACIÓN

Para que el sistema de información de una organización sea fiable hay que garantizar que se mantengan los tres principios de la triada CID

Para evitar riesgos innecesarios debemos:
Formar a los trabajadores la cultura de ciberseguridad.
Limitar el uso a los trabajadoress en los ordenadores de la empresa.

TÉCNICAS DE ASEGURAMIENTO DEL SISTEMA

Tener instalado en la máquina únicamente el software necesario reduce riesgos

Tener controlado el software asegura la calidad de la procedencia del mismo

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

CRIPTOGRAFÍA CLÁSICA: UN PRIMER ACERCAMIENTO

Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet

Un mensaje codificado por un método de criptografía debe ser privado, o sea, solamente aquel que envió y aquel que recibe debe tener acceso al contenido del mensaje.

Las claves criptográficas pueden ser básicamente de dos tipos:
1.- Simétricas
2.- Asimetricas

CRIPTOGRAFÍA EN LA ANTIGÜEDAD

La criptografía es una técnica muy antigua, y durante mucho tiempo se ha relacionado con los círculos militares, religiosos y comerciales.

El origen de esta técnica se remonta al año 400 a. C. Era utilizada en la antigua Grecia por los espartanos para enviar mensajes ocultos entre las tropas militares.

Remontándose al 100 a.C. el "Cifrado Cesar" nació con la necesidad de ocultar información escrita en latín por parte del ejército de Julio César. La técnica utilizada para cifrar un mensaje en el "Cifrado Cesar" era sustituir cada una de las letras del mensaje por aquella que ocupaba tres posiciones más en el alfabeto.