TRABAJO PRACTICO
N° 1

SEGURIDAD INFORMATICA

Mariano Cerusico leg 21826

Cesar Paz leg 29247

Legajo: 21826

Comisión: 3k3 Año: 2021

Cerusico Mariano
Bermúdez Carlos
Paz Cesar

¿Qué es la Seguridad Informática? Importancia en un ámbito informatizado.

La seguridad informática es una disciplina de la informática que se encarga de proteger los objetivos básicos de la seguridad brindando a través políticas, métodos, estándares que debería ser implementados además de los conocimientos para proteger nuestros entornos informáticos y hacerlos más seguros.

En general, podemos definir la SEGURIDAD INFORMATICA, como: "La característica que indica que un sistema está libre de todo peligro, daño o riesgo."

Otro tema que deberíamos abordar, para tener en cuenta es, la seguridad de la información: ya que, estamos hablando de que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

La detección de vulnerabilidades y la seguridad informática es fundamental para mantener siempre segura e intacta la información privada de las empresas, por ello, contar con este tipo de herramientas constituye, además de una necesidad, una inversión a corto, mediano y largo plazo.

¿Como se debe considerar la INFORMACIÓN? ¿Cuál es su Valor?

La información es hoy en día considerada como un bien activo en la organización, de un importante valor económico no tangible, por lo que se hace necesaria la instalación de controles destinados a su protección.

Definir que es Autenticidad, Integridad, Operatividad y confidencialidad.

La información está sujeta a determinadas contingencias que pueden afectar las propiedades que la caracterizan. Estas propiedades se refieren a su *INTEGRIDAD, OPERATIVIDAD, CONFIDENCIALIDAD , Y AUTENTICIDAD.*

- **INTEGRIDAD:** Es una característica que asegura que su contenido permanezca invariable a menos que sea modificado por una personas y/o procesos debidamente autorizados. Podríamos decir que la integridad existe cuando la información no difiere de la contenida en sus documentos originales y no ha sido accidentalmente o maliciosamente alterada o destruida.
- **OPERATIVIDAD O DISPONIBILIDAD**: Capacidad de tener la informacion accesible para ser procesada y/o consultada. Esto requiere que esté correctamente almacenada en los formatos preestablecidos y que el hardware que lo contiene funcione adecuadamente.
- **CONFIDENCIALIDAD O PRIVACIDAD:** Es la necesidad de que la información sea sólo conocida por personas y/o procesos debidamente autorizados.
- **AUTENTICIDAD:** Es la propiedad de poder reconocer y certificar el origen y destino de la información, como así la documentación que la sustenta. Podemos corroborar que una entidad, ya sea de origen o destino de la información, es la deseada.

Sistemas de Información y Sistemas Informáticos.

Sistema de información: es un conjunto de elementos relacionados entre sí, que se encarga de procesar manual y/o automáticamente datos, en función de determinar los objetivos.

Sistema Informático: es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan.
Un Sistema Informático puede formar parte de un Sistema de Información; en este último la información, uso y acceso a la misma, no necesariamente está informatizada.

Dispositivos Lógicos y Físicos

Dispositivos Lógicos:

El software se refiere a los programas y datos almacenados en un ordenador. En otras palabras, son las instrucciones responsables de que el hardware (la máquina) realice su tarea.
El software puede dividirse en tres categorías básicas:

- **Software del sistema:** Es un conjunto de programas que controlan los trabajos de la computadora. Se encarga de administrar y asignar los recursos del Hardware.
- **Software de aplicación**: Son los programas que controlan y dirigen las distintas tareas que se realizan la computadora. Creando un ambiente amigable entre el PC y el usuario.
- **Software de Programación:** Son los lenguajes de programación, intérpretes, compiladores y aplicaciones similares utilizadas por los desarrolladores de sistemas.

Dispositivos Físicos:

Llamados Hardware, son todos los componentes y dispositivos físicos y tangibles que forman una computadora como la CPU o la placa madre, etc.
Los dispositivos del Hardware se dividen en dos.

- **El Hardware Básico:** son las piezas fundamentales e imprescindibles para que la computadora funcione como son: Placa base, monitor, teclado y ratón.
- **El Hardware Complementario:** son todos aquellos dispositivos adicionales no esenciales como pueden ser: impresora, escáner, cámara de vídeo digital, webcam, etc.

Definir Ataques Pasivos y Activos.

Ataque Pasivo:

Los ataques pasivos ponen en peligro la confidencialidad, ya que se centran en observar o copiar el contenido de archivos o mensajes.

Ataque Activo:

Los ataques activos buscan cambiar o modificar el contenido de los mensajes, suponiendo un peligro para la integridad y la disponibilidad.

Definir lo que es un Plan sobre Seguridad Informática – Cuales son las partes y definir cada una de ellas.

El Plan de Seguridad Informatica es la expresion grafica del Distema de Seguridad Informatica diseñado u constituye el documento basico que establece los pirncipios organizativos y funcionales de la actividad de Seguridad Informatica en una Entidad y recoge claramente las politicas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informatico, asi como las medidas y procedimientos que permitan prevenir, detecar y responder a las amenzas que gravitan sobre el mismo.

¿Qué es el Análisis de Riesgo? . Clasificación de los Riesgos y Contingencias.

En un Sistema informático los riesgos son muchos y, además, de variada naturaleza. Para la toma de decisiones basadas en elementos de juicio que posibiliten, hasta donde resulte factible, la eliminación de la incertidumbre, resultará necesario un análisis de los riesgos que permita su conocimiento, probabilidad de ocurrencia y cuantificación.
Es necesario determinar:

A) Qué se necesita proteger?

B) De qué debo protegerlo?

C) En qué grado se necesita proteger?

En respuesta a la primera interrogante, o sea determinar cuáles son los elementos componentes del sistema a proteger, se debe realizar una lista minuciosa del sistema informático y sus interrelaciones, haciendo incapie en el conjunto de datos críticos

1) para el desembolvimiento de la organización y

2) para el funcionamiento del sistema en sí.

A partir de esta respuesta, podemos, partiendo de una clasificación básica de los riesgos, determinar de qué debemos proteger el sistema de la organización.

Clasificación de riesgos:

- **Riesgos de origen natural:** Catástrofes climáticas o tectonicas o atmosféricos: solo determinadas zonas de una región so propensas a terremotos, vulcanismo, tornados, inundaciones, grandes lluvias, napas freaticas, etc., que representan en general un riesgo para la operatividad del sistema, que en su extremo puede ocasionar la imposibilidad de seguir operando el sistema.
- **Riesgos de origen técnico:** Las contingencias debidas a fallas de origen técnico en un sistema informático pueden provenir del mismo sistema (fallas de hardware o de software) o de sistemas externos vinculados o no con aquel (incendios, alimentación eléctrica, aire acondicionado, telecomunicaciones).

En estas situaciones, difíciles de preveer no solo en su ocurrencia sino también en su magnitud.

El objetivo esencial del control y de la seguridad de los sistemas informáticos es mantener la autenticidad, integridad, operatividad y confidencialidad de la información manejada o almacenada en computadoras, frente a contingencias que pueden generar la pérdida de archivos, o de registros o bien la alteración de uno o más registros, o que alteren la prestación de un servicio o la rentabilidad de la organización.

Para la seguridad informática, un sistema informático está formado por las personas, computadoras, papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones.

Para eliminar o disminuir el riesgo de ocurrencia o bien para limitar las consecuencias de una contingencia, existen distintos tipos de actividades o funciones de control o seguridad.

Las contingencias pueden ser de carácter intencional o accidental y pueden ser categorizadas en actos de naturaleza, errores u omisiones, actos fraudulentos y daño intencional ocasionado por los individuos.

En base a ello podemos ensayar una clasificación por el origen de la contingencia en:

- **Contingencias de Origen Natural:** producidas por fenómenos naturales, climatológicos o tectónicos. Incendios forestales, inundaciones, tormentas eléctricas, terremotos, maremotos, etc.
- **Contingencias de Origen Técnico:** las que podremos subdividir en **Contingencias de Origen Técnico vinculadas directamente con el sistema informático** (Fallas de Hardware -disco rígido, fuente de alimentación, fallas en las impresoras, en los modems, en el monitor; Fallas de Software - incompatibilidades de librerías, conflictos en el uso de recursos, errores de programación);

  y **Contingencias de Origen Técnico no vinculadas directamente con el sistema informático** (Fallas en la red de Energía Eléctrica, fallas en los sistemas de climatización, proximidad a sistemas generadores de campos electromagnéticos - motores, ascensores-, fallas en sistemas de distribución de fluidos -gases o líquidos - por explosiones, humedad)

- **Contingencias de Origen Humano:** ocasionadas por la interacción entre el hombre y el sistema informático, puede tratarse de hechos fortuitos o no; que actúan contra el recurso físico o lógico (datos erróneos, alteración de programas, destrucción de periféricos, virus informáticos, negación de servicios).

Ejercicio de Cálculo de Pérdida Potencial por Incidencia

*P.P.P.I. = (FACTOR DE RIESGOS * PERDIDA POTENCIAL)/ 1.000*

Riesgos	*Factor de Riesgos*	*Perdida Potencial*	*PPPI*
Inundación	*1*	*$20.000*	*20*
Robo Común	*2*	*$20.000*	*40*
Errores de Carga de Datos	*2*	*$25.000*	*50*
Accesos No Autorizados	*3*	*$50.000*	*150*

Fraude	*3*	*$15.000*	*45*
Virus	*3*	*$ 5.000*	*15*
Fuego	*1*	*$20.000*	*20*
Fallas en el Sistema de Alimentación Eléctrica	*2*	*$10.000*	*20*
Fallas de Sistemas de Terceros Instalados	*4*	*$25.000*	*100*

Riesgos	PPPI	Contramedidas Alternativas
Fallas de Sistemas de Terceros Instalados	100	Mecanismos de control de acceso
Accesos No Autorizados	150	Mecanismos de identificación e autentificación y Mecanismos de control de acceso
Fraude	45	Mecanismos de seguridad en las comunicaciones y Mecanismos de control de acceso.
Virus	15	Prevención, Detección y Recuperación
Errores de Carga de Datos	50	Mecanismos de Identificación e autenticación
Robo Común	40	Mecanismos de Separación y Mecanismos de seguridad en las comunicaciones
Fallas en el Sistema de Alimentación Eléctrica	20	Prevención, Detección y Recuperación
Fuego	20	Prevención, Detección y Recuperación
Inundación	20	Prevención, Detección y Recuperación